

CA Risk Analytics® - 5.2 Administering

Date: 31-Dec-2014

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Table of Contents

Getting Started with the Administration Console	13
About the Administration Console	13
Elements of Administration Console	14
Supported Roles	15
Users	15
Administrative Roles	15
What is the Scope of an Administrative Role	17
Important Notes About Scope	17
Master Administrator	17
Global Administrator	18
Organization Administrator	19
User Administrator	20
What are Custom Roles	20
Summary of Administrative Privileges	21
How to Access the Administration Console	25
How to Change Password and Profile Information	26
Security Recommendations While Using Administration Console	27
 Quick Administration	 28
For Simple Deployments	28
For Complex Deployments	29
 Configuring Administration Console Settings	 31
How to Create a Global Administrator Account	31
How to Specify Basic Authentication Policy Settings	32
How to Configure the Master Administrator Authentication Policy	34
How to Change the Default Organization	35
How to Update UDS Configurations	36
How to Change the Default UDS Connectivity Configuration	36
How to Change the Default UDS Parameters	38
How to Refresh the Cache	40
How to Refresh the Administration Console Cache	41
How to View the Status of Cache Refresh Requests	41
How to Configure Custom Locales	43
How to Configure Attribute Encryption	44

How to Configure Web Services Authentication and Authorization	45
Other Miscellaneous Optional Tasks	45
How to Configure Account Types	45
How to Configure Email and Telephone Types	48

Working with Custom Roles 50

Understanding Custom Roles	50
Things That You Should Know About Custom Roles	50
Pre-Defined Custom Roles	51
How to Create a Custom Role	51
How to Update a Custom Role Information	52
How to Delete a Custom Role	53

Managing Server Instances 54

How to Configure Server Connectivity	54
For Transaction Server Management	55
For Case Management Server Management	56
For Risk Analytics Administration	57
For Case Management Server	58
How to Create Trust Stores	59
How to Configure Communication Protocols for Server Instances	60
Configuring SSL Communication	64
How to Refresh a Server Instance	65
By Using Administration Console	65
By Using the arrfclient Tool	66
How to Update Server Instance Configurations	67
How to Shut Down a Server Instance	69
How to Restart a Server Instance	69

Managing Model and Other Server Configurations 71

How to Update the Risk Analytics Predictive Model	71
How to Configure the Default Card Issuer Organization	73
How to Configure the Default Transaction Acquirer Organization	74
How to Configure Default NBIN Mapping	74

Managing Global Configurations 76

How to Configure Global Settings	76
How to Configure Organization-Level Settings	77

Managing Organizations	77
How to Create and Activate an Organization	78
How to Create an Organization in Arcot Repository	78
How to Create an Organization in LDAP Repository	82
How to Create an Org Family	88
How to Search for an Organization	88
How to Update an Organization	88
For Basic Organization Configurations	89
For Risk Analytics-Specific Configurations	90
How to Upload Users and User Accounts in Bulk to an Organization	91
How to View the Status of the Bulk Data Upload Request	94
How to Refresh the Organization Cache	95
How to Deactivate an Organization	95
How to Activate an Organization	96
How to Activate an Organization that is in Initial State	96
How to Delete an Organization	97
Managing Administrators	98
How to Create an Administrator	98
How to Change Profile Information for an Administrator	100
How to Search for an Administrator	101
How to Update Administrator Information	102
How to Demote an Administrator to User Role	103
How to Configure Account IDs for Administrators	103
How to Create Account IDs	104
How to Update Account IDs	104
How to Delete Account IDs	105
How to Deactivate an Administrator Account	105
How to Temporarily Deactivate an Administrator	106
How to Activate an Administrator Account	107
How to Delete an Administrator Account	107
Working with Models	108
How the Rule Engine Uses Model	109
How to Configure Predictive Model Parameters	110
How to Enable the Predictive Model for an Organization	112
How to Configure DSP Model for Organizations with no Existing Models	114
Step 1 How to Create Organization-Level Model Configuration	114
Step 2 How to Set the Model as the Referenced Model	115
Step 3 How to Enable the Model	116
How to Configure DSP Model for Organizations with Existing Models	116
Step 1 How to Create an Organization-Level Model Configuration	117
Step 2 How to Enable the DSP Model as the Secondary Model to Initiate Priming	119
Step 3 How to Switch Over from the GDP Model to DSP Model for Use in Rules	119
Step 4 How to Remove the GDP Model	121
When Is Roll Back from DSP to GDP Model Possible	121
Step 5 How to Display the DSP Model Score in UI and Reports	122

