CA RiskMinder™

Release Notes

r3.1

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 9

Operating System Support 9
Documentation 9
Technical Support 9

Chapter 2: New Features 11

Support for MySQL 11
Silent Execution of Rules 11
Deleted Rule Listed in the Active Set 12
Support for the Plugin Store 12
Deleting Rulesets 12
Adding Custom Actions 12
Introduction of Rule Builder User Interface for Creating and Managing Rules 13
Introduction of Instance Management 14
Enhancements to DeviceDNA 15
  Integration with Advanced Version of DeviceDNA 15
  Collection of System Fonts to Generate Risk Profile 15
  Client Not Dependent on Java Runtime Environment 15
  Support for Logical Upgrade of DeviceDNA Elements 15
Support for Device ID Categories 16
Introduction of Two New Rules Based on Device ID 16
Support for Configuration of Reverse Lookup Threshold for Device MFP Match Rule 16
Support for Identification of Device Types 17
Support for Cross-Channel Information for Risk Evaluation 17
Enhancements to Case Management 18
  Support for Multiple Queues 18
  Separation of Case Management Queuing Server Cache Refresh and Queue Rebuild 19
  Other Enhancements to Case Management 19
Support for Additional Software (Application Server and Directory Servers) 20
Enhancements to Rule-Writing and Related Capabilities 20
  Introduction of New Rule Based on Action Velocity 20
  Support for Writing New Rules Based on System Time 21
  Support for Amount Check Rule Using Currency Conversion 21
  Support for Writing New Rules Based on Transaction Actions 21
  Improved Performance of List-Based Lookup Rules 21
Support for Encryption of Information Stored by RiskMinder 22

Enhancements to the Administration Console 22
Support for Additional Administrator Profile Settings 22
Support for Separate Password Policy for Master Administrators 23
Provision to Temporarily Lock Administrator's Password Credential 23
Support for Password History Check 23
Support for Configuration of a Different Encryption Key Per Organization 23
Support to Re-Create a New User With Deleted User's User Name 23
Support to Re-Create a New Administrator With Deleted Administrator's User Name 24
Support for Additional Contact Information 24
Support to Add Custom Attributes to Users From an LDAP-Based Organization 24
Support for Uploading Users and User Account Information in Bulk 24
Provision for Setting Miscellaneous Configurations 24
Support for Reverse Lookup for Device Identification 25
Enhancements to RiskMinder Server 25
Integrated Cache Refresh 25
Support for Database Query Timeout 25
Provision to Process Ongoing Transactions During Server Shutdown 26
Enhanced Quova Upload Tool 26
Support for RiskMinder Server to Use One Database Connection Per Transaction 26
Introduction of Accounts 26
Support for Multiple Accounts 27
Support for Temporarily Deactivating User Account 27
Enhancements to Reporting 27
Support for Exporting Administrator Reports Before Viewing 27
Introduction of New Report Download Tool 28
Introduction of New Device Summary Report 28
Enhancements to RiskMinder APIs 28
Response Codes and Reason Codes 28
Null Machine FingerPrint (MFP) and IP Address Values Allowed 28
Enhancements to RiskMinder Web Services 28
Support for Authentication and Authorization for Risk Evaluation Web Services 29
Support to Expose Organization Management Features Through Web Services 29
Logging Enhancements 30

Chapter 3: Changed Features 31

New Rules to Replace Four Existing Rules 31
Location of Case Management Reports 32
Deprecated Features 32

Chapter 4: Known Issues 33

Documentation Not Available for One-Way SSL Communication Between RiskMinder Components and Database Servers 33
Cannot Use Administration Console to Delete Information About Users Deleted from LDAP Organization 34
Localization Configuration Not Supported for Date and Time Input Values 34
Bulk Upload of User Accounts Does Not Accept a Range of Values for the Account Status 34
Uninstallation Must Be Performed in Reverse Order 34
Administrators Allowed to Create an Organization Called SYSTEM 35
Multi-Byte Characters Supported for List Name and Category Mapping Name 35
Implicit User Creation Successful if Email is the Only Mandatory Parameter 35
Cache Refresh Fails After Database Failover 35
Administration Console Not Connecting to RiskMinder Server During Database Failover 35
Issue with Reverse Lookup Functionality 35
Risk Evaluation with Empty MFP Value Fails in Sample Application 2.0 36
Administration Console Not Displayed Correctly After Upgrading to Internet Explorer 9.0 36
Registry Entries are Not Removed After Uninstallation 36
Log File Location Displayed on Installer Screen is Not Intuitive 37
Null Pointer Exception is Logged When arcotcommon.ini is Missing 37

Chapter 5: Defects Fixed 39

Default Ruleset Not Created for an Organization That Was Created When RiskMinder was Down 39
Refreshing RiskMinder Resulted in Performance Issues 39
RiskMinder Occasionally Unable to Switch to Backup Database 40
Rule Mnemonic Length was Not Restricted to 25 Characters 40
Two Levels of Cache Refresh Required After Updating Default Organization Configuration 40
Filtering By Rule When Analyzing Transactions in Case Management Did Not Work for Microsoft SQL Server 41
Organizations Created Before RiskMinder Deployment Not Read by RiskMinder 41
Incoming Transactions Processed Even When the Server was Stopped 41