How to Validate DSP Model Configuration	122
How to Validate the Model Configuration at Organization-Level	123
How to Validate the Model State at Ruleset-Level	124
Error Codes When RA is Configured to Use DSP Model	125
Configuring RA Properties and Related Configurations	125
How to Configure Channels and Accounts Associations	126
How to Configure a Card Issuer	128
How to Delete the Card Issuer Mapping	130
How to Configure the NBIN Mapping	130
How to Delete the NBIN Mapping	131
How to Configure the Transaction Acquirer	131
How to Delete the Transaction Acquirer Mapping	132
How to Configure Miscellaneous Risk Analytics Properties at the Organization Level	132
How to Configure Miscellaneous Risk Analytics Properties at the System Level	135
How to Upload Compromised Card Information	136
Configuring RA Callouts	136
What are Callouts and How they Work	137
What Different Types of Callouts are Available	137
How are Callouts Implemented	139
How to Configure an Evaluation Callout	140
How to Configure a Scoring Callout	141
How to Work with the Sample Callout	143
How to Deploy the Sample Callout	143
How to Configure the Transaction Server to Communicate with Sample Callout	144
Managing Users	145
How to Create a User	146
How to Search for Users	146
How to Update User Information	147
How to Promote a User to Administrator	148
How to Configure Account IDs for Users	149
How to Create Account IDs	150
How to Update Account IDs	150
How to Delete Account IDs	151
How to Deactivate a User Account	151
How to Temporarily Deactivate a User Account	152
How to Activate a User Account	153
How to Delete a User Account	153
Managing Rules	155
Understanding the Building Blocks of Rules	155
Basic Rule Concepts	155
What Are Rules	155
Characteristics of a Rule	156
Types of Rules Supported in RA	156

Out-of-the-Box Rules	156
Configurable Predefined Rules	156
Non-Configurable Predefined Rules	159
Custom Rules	160
Custom Rules Built Using Rule Builder	160
Custom Evaluations Built Using Callouts	161
What are Evaluation Callouts	161
How Evaluation Callouts Work	161
What are Scoring Callouts	162
How Scoring Callouts Work	162
How Are Callouts Implemented	163
What are Rulesets	164
What Are Channels	164
What Is Predictive Model	166
What Is Rules Engine	166
What Is Scoring Engine	167
What Is Rule Priority	167
How Does Risk Score Work	167
What Does Risk Advice Mean	168
How Does Rule Engine Work	169
How Are Rules Triggered	169
How Rule Engine Uses Model to Calculate Model Score	170
How Rules Engine Uses Rules to Calculate a Risk Score and Advice	171
State Diagrams	171
States of Rules	171
States of Rulesets	172
Understanding the Data RA Uses	172
How Is Geolocation Information Derived from IP Address Used	173
How Is Geolocation Data Derived from Address Used	174
How Is Geolocation Data Derived from Anonymizers Used	175
How Is Zone Hopping Information Used	175
How Is Negative IP Address List Used	176
How Is Device Identification Data Used	176
How Is Device User Association Data Used	178
How Is User Information Used	178
How Is Transaction Information Used	179
How Is Case Management Information Used	179
How Is Model Information Used	180
How Is Currency Conversion Used	180
Understanding RA Predictive Model	181
How the Rule Engine Uses the Predictive Model	181
Error Codes When RA Is Configured to Use DSP Model	182
Working with Rulesets	183
How Do Rulesets Work	183
How to Create a Ruleset	183