Chapter 6: Product Limitations 43

Chapter 1: General Release Information

This section contains the following topics:

Operating System Support (see page 9)
Documentation (see page 9)
Technical Support (see page 9)

Operating System Support

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

For detailed information about platform support and system requirements, see the *CA RiskMinder 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 RiskMinder Installation and Deployment Guide for UNIX Platforms
- CA RiskMinder Installation and Deployment Guide for Microsoft Windows
- CA RiskMinder Administration Guide
- CA RiskMinder Java Developer's Guide
- CA RiskMinder Web Services Developer's Guide
- CA RiskMinder 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 MySQL (see page 11)
Silent Execution of Rules (see page 11)
Deleted Rule Listed in the Active Set (see page 12)
Support for the Plugin Store (see page 12)
Deleting Rulesets (see page 12)
Adding Custom Actions (see page 12)
Introduction of Rule Builder User Interface for Creating and Managing Rules (see page 13)
Introduction of Instance Management (see page 14)
Enhancements to DeviceDNA (see page 15)
Support for Device ID Categories (see page 16)
Introduction of Two New Rules Based on Device ID (see page 16)
Support for Configuration of Reverse Lookup Threshold for Device MFP Match Rule (see page 16)
Support for Identification of Device Types (see page 17)
Support for Cross-Channel Information for Risk Evaluation (see page 17)
Enhancements to Case Management (see page 18)
Support for Additional Software (Application Server and Directory Servers) (see page 20)
Enhancements to Rule-Writing and Related Capabilities (see page 20)
Support for Encryption of Information Stored by RiskMinder (see page 22)
Enhancements to the Administration Console (see page 22)
Enhancements to RiskMinder Server (see page 25)
Introduction of Accounts (see page 26)
Enhancements to Reporting (see page 27)
Enhancements to RiskMinder APIs (see page 28)
Enhancements to RiskMinder Web Services (see page 28)
Logging Enhancements (see page 30)

Support for MySQL

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

Silent Execution of Rules

From this release onward, a rule whose score is 0 is considered to be a silent rule. Such a rule is not used for scoring. This feature allows you to observe how a rule would execute during transactions, without the risk of unintended effects on end users. In earlier releases, a rule whose score is 0 always generates the ALLOW advice.

Deleted Rule Listed in the Active Set

In earlier releases, when a rule is deleted by using the rule editor, it is removed from the proposed and active set that are displayed in the Administration Console. This is regardless of the fact that the rule is still active in the production environment. From this release onward, when you delete a rule, it continues to be displayed in the active set. In addition, a message stating the rule is deleted is displayed in the proposed set.

Support for the Plugin Store

From CA RiskMinder Client release 2.1 onward, the CA AuthMinder plugin store is supported as one of the options for storing the Device ID on an end user’s device. This plugin store is created when the CA ArcotID OTP client application is installed on the end user's device. Among the storage options that are supported, the plugin store is the most persistent storage option. A Device ID that is placed in the plugin store cannot be deleted by common end user actions such as clearing browser cache and deleting browser cookies.

Deleting Rulesets

From this release onward, you can delete rulesets that are not currently assigned to an organization.

Adding Custom Actions

From this release onward, you can add custom actions and then use these actions to build rules.

Introduction of Rule Builder User Interface for Creating and Managing Rules

The user interface for rule management has been simplified and made more intuitive in this release. You can now write most of the rules by simply clicking and selecting elements on the Rule Builder, which now serves as the central dashboard for defining and editing all rules, irrespective of whether they are out-of-the-box rules or new rules.

The main changes in this release are:

- The differentiation between out-of-the-box rules and new rules has been deprecated. As a result, you can now configure all rules using a single page.
- The Scoring Configuration page has been deprecated. You can configure the scores for the rules by using the Rules and Scoring Management page.
- You can build your own rules using the Rule Builder and add them to a Ruleset. Several new rules can be written using GeoLocation information available in the Rule Builder. Refer to the CA RiskMinder Administration Guide for a list of custom tags that can be used to write a rule.
- The approach to model configuration has now changed.
    - You can configure the URL and connection parameters for the model under the Services and Server Configurations tab.
    - By default, the model is disabled for execution for each organization. The model is an optional custom module. Only Global Administrators (not Organization Administrators) can enable the model for an organization.
    - If the model is enabled for any organization, it will use the configuration done at the global level for evaluating the model score. Rule writers will be able to use the element called "MODEL_SCORE" in the Rule Builder to write a rule based on Model Score.

Other changes include:

- The Rule Builder page now displays a list of all currently configured rules. There is separation of the "Read-only" view and "Edit" mode for each rule.
- To define a new rule, you must first specify Channel, Action, and the Element(s) that the rule will depend on. Only then, you can proceed further.
- The Enable or Disable Execution option is has been removed. The Rule Builder automatically decides if a rule needs to be executed or not. As a rule writer, you only need to specify whether a rule is enabled for scoring or not.
- Changing the scoring priority is now intuitive.
- You can now create multiple instances of all of the out-of-the-box rules, except Exception User Check rule.

- Since the Rule Builder needs the Transaction element to start building a rule, it is very important that the channel be defined carefully. Channel definition is usually a one-time activity in a given deployment.

  Contact CA Support to define your custom channels.

Note: From this release, all reports will display all rule results in one column. This was not the case in the previous releases, where the out-of-the-box rule results were displayed in individual columns, but all Add-On rule results were displayed in one single column as name-value pairs, separated by semicolons (;).

Introduction of Instance Management

RiskMinder now provides a comprehensive screen that you can use to manage the RiskMinder Server instances that you have deployed. Using this Administration Console screen, the Master Administrator (MA) can perform the following instance management operations:

- Refresh cache for all or selected instances.

  Note: The MA can trigger cache refresh for a specified set of organizations or at the system level. The cache refresh is granular. Therefore, if the cache refresh request is issued for an organization, it does not affect the ongoing transactions for other organizations.
- Shut down all or selected instances of RiskMinder Server.
- Shut down all or selected instances of Case Management Queuing Server.
- Configure instance-level configuration parameters, such as log file, log level, trace logging, and database connection pool configuration.
- Fetch detailed statistical information of the instance.

You can still refresh the cache of RiskMinder Server from the command line by using a new tool, arrfclient. See the CA RiskMinder Administration Guide for instructions on using this tool.

There is a new Instance Management Report that lists all Instance Management related activities done by the MA.

The existing functionality of cache refresh of Case Management Queuing Server has changed in this release. Refer to the "Separation of Case Management Queuing Server Cache Refresh and Queue Rebuild" feature.

Enhancements to DeviceDNA

The following are the enhancements to DeviceDNA in this release:

- Integration with Advanced Version of DeviceDNA (see page 15)
- Collection of System Fonts to Generate Risk Profile (see page 15)
- Client Not Dependent on Java Runtime Environment (see page 15)
- Support for Logical Upgrade of DeviceDNA Elements (see page 15)

Integration with Advanced Version of DeviceDNA

RiskMinder now uses DeviceDNA 2.1 to identify devices and score them accordingly. RiskMinder stores DeviceDNA elements in the database with fine granularity, allowing for device analysis in the future.

Collection of System Fonts to Generate Risk Profile

RiskMinder DeviceDNA now collects system fonts installed on the end-user's machine as one of the attributes to generate the risk profile of a device.

Client Not Dependent on Java Runtime Environment

The RiskMinder DeviceDNA client now does not depend on the Java Runtime Environment (JRE) on the end-user's machine to collect any attributes.

Support for Logical Upgrade of DeviceDNA Elements

Logical upgrade is supported for operating system, browser, and Flash.

Support for Device ID Categories

For each transaction, the Device ID is categorized into the following types, based on how the Device ID was acquired:

- NEW: A Device ID is assigned to the device in the following cases:
    - The device is new.
    - The Device ID cannot be determined due to insufficient fingerprint match information.
- READ: The Device ID is read from the device.
- REVERSE LOOKUP: The Device ID is determined by matching the input device signature against the device signatures that were successfully associated with the user.

Introduction of Two New Rules Based on Device ID

Two new rules called Device User Velocity and Device User Maturity have been introduced in this release.

Device User Velocity

The new Device User Velocity rule allows a device to be used by n distinct users in any configured duration. If the device is used by more than n distinct users in the configured duration, then it indicates fraudulent activity.

For example, consider a configuration of 5 transactions per device in 60 minutes. This rule is not triggered when User1 performs five transactions per hour from Device1. But if there are transactions from five different users using Device1 in one hour, then this rule is triggered.

Device User Maturity

The Device User Maturity rule enables setting a level of trust in the device. For example, a User-Device association that has existed for a month, assuming that there has been no fraudulent activity identified for that user or device, should be more trusted than a User-Device association that has been established recently.

Support for Configuration of Reverse Lookup Threshold for Device MFP Match Rule

A new threshold called Reverse Lookup Threshold has been added to the Device Signature Match rule configuration. This threshold is used when the signature match is performed using reverse lookup mechanism.

Support for Identification of Device Types

RiskMinder now identifies the following device types:

- PC
- Apple Macintosh
- Apple iPad
- Apple iPhone
- Apple iPod
- Amazon Kindle
- Google Android
- Linux
- BlackBerry
- BlackBerry PlayBook
- Nokia
- WebOS
- HP Tablet
- Sony
- PlayStation
- Nintendo Wii
- Others

You can write new rules based on the type of the device from where the request originated. The device type for each transaction is displayed in the Risk Evaluation Detail Activity Report and Device Summary Report.

Support for Cross-Channel Information for Risk Evaluation

From this release, RiskMinder supports transaction requests from multiple channels and uses the transaction patterns across these channels to come up with a risk score based on all factors. For example, a home banking login from USA and a 3D-Secure transaction performed from South Africa in quick succession should indicate possible fraud.