How to Create a Ruleset at the Global Level	184
How to Create a Ruleset at the Organization Level	184
How to Clone a Ruleset	185
How to Clone from SYSTEM Ruleset	185
How to Clone an Existing Ruleset	187
How to Assign a Ruleset to an Organization	188
How to Edit a Ruleset	189
How to Migrate a Ruleset to Production	190
How to Migrate a Ruleset to Production at the Global Level	190
How to Migrate a Ruleset to Production at the Organization Level	191
Working with Out-of-the-Box Rules	192
What are Out-of-the-Box Rules	192
How to Create and Deploy Out-of-the-Box Rules	192
How to Create a Device-Based Rule	193
How to Configure the Out-of-Box Device User Velocity Rule	194
How to Configure Organizations for Device Velocity Rules with Scope as Org Family ..	195
How to Configure the Out-of-Box Device User Maturity Rule	196
I Have Configured My Rule, Now What	197
How to Upload Rule List Data	198
For Negative Country List	199
For Untrusted IP Addresses	200
For Trusted IP Addresses	201
For Trusted Aggregators	203
For Simple Lists	206
For Category Mapping Lists	207
How to Create a List	208
How to Edit a List	209
How to Activate a Rule (Migrate Rules to Production)	210
How to Refresh Server Cache	211
How to Refresh Server Cache at System Level	211
How to Refresh Server Cache at Organization Level	212
How to Edit Rule Definitions	212
Editing Untrusted IP Types	213
Editing User Velocity	214
Editing Device Velocity	215
Editing Zone Hopping	217
Editing Machine FingerPrint (MFP) Match Percentage	218
How to Delete a Rule	219
Creating Custom Rules by Using Rule Builder	220
What are Data Elements	220
What are Rule Tags	221
What are Operators	223
What are Multi-Byte Character and Encrypted Parameters	224
Examples of Using New Rules	226
How to Create a Custom Rule	229

After Creating a Custom Rule, What Next	230
What Else Can I Do with My Custom Rule	231
Understanding Data Elements	232
Quick Overview of Data Elements	232
Transaction Elements	234
Transaction Elements for the Default Channel	234
Transaction Elements for 3D Secure Channel	240
Transaction Elements for ATM and POS Channels	246
Transaction Elements for IMPS Channel	261
Transaction Elements for ECOM Channel	266
Device Elements	267
Geolocation Elements	271
Geolocation Elements (Applicable to All Channels)	271
Geolocation Elements for PINCode-Based Zone Hopping for POS Channels	276
Predictive Model Elements	279
Custom Elements	280
History Rule Elements for ATM and POS	282
Understanding the Types of Operators Used by the Rule Builder	285
Generic Operators	285
Operators Specific to ATM and POS Channels	286
History-Based Operators	287
Using Geolocation and Anonymizer Data in Rules	290
What Is Geolocation Data	291
How to Use Geolocation Data in Rules	292
Negative Country Check	292
Zone Hopping Check	292
IP Routing Type	293
Connection Type	294
Line Speed	295
Region	295
Continent	295
Using Anonymizer Data	296
How to Use the Negative IP Address List	297
Understanding Currency Conversion	297
How Currency Conversion Works	297
Currency Conversion Table	297
Guidelines for Using the ARRFCURRCONVRATES Table	298
Managing Cases	299
Understanding Case Management	299
What Is a Case	299
What Are the Different States a Case can Undergo	300
New	300

Open	301
In Progress	301
On Hold	301
Expired	301
Closed	301
What Is Case Management	302
What Are the Components of Case Management	302
Case Queues	303
Queue Server	304
Queue Monitor Thread	305
Case Dispatcher Module	305
Expiry Monitor Thread	306
Supported Case Management Roles that You Will Use	306
Customer Service Representatives (CSRs)	307
Working on Cases	307
Handling Customer Calls	308
Queue Managers	308
Fraud Analysts	309
Summary of Case Management Role Privileges	309
Supported Case Management Workflows	310
Case Generation	310
Case Queuing	311
Case Assignment	311
Case Handling	311
Case Expiry	312
Case Escalation	312
Fraud Analysis	312
Working with Case Queues	313
How to Create a Queue	313
How to View Queue Status	315
How to Update Queue Status	316
How to Rebuild a Queue	318
How to Disable a Queue	319
How to Enable a Queue	320
How to Delete a Queue	320
Searching for Cases	321
How to Search for Cases Using Search Criteria	322
How to Search for Cases Using Case ID	323
What Are the Cases Summary Page Fields	323
Customer Support Representatives Handling Cases	324
How to Work on Cases	324
How to Manage Inbound Customer Calls	330
How to Add a User to the Exception User List	330
How to Blacklist a Device	332
Fraud Analysts Analyzing Transactions	333

How to View Transactions Summary	333
How to Search for Transactions Based on Search Criteria	334
How to Search for Transactions Based on Transaction ID	335
What Are the Fields in the Transaction Summary Page	336
How to View Case Details	342
How to View Similar Transactions	350
How to View Related Transactions	350
How to Mark Transactions for Further Investigation	351