Supported channels include:

- Default: For actions or transactions that are initiated through a Web browser. These can originate from either a computer, smart phone, or a tablet.
- 3D-Secure: For online purchase transactions that are protected by the 3D-Secure program for cardholder identification and authentication.

Enhancements to Case Management

The following are the enhancements to case management in this release:

- Support for Multiple Queues (see page 18)
- Separation of Case Management Queuing Server Cache Refresh and Queue Rebuild (see page 19)
- Other Enhancements to Case Management (see page 19)

Support for Multiple Queues

From this release, you can create multiple criteria-based queues for each organization. However, each organization will continue to have a DEFAULT queue, as was the case in previous releases.

The Matched Rule and Risk Advice values of the first transaction of a case decide which case is assigned to a queue. For example, if a case was created due to the Userknown-Alert transaction, then throughout the life of the case, the Queue Criteria will use this value, even if a DENY transaction gets added to the case later.

A transaction with the highest risk score is called the "Riskiest Transaction". Risk Advice and Risk Score of the riskiest transaction in the case decide the overall case Risk Score.This case Risk Score is used to prioritize cases within the Queue. While the case remains assigned to the same queue even if new transactions get added to the case, the priority of the case gets changed if a new transaction with higher score is added to the case.

Before you delete a Queue, it is highly recommended that you edit the Queue definition such that no cases are present in this Queue, refresh the cache, rebuild the Queue, and then delete this queue. This ensures that cases, which were in this queue, are not lost.

With support for multiple queues, you must note that:

- All the cases that do not match any of specified queue definitions are directed to the Default queue.
- If a new case is assigned to a queue, then it continues to remain in the same queue throughout its lifecycle, unless it is manually reassigned to another queue.

Queue Managers must issue a Queue rebuild for the changes to take effect immediately. Else, the changes come into effect when the regular automated Queue rebuild happens (at a default frequency of 30 minutes).

Note: A change in Customer Support Representative (CSR) assignment to Queues still requires a cache refresh.

Separation of Case Management Queuing Server Cache Refresh and Queue Rebuild

In previous releases, every time you performed a cache refresh operation for Case Management Queuing Server, the Case Management queue was also rebuilt. From this release, because of the introduction of the Integrated Cache Refresh feature, the two operations (Server cache refresh and Queue Rebuild) have been decoupled.

Now, you need to refresh the Case Management Queuing Server cache only if:

- The administrator created a new queue.
- The list of administrators associated with one or more queues has changed.

On the other hand, Queue Rebuild (automated or issued by Queue manager) is required when:

- One or more of the queue definitions have changed or a new queue is defined.

Note: The administrators will still need to do both cache refresh as well as queue rebuild, if they want to redistribute cases according to the new set of queues or their definitions.

Other Enhancements to Case Management

In this release, the Case Management user interface has been reworked to accommodate the multi-account and cross-channel features. Customer Support Representatives (CSRs) will now be presented with a unified view of all transactions for a specified user across channels. On the other hand, Fraud Analysts (FAs) will see the transactions for different channels under different tabs. These views are customizable and must be considered when defining a new channel.

In this release, the default set of advices for which a case is generated is ALERT and DENY. In previous releases, the default set of advices for which a case was generated was INCREASE_AUTH and DENY.

CSRs (Inbound Call Handlers) and FAs can search for transactions for a given user by using any user identifier, such as user name or AccountID. In addition, FAs can continue to use the additional filters available in previous releases.

In this release, searching for Related Transactions on the Analyze Transactions page is always associated with a date range. In previous releases, it was possible to search without providing any date range, which might result in performance issues.

Case Management Queuing Server has been enhanced to use either the primary or the backup Case Management Queuing Server while rebuilding a queue.

Support for Additional Software (Application Server and Directory Servers)

RiskMinder now supports the following Application Server and Directory Servers:

- JBoss Application Server
- Oracle Directory Server 11g
- Windows Active Directory 2008
- CA Directory JXweb r12.0

Enhancements to Rule-Writing and Related Capabilities

The following are the enhancements to rule-writing and related capabilities:

- Introduction of New Rule Based on Action Velocity (see page 20)
- Support for Writing New Rules Based on System Time (see page 21)
- Support for Amount Check Rule Using Currency Conversion (see page 21)
- Support for Writing New Rules Based on Transaction Actions (see page 21)
- Improved Performance of List-Based Lookup Rules (see page 21)

Introduction of New Rule Based on Action Velocity

A new rule called Action Velocity Rule has been introduced in this release. This rule enables you to limit the number of transactions by a user for a specific action or a combination of actions in a specified interval of time.

For example, if you specify 5 as the value for the "Greater or Equal To" field, 60 minutes as the value of the "In Last" field, and select the action as "Login", then the rule will trigger if the count of Login transactions in an hour is 5 or more.

This rule differs from other velocity rules in the following ways:

- This rule will trigger if there are 5 transactions in the last 60 minutes with the action set to "Login"; including or excluding the current transaction.
- Other velocity rules kick in when the threshold set is exceeded (>5 in the example above). This rule kicks in when the threshold set is hit (=5 in the example above).

Support for Writing New Rules Based on System Time

You can now write new rules by using the following elements of system information:

- DATE (YYYYMMDD)
- DAYOFMONTH (01-31)
- DAYOFWEEK (MONDAY-SUNDAY)
- MONTH (01-12)
- YEAR (YYYY)
- CURRENTTIME (HHMM)

All these values are in GMT.

Support for Amount Check Rule Using Currency Conversion

From this release, you can define the base currency for each organization, and use this base currency to further define the amount thresholds. Optionally, you can also define the amount thresholds in other currencies.

If the incoming transaction is in base currency, then the amount will be compared according to the amount threshold you set. However, if the incoming transaction is in a different currency, then the amount is compared as follows:

- If you have defined the threshold for that currency, then the amount is compared to the threshold.
- If you have not defined the threshold for that currency, then the incoming amount will be converted to base currency and will be compared with the set threshold.

The Case Management screens also show the amount in base currency and the currency used in that transaction.

Support for Writing New Rules Based on Transaction Actions

You can now write new rules based on the types of transactions (or Transaction Actions) by using the Action element as the base element. The transaction type can be either LOGIN, ENROLLED_PURCHASE, UNENROLLED_PURCHASE, or FORGOT_PWD.

Improved Performance of List-Based Lookup Rules

Performance of the list-based lookup rules has been improved to do a constant time search, irrespective of the list size.

Support for Encryption of Information Stored by RiskMinder

RiskMinder now supports encryption of user name and user accounts. You can choose to encrypt sensitive attributes and also decide whether you want to display clear text data or encrypted data in Reports.

Enhancements to the Administration Console

The following are the enhancements to the Administration Console:

- Support for Additional Administrator Profile Settings (see page 22)
- Support for Separate Password Policy for Master Administrators (see page 23)
- Provision to Temporarily Lock Administrator's Password Credential (see page 23)
- Support for Password History Check (see page 23)
- Support for Configuration of a Different Encryption Key Per Organization (see page 23)
- Support to Re-Create a New User With Deleted User's User Name (see page 23)
- Support to Re-Create a New Administrator With Deleted Administrator's User Name (see page 24)
- Support for Additional Contact Information (see page 24)
- Support to Add Custom Attributes to Users From an LDAP-Based Organization (see page 24)
- Support for Uploading Users and User Account Information in Bulk (see page 24)
- Provision for Setting Miscellaneous Configurations (see page 24)
- Support for Reverse Lookup for Device Identification (see page 25)

Support for Additional Administrator Profile Settings

The 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 Separate Password Policy for Master Administrators

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 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.

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 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 reused.

Support for Configuration of a Different Encryption Key Per Organization

RiskMinder enables you to use hardware- or software-based encryption of your sensitive organization data. While creating organizations, you can choose to override the Global Key Label you specified in the bootstrap process and specify a new key label that will be used for encrypting organization-specific data.

Refer to the CA RiskMinder Administration Guide for information on keys that are used to encrypt the organization data.

Support to Re-Create a New User With Deleted User's User Name

After a user is deleted, all privileges associated with the user are permanently deleted. As a result, the user can no longer log in to your application. Their account information and credentials are also deleted from the database. You can create a new user with the same name as a previously deleted user. But the new user does not automatically assume the privileges of the previously deleted user. If you need to duplicate a deleted user, then you must manually re-create all privileges.

Support to Re-Create a New Administrator With Deleted Administrator’s User Name

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 your application. Their account information and credentials are also deleted from the database. You can create a new administrator with the same name as a previously deleted administrator. But the new administrator does not automatically assume the privileges of the previously deleted administrator. If you need to duplicate a deleted administrator, then you must manually re-create all privileges.

Support for Additional Contact Information

You can now add multiple email addresses and telephone numbers for every user, either at the global level or at the organization level, through the Administration Console.

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

While creating LDAP users, you can provide additional information about the user in the Custom Attributes section on the Create User page.

Support for Uploading Users and User Account Information in Bulk

RiskMinder 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.

Provision for Setting Miscellaneous Configurations

You can use the Miscellaneous Configurations page to configure case management parameters, rule parameters, and any channel-specific parameters. These configurations are expected to be one-time, but can be edited and will be effective after Cache Refresh is performed.

Some of the parameters are configurable at the global level under the Services and Server Configurations tab, while others are configurable at the organization level. By default, each parameter for the organization uses the global-level configuration, but each organization can override any or all such configurations.

Support for Reverse Lookup for Device Identification

In previous releases, reverse lookup was configurable at the system level. Now, using the Miscellaneous Configurations page in the Administration Console, you can configure reverse lookup at the organization level.

Enhancements to RiskMinder Server

The following are the enhancements in the RiskMinder Server:

- Integrated Cache Refresh (see page 25)
- Support for Database Query Timeout (see page 25)
- Provision to Process Ongoing Transactions During Server Shutdown (see page 26)
- Enhanced Quova Upload Tool (see page 26)
- Support for RiskMinder Server to Use One Database Connection Per Transaction (see page 26)

Integrated Cache Refresh

From this release, you can also refresh the cache for all instances of CA Arcot products and their sub-components by using the Refresh Cache page. This functionality is available to the MA, as well as to Global Administrators (GAs) and Organization Administrators (OAs) for the organizations in their scope.