Managing Reports 352

Summary of Reports Available to All Administrators	352
Administrator Reports	354
My Activity Report	354
Administrator Activity Report	356
User Activity Report	356
User Creation Report	357
Organization Report	358
Risk Analytics Reports	359
Risk Evaluation Detail Activity Report	359
Risk Advice Summary Report	362
Exception User Report	363
Rule Configurations Report	363
Rules Data Report	364
Device Summary Report	364
Case Management Reports	365
Case Activity Report	367
Average Case Life Report	367
Fraud Statistics Report	368
Rule Effectiveness Report	369
False Positives Report	370
Reviewer Efficiency Report (Case Status)	370
Reviewer Efficiency Report (Fraud Status)	371
Rule Effectiveness (Fraud) Report	371
Generating Reports	372
Notes for Generating Reports	372
How to Generate Reports	373
How to Export Reports	374
How to Use the Report Download Tool to Export Reports	374
Using the Tool	374
List of Report Identifiers	377
List of Report URLs	377
Examples of Using the Tool	377

Administrating

The following topics in this section describe how to use the Administration Console to configure CA Risk Analytics:

- [Getting Started with the Administration Console](#)
- [Quick Administration](#)
- [Configuring Administration Console Settings](#)
- [Working with Custom Roles](#)
- [Managing Server Instances](#)
- [Managing Model and Other Server Configurations](#)
- [Managing Global Configurations](#)
- [Managing Rules](#)
- [Managing Cases](#)
- [Managing Reports](#)

Getting Started with the Administration Console

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

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

This article provides information for setting up and managing CA Risk Analytics (referred to as RA later in the section) by using the Administration Console. It introduces you to the Administration Console interface and the supported administrator hierarchy. It covers the following topics:

- [About the Administration Console](#)
- [Elements of Administration Console](#)
- [Supported Roles](#)
- [What are Custom Roles](#)
- [Summary of Administrative Privileges](#)
- [How to Access the Administration Console](#)
- [How to Change Password and Profile Information](#)
- [Security Recommendations While Using Administration Console](#)

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

About the Administration Console

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

You can use the Administration Console to manage the Case Management server, work with cases, assign case roles, and complete other administrative operations and configuration tasks in your purview, such as:

- Manage case administrators
- Manage cases

- Manage case queues
- Generate reports

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

Elements of Administration Console

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

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

The following table describes the elements of the Administration Console.

Element	Description
Header	<p>Displays the login information (administrator name, current organization, the last login date, and time).</p> <p>You can use the links in the header to:</p> <ul style="list-style-type: none"> ▪ Change the administrator profile information (name, phone number, email ID), current password, Date Time format, Locale, and Time Zone. You can also specify the organization that you want to use as a preferred organization for all tasks that you might perform in future. ▪ Log out from the Administration Console.
Main Menu	Displays the main configuration and management options available to the current administrator.
Sub Menu	Displays the options available for the Main Menu item that you clicked.
Tasks	Displays the tasks available for the Sub Menu item that you clicked.
Body	Displays the corresponding page for the selected task.

Console Messages

All the information, warning, and error messages that are generated in the course of using the Administration Console are displayed under the Title area of the body page.

While the error messages are displayed in red, the messages indicating success are displayed in blue.

Supported Roles

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

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

The Administration Console supports the following types of roles:

- [Users](#)
- [Administrative Roles](#)
- [Custom Roles](#)

Users

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

If the user already exists in your LDAP system, then an administrator needs to map the LDAP attributes to Arcot supported attributes. To enroll the users in the RA database, the administrator must select the organization whose repository type is Arcot Database.

In RA, only the administrators who are assigned User Administrator role can work with users. Other administrators (Master Administrator, Global Administrator, or Organization Administrator) do not work with end users.

Administrative Roles

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

Note: See [Summary of Administrative Privileges](#) for a comprehensive list of privileges available.

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

- [Master Administrator](#)
- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