Note: The MA and GAs can also perform the cache refresh operation by using the Refresh Cache page. The difference between refreshing the cache using the Instance Management page and using the Refresh Cache page is that you can select specific instances of RiskMinder Server and Case Management Queuing Server that you want to refresh by using the Instance Management screens. On the other hand, if you refresh the cache using the Refresh Cache page, then all available instances are refreshed.

Support for Database Query Timeout

In this release of RiskMinder, ODBC query timeout has been introduced in the RiskMinder Server and Case Management Queuing Server.

Provision to Process Ongoing Transactions During Server Shutdown

RiskMinder Server has been enhanced to process ongoing transactions even when a server shutdown is initiated. Therefore, when RiskMinder Server receives a shutdown request, all ongoing transactions are processed first, and then the shutdown request is processed.

Enhanced Quova Upload Tool

RiskMinder uses Quova data to identify the geolocation information of a user by using the IP address of the system from which the transaction originated. It then uses this data to evaluate Negative Country, Negative IP, and Zone Hopping rules.

The Quova data upload tool can now be scheduled to automate the upload of both GeoAnonymizer and GeoPoint data feeds from same machine. A new command line option has been added to the tool's usage which helps achieve this.

Support for RiskMinder Server to Use One Database Connection Per Transaction

RiskMinder Server now uses only one database connection while processing a transaction.

Introduction of Accounts

The following are the new Account-related features:

- Support for Multiple Accounts (see page 27)
- Support for Temporarily Deactivating User Account (see page 27)

Support for Multiple Accounts

From this release, in addition to the UserName attribute, users can also be identified by an alternate ID called AccountID. 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. RiskMinder can perform risk evaluation by using either the user account or the UserName.

A user can have one or more accounts in RiskMinder.

The AccountID associated with each user for different account types can be created by using Issuance APIs provided by User Data Service (UDS). A default account can be configured for each organization for each channel (See the “Support for Cross-Channel Information for Risk Evaluation” feature.) See the RiskMinder Java SDK and WSDL docs and the UDS WSDL docs for more details on how to integrate your application to use this feature.

Note: RiskMinder Sample Application demonstrates risk evaluation integration using Java SDK. The Issuance Java SDK shipped with previous releases of RiskMinder has been deprecated. You can configure the organization for "Implicit User Enrollment" to demonstrate user enrollment with or without accounts.

Support for Temporarily Deactivating User Account

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.

Enhancements to Reporting

The following are the enhancements to the reporting feature:

- Support for Exporting Administrator Reports Before Viewing (see page 27)
- Introduction of New Report Download Tool (see page 28)
- Introduction of New Device Summary Report (see page 28)

Support for Exporting Administrator Reports Before Viewing

The Administration Console provides the ability to export reports to a file. By exporting a report, you can save a local copy of the report, which enables you to track trends. You can also work with the saved report data in another application.

Introduction of 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.

Introduction of New Device Summary Report

A new report called Device Summary Report has been introduced in this release. This report displays the total number of transactions by device type and the method by which the Device ID was determined.

Enhancements to RiskMinder APIs

The following are the enhancements to RiskMinder APIs:

- Response Codes and Reason Codes (see page 28)
- Null Machine FingerPrint (see page 28)

Response Codes and Reason Codes

All RiskMinder APIs now return response codes and reason codes. For detailed information on response codes and reason codes, see the CA RiskMinder Java Developer's Guide.

Null Machine FingerPrint (MFP) and IP Address Values Allowed

RiskMinder is now enhanced to allow null values in the MFP and IP Address fields in case a channel does not have values for the same.

Enhancements to RiskMinder Web Services

The following are the enhancements to RiskMinder Web Services:

- Support for Authentication and Authorization for Risk Evaluation Web Services (see page 29)
- Support to Expose Organization Management Features Through Web Services (see page 29)

Support for Authentication and Authorization for Risk Evaluation Web Services

Starting with this release, all Risk Evaluation Web services calls are protected from rogue requests through authentication and authorization. As a result, all requests to the Risk Evaluation Web services are authenticated for valid credentials after which all requests are then validated for appropriate privileges to access the Web services.

Support to Expose Organization Management Features Through Web Services

In this release, support has been added to expose various organization management features through the Web services interface from the User Data Service component.

Logging Enhancements

The following are the logging enhancements in this release:

- The Master Administrator can now change log levels without restarting the RiskMinder Server and Case Management Server.
- RiskMinder Java SDK now logs additional information for easy correlation with the RiskMinder Server log files.
- RiskMinder now logs information in a concise manner at the INFO level to gather sufficient information about a transaction.
- New Startup Log Files:

  Because RiskMinder comprises two server modules, RiskMinder Server and Case Management Queuing Server, two new startup log files have been introduced:

  - arcotriskfortstartup.log: When you start the RiskMinder Server, it records all startup (or boot) actions in this file. The information in this file is very useful in identifying the source of the problems if the RiskMinder service does not start up.
  - arcotriskfortcasemgmtstartup.log: When you start the RiskMinder Case Management Queuing Server, it records all startup (or boot) actions in this file. The information in this file is very useful in identifying the source of the problems if the Case Management Queuing service does not start up.
- For all organizations, RiskMinder Server now logs active Rulesets and parameters of all the rules belonging to a particular Ruleset during server startup and refresh.
- Logging at the DETAIL level has been reduced significantly to reduce disk space requirements in case the servers need to be run at the DETAIL logging level.
- A new log level called Trace has been added in RiskMinder Server and Case Management Queuing Server components.

  This log level is useful in production systems to gather vital information to investigate complex issues.
- RiskMinder Server now performs audit logging after a response is returned.
- Logging has been enhanced on the Case Management page to help with database query performance tuning.

Chapter 3: Changed Features

This section contains the following topics:

New Rules to Replace Four Existing Rules (see page 31)
Location of Case Management Reports (see page 32)
Deprecated Features (see page 32)

New Rules to Replace Four Existing Rules

Four of the predefined rules have been deprecated in this release. Alternative rules have been introduced for these deprecated rules. The following table lists the deprecated and new rules and rule mnemonics:

Deprecated Rule Name and Rule Mnemonic	**New Rule Name and Rule Mnemonic**
DeviceID Known (DEVICEIDCHECK)	Unknown DeviceID (UNKNOWNDEVICEID)
Device MFP Match (SIGMATCH)	Device MFP Not Match (MFPMISMATCH)
User Associated with DeviceID (USERDEVICEASSOCIATED)	User Not Associated with DeviceID (USERDEVICENOTASSOCIATED)
User Known (USERKNOWN)	Unknown User (UNKNOWNUSER)

Important! Although these rules have been deprecated, they are still available and can be used after you upgrade to release 3.1. However, it is recommended that you replace each deprecated rule with the corresponding new rule by making the required changes in the rule expression.

For any of the four deprecated rules, if the rule evaluates to No, then the rule is considered to have matched. It is then used for scoring. In contrast, each of the other predefined rules are considered to have matched when they evaluate to Yes.

In each of the four new rules introduced in release 3.1, if the rule evaluates to Yes, then the rule is considered to have matched. In this way, the four new rules are consistent with the other predefined rules.

Location of Case Management Reports

In the Administration Console, all the Case Management reports are now available on the Reports tab.

Deprecated Features

The following features have been deprecated in this release:

- The ability to create a new ruleset by referring to another ruleset.
- The ability to edit rule configurations to refer to another ruleset.
- The ability to edit a rule to copy from another ruleset.
- The ability to create an add-on rule type by importing an XML file through the Administration Console.
- RiskFort Issuance APIs and Web Services. Both Java SDK and Web Service have been deprecated. Instead, a new Web Service that is directly exposed by UDS is now available. This change was done because UDS provides a much broader list of Web Services for user management. For details, refer to the WSDL document available with the release.
- Older DeviceDNA client collection APIs. You must use the new DeviceDNA client with the new set of APIs.

Chapter 4: Known Issues

This section contains the following topics:

Documentation Not Available for One-Way SSL Communication Between RiskMinder Components and Database Servers (see page 33)
Cannot Use Administration Console to Delete Information About Users Deleted from LDAP Organization (see page 34)
Localization Configuration Not Supported for Date and Time Input Values (see page 34)
Bulk Upload of User Accounts Does Not Accept a Range of Values for the Account Status (see page 34)
Uninstallation Must Be Performed in Reverse Order (see page 34)
Administrators Allowed to Create an Organization Called SYSTEM (see page 35)
Multi-Byte Characters Supported for List Name and Category Mapping Name (see page 35)
Implicit User Creation Successful if Email is the Only Mandatory Parameter (see page 35)
Cache Refresh Fails After Database Failover (see page 35)
Administration Console Not Connecting to RiskMinder Server During Database Failover (see page 35)
Issue with Reverse Lookup Functionality (see page 35)
Risk Evaluation with Empty MFP Value Fails in Sample Application 2.0 (see page 36)
Administration Console Not Displayed Correctly After Upgrading to Internet Explorer 9.0 (see page 36)
Registry Entries are Not Removed After Uninstallation (see page 36)
Log File Location Displayed on Installer Screen is Not Intuitive (see page 37)
Null Pointer Exception is Logged When arcotcommon.ini is Missing (see page 37)

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

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

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.

Localization Configuration Not Supported for Date and Time Input Values

Localization configuration is not supported for date and time input values. The default locale is en_US.

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

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]

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 RiskMinder Server followed by Administration Console, then you have to first uninstall Administration Console, and then uninstall RiskMinder Server.

Administrators Allowed to Create an Organization Called SYSTEM

RiskMinder allows administrators to create an organization with the name SYSTEM. Such an organization inherits all configurations of the global RiskMinder organization of the same name.