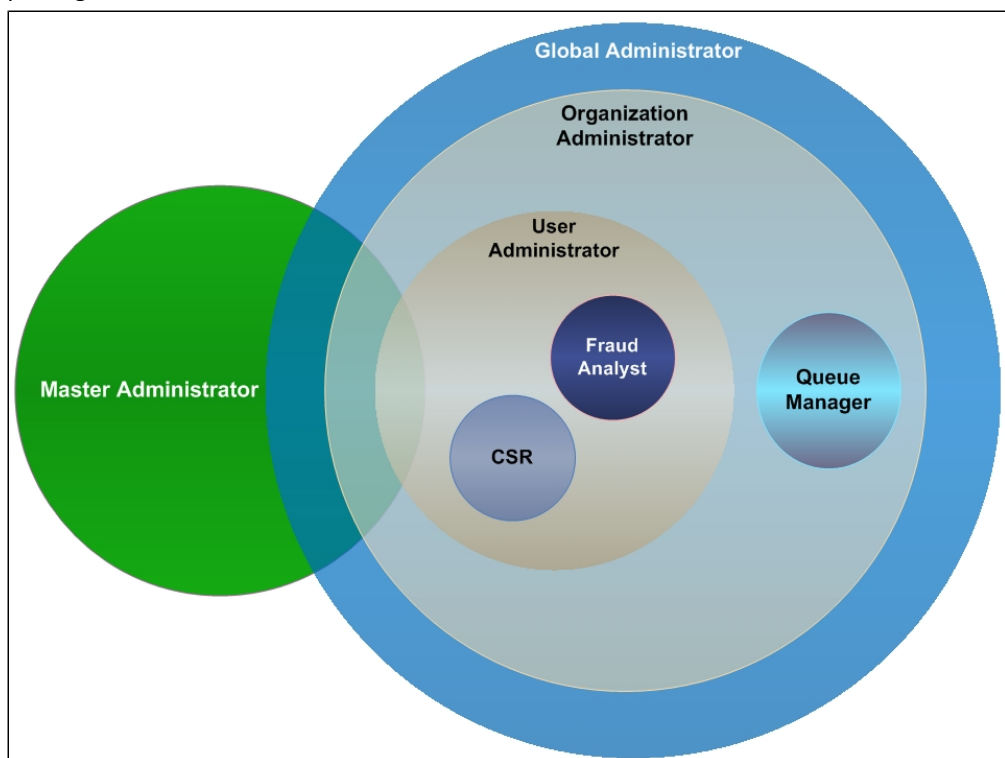
In addition, you can also create custom roles. RA is shipped with three pre-defined custom roles that are required for Case Management:

- Queue Manager
- Customer Support Representative
- Fraud Analyst

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

The following figure depicts these administrative roles and the relationships between the privileges available to these roles. The topics following the figure discuss the supported administrator levels in details.

As can be seen in the figure, the hierarchical distribution of privileges does not allow the administrators to access features beyond their fixed boundaries. Each level has a pre-defined privilege or role.



What is the Scope of an Administrative Role

The *scope* of an administrative role in RA consists of:

All the organizations that an administrator with a specific role can manage.

The privileges associated with the role.

Important Notes About Scope

While creating an administrative role, you must remember that:

- The scope of the Master Administrator is All Organizations, and this administrator manages *all* existing and other organizations that will be created in the future.
- A role (Global Administrator, Organization Administrator, or User Administrator) can manage their peers and the roles with lesser privileges, provided they have scope on the organization to which the administrators belong to.

For example, a Global Administrator can manage other Global Administrators, Organization Administrators and User Administrators. However, they *cannot* manage a Master Administrator.

- The scope of a Global Administrator role *can* be defined as All Organizations, in which case the administrator can manage all existing as well as future organizations.
- An Organization Administrator or a User Administrator role can be limited to manage only specific organizations.

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

Master Administrator

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

The primary responsibilities of an MA are to:

- Bootstrap (or initialize) the system after installation.
- Configure the User Data Service (UDS) connection parameters.
- Configure the global settings for organizations and cache refresh settings for the Administration Console.
- Configure custom locales.
- Set the Default Organization.
- Configure attributes for encryption.

- Configure account types and email and telephone types.
- Enable authentication and authorization for Web services.
- Configure the Transaction Server communication parameters.
- Configure and manage Transaction Server and Case Management Server instances.
- Configure the Transaction Server protocol settings.
- Configure the default Card Issuer organization.
- Configure the default Transaction Acquirer organization.
- Configure the authentication mechanism for the Administration Console, Server components, and other miscellaneous settings.
- Create and manage organizations, if required.
- Create and manage administrators of any role (Global, Organization, or User Administrator), as required.
- Manage [Custom Roles](#).

At the end of a successful deployment of Administration Console, you must log in for the first time as an MA. A default password (master1234!) is assigned to the MA account (masteradmin). Because the actions of an MA can affect the security of the entire system, you must change this password after you log in to the console for the first time. You must also safeguard this password and change it regularly.

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

Global Administrator

The Global Administrator (GA) is the second level in the administrative hierarchy. These administrators can perform most of the tasks of an MA, except for the following:

- Bootstrapping the system
- Performing initial Administration Console configurations
- Setting the Default Organization
- Configuring custom locales
- Enabling authentication and authorization for Web services
- Configuring global attribute encryption set
- Configuring global email and telephone types
- Specifying server configurations

- Managing custom roles

The main tasks of a GA are to:

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

Note: This includes editing the organization details.

- Create and manage users, as required.
- Configure global rules and scoring.
- Assign configurations.
- Configure Callouts.

To track and analyze the available information, GAs can generate and view all administrative activities, configuration, and case management reports for the organizations under their administrative purview. They can also view the reports for all the users and Organization Administrators (OAs) and User Administrators (UAs) assigned to them.

Organization Administrator

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

The main tasks of an OA are to:

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

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

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

User Administrator

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

- Create and manage users.
- Manage end user cases.

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

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

What are Custom Roles

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

- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

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

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

In addition to the custom roles that you can create, RA is also shipped with three pre-defined custom roles that are required for Case Management. These roles include:

- Queue Manager (QM): The QM role has the required privileges to supervise cases.
- Customer Support Representative (CSR): The CSR role has the required privileges to work on cases and attend inbound calls from the end users, if required.
- Fraud Analyst (FA): The FA role has the required privileges to analyze cases to find hidden trends and patterns.

See [Working with Custom Roles](#) for more information about working with these custom roles. See [Managing Cases](#) for more information about Case Management roles.

Summary of Administrative Privileges

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

The column name acronyms used in the table are:

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

Privilege	GA	OA	UA
-----------	----	----	----

Organization Management Privileges

See [Managing Organizations](#) for more information about the tasks related to these privileges.

Create Organization	Y	N	N
Update Organization	Y	Y	N
Update Organization Status	Y	Y	N
List Organizations	Y	Y	Y
Retrieve Default Organization	Y	Y	Y
Delete Organization	Y	Y	N
Decrypt Sensitive Information	Y	Y	Y

Account Type Management Privileges

See "How to Configure Account Types" for more information about the tasks related to these privileges.

Create Account Type	Y	X	X
Update Account Type	Y	Y	X
Delete Account Type	Y	X	X

Administrator Management Privileges

See [Managing Administrators](#) for more information about the tasks related to these privileges.

Create Administrator	Y	Y	N
Update Administrator	Y	Y	Y
Delete Administrator	Y	Y	N

User Management Privileges

See [Managing Users](#) for more information about the tasks related to these privileges.

Create User	Y	Y	Y
-------------	---	---	---

Update User	Y	Y	Y
Update User Status	Y	Y	Y
List Users	Y	Y	Y
List Users for Account	Y	Y	Y
Get User Status	Y	Y	Y
Set User Custom Attributes	Y	Y	Y
Search Users	Y	Y	Y
Get User Profile	Y	Y	Y
Get User Details	Y	Y	Y
Get PAM	Y	Y	Y
Set PAM	Y	Y	Y
Delete User	Y	Y	Y
User Account Management Privileges			
Create User Account	Y	Y	Y
Update User Account	Y	Y	Y
List User Accounts	Y	Y	Y
Retrieve User Account	Y	Y	Y
Delete User Account	Y	Y	Y
Cache Management Privileges			
Refresh System Cache	Y	N	N
Refresh Organization Cache	Y	Y	N
View Global Cache Refresh Requests	Y	N	N
View Organizational Cache Refresh Requests	Y	Y	N
Email and Telephone Type Privileges			
Add Email/Telephone Types	Y	Y	N
Update Email/Telephone Types	Y	Y	N
List Email Types	Y	Y	Y
List Telephone Types	Y	Y	Y
Basic Authentication Privileges			
Update Global Basic Authentication Policy	Y	N	N
Update Organization Basic Authentication Policy	Y	Y	N

Privilege	GA	OA	UA
Encryption Privileges			
Configure the Encryption Set Selected at the Organization Level	Y	Y	N
List Configured Attributes for Encryption	Y	Y	N
Case Management Privileges			
See Managing Cases for more information about the tasks related to these privileges.			
Acquire Case	Y	Y	Y
Acquire Next Case	Y	Y	Y
Get Case Details	Y	Y	Y
Get Transactions	Y	Y	Y
Get Transaction Details	Y	Y	Y
List Next Case	Y	Y	Y
Update Case	Y	Y	Y
Manage Queues	Y	Y	N
Rebuild Queues	Y	Y	N
View Queue Status	Y	Y	N
Manage Inbound Calls	Y	Y	Y
Analyze Transactions	Y	Y	Y
Add User to Exception List	Y	Y	Y
Delete User from Exception List	Y	Y	Y
Search Cases	Y	Y	N
RA Configurations			
See Managing Global Configurations for more information about the tasks related to these privileges.			
Create Ruleset	Y	Y	N
Assign Ruleset	Y	Y	N
Assign Channel and Configure Default Account Types	Y	N	N
Manage Miscellaneous Configurations (global level)	Y	N	N
Manage Miscellaneous Configurations (organization level)	Y	Y	N

Privilege	GA	OA	UA
Model Configuration (global level)	Y	N	N
Model Configuration (organization level)	Y	N	N
Configure Risk Analytics Callouts	Y	Y	N
Migrate to Production	Y	Y	Y
Card Issuer Mapping	Y	Y	N
Transaction Acquirer Mapping	Y	Y	N
Configure Card Numbers	Y	N	N

Rule Management Privileges

See [Managing Rules](#) for more information about the tasks related to these privileges.

Evaluate Risk	Y	Y	Y
List User Device Associations	Y	Y	Y
Delete User-Device Associations	Y	Y	Y
Manage List Data and Category Mappings	Y	Y	N
Rules and Scoring Management	Y	Y	N
Post Evaluate	Y	Y	Y

Other Privileges

Get QnA Attributes	Y	Y	N
Get QnA Values	Y	Y	Y
List Arcot Attributes	Y	Y	N
List Repository Attributes	Y	Y	N
Perform QnA Verification	Y	Y	Y
Bulk Upload	Y	Y	N
View Bulk Upload Requests	Y	Y	N
Get Location and Connection Info	Y	Y	Y

Report Privileges

See [Managing Reports](#) for more information about the tasks related to these privileges.

View My Activity Report	Y	Y	Y
	Y	Y	Y

Privilege	GA	OA	UA
View User Activity Report			
View User Creation Report	Y	Y	Y
View Organization Report	Y	Y	N
View Administrator Activity Report	Y	Y	Y
Risk Detail Activity Report	Y	Y	Y
View Advice Summary Report	Y	Y	Y
Device Summary Report	Y	Y	N
View Exception User Report	Y	Y	Y
View Rules Configuration Report	Y	Y	N
View Rules Data Report and Category Mappings	Y	Y	N
Case Activity Report	Y	Y	N
Average Case Life Report	Y	Y	N
False Positives Report	Y	Y	Y
View Fraud Statistics Report	Y	Y	Y
Rule Effectiveness Report	Y	Y	Y
Reports Summary	Y	Y	Y

How to Access the Administration Console

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

- **User Name:** masteradmin
- **Password:** <password set during bootstrap>

To log into the console, follow these steps:

1. Open a Web browser window.

2. Enter the URL to access Administration Console. The default Administration Console address is:

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

In the preceding URL:

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

The Master Administrator Login page appears.

3. In the **Password** field, enter the password that you set during bootstrap, and click **Log In**. The landing page of Administration Console appears.

How to Change Password and Profile Information

You must change your Master Administrator password regularly to maintain high security, so that unauthorized persons do not gain access to Administration Console by using the MA credentials. Use the My Profile page to change your current password and your preferences that will be reflected by default for all administrator-related and user-related tasks that you perform in future.

To change your account password and profile information:

1. Ensure that you are logged in as the MA.
2. Click the **MASTERADMIN** link in the console header.
The My Profile page appears.
3. In the **Change Password** section, specify:
 - a. The **Current Password**.
 - b. The **New Password**.
 - c. The new password again in the **Confirm Password** field.
4. In the **Administrator Preferences** section, specify:
 - a. Whether you would like to **Enable Preferred Organization**.
This organization will be selected by default in the "Organization" field for all administrator-related and user-related tasks that you perform from now on. For example, when you search the administrators, by default they will be searched in the preferred organization.
 - b. The **Preferred Organization** that will be selected by default in the "Organization" field from now on.

- c. The preferred **Date Time Format**.

This **Date Time Format** will be shown from now on in all date-related fields, except the report criteria page, user deactivate dialog box, and the administrator credential lock section where you need to provide the date input.

- d. The preferred **Locale** for your login of Administration Console.

- e