Multi-Byte Characters Supported for List Name and Category Mapping Name

The List name and Category Mapping name must not accept multi-byte characters, but they accept them in this release.

Implicit User Creation Successful if Email is the Only Mandatory Parameter

Implicit user creation fails when any parameter other than email is set as mandatory for an organization.

Cache Refresh Fails After Database Failover

Performing a cache refresh after a database failover has occurred results in an error.

Administration Console Not Connecting to RiskMinder Server During Database Failover

The Administration Console is not able to connect to the RiskMinder Server during database failover.

Issue with Reverse Lookup Functionality

Reverse lookup functionality does not work if the MFPMISMATCH rule is included as an add-on rule.

Risk Evaluation with Empty MFP Value Fails in Sample Application 2.0

If you have deployed sample application 2.0 with RiskMinder 3.1, and if you remove the existing MFP value for a user and try to evaluate risk for that user, evaluation fails.

Administration Console Not Displayed Correctly After Upgrading to Internet Explorer 9.0

Symptom:

After you upgrade to Internet Explorer 9.0, the Administration Console is not displayed correctly.

Solution:

Restore the Internet Explorer 9.0 settings by navigating to **Internet Options**, **Advanced**, and then click **Restore advanced settings**.

Registry Entries are Not Removed After Uninstallation

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 Displayed on Installer Screen 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.

Chapter 5: Defects Fixed

This section contains the following topics:

Default Ruleset Not Created for an Organization That Was Created When RiskMinder was Down (see page 39)
Refreshing RiskMinder Resulted in Performance Issues (see page 39)
RiskMinder Occasionally Unable to Switch to Backup Database (see page 40)
Rule Mnemonic Length was Not Restricted to 25 Characters (see page 40)
Two Levels of Cache Refresh Required After Updating Default Organization Configuration (see page 40)
Filtering By Rule When Analyzing Transactions in Case Management Did Not Work for Microsoft SQL Server (see page 41)
Organizations Created Before RiskMinder Deployment Not Read by RiskMinder (see page 41)
Incoming Transactions Processed Even When the Server was Stopped (see page 41)

Default Ruleset Not Created for an Organization That Was Created When RiskMinder was Down

Symptom:

If an organization was created when the RiskMinder Server was down, no default ruleset could be created for that organization.

Solution:

In this release, all organization-related information is stored in User Data Service (UDS). Therefore, even if you created an organization (by using the Administration Console) while the Server was down, you can still create ruleset(s) for this organization after restarting RiskMinder server.

Refreshing RiskMinder Resulted in Performance Issues

Symptom:

Refreshing the RiskMinder Server cache resulted in slowing down of ongoing operations.

Solution:

The issue has now been resolved, such that the impact of cache refresh is minimal on ongoing transactions.

RiskMinder Occasionally Unable to Switch to Backup Database

Symptom:

At the time of Server startup, if the connection to the primary database failed, RiskMinder, on occasions, was unable to switch to the backup database.

Solution:

The issue has now been resolved.

Rule Mnemonic Length was Not Restricted to 25 Characters

Symptom:

The rule mnemonic length was not restricted to 25 characters.

Solution:

The rule mnemonic length is now restricted to 25 characters. Existing rule mnemonics will be migrated even if they have longer mnemonics. However, it is strongly recommended that you delete the rules and create new rules with rule mnemonics having less than 25 characters.

Two Levels of Cache Refresh Required After Updating Default Organization Configuration

Symptom:

Two levels of cache refresh were required to change the Default Organization configuration.

Solution:

In this release, changing the Default Organization configuration requires only one system-level cache refresh.

Filtering By Rule When Analyzing Transactions in Case Management Did Not Work for Microsoft SQL Server

Symptom:

In the Analyze Transactions screen in Case Management, filtering transactions by Rule does not work for MS SQL Server.

Solution:

This issue has now been resolved.

Organizations Created Before RiskMinder Deployment Not Read by RiskMinder

Symptom:

If you installed AuthMinder and then RiskMinder, and if an organization was created before the RiskMinder instance was deployed, then that organization was not read by RiskMinder after the deployment.

Solution:

This issue has now been resolved. Organizations created prior to RiskMinder deployment are now read by the RiskMinder instance after deployment.

Incoming Transactions Processed Even When the Server was Stopped

Symptom:

Incoming transactions continued to be processed simultaneously even if the RiskMinder Server was stopped. This resulted in the server going into an unwanted state.

Solution:

This issue has now been resolved.

Chapter 6: Product Limitations

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

- On IBM WebSphere, using certain multi-byte characters in the name and description of add-on rules results in all the base rules being removed.
- If the network cable for the primary database is unplugged, then the RiskMinder or Case Management Server and the Administration Console take a long time to connect to the backup database.
- Migration of a custom add-on rule type created in a release prior to 3.x is not supported during an upgrade to 3.1 using the default upgrade script. Migrating such rules requires an upgrade script to be written separately. Contact CA Support for more information.
- 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 RiskMinder on the same system in different folders. If you try to install multiple instances, then the installation is not completed successfully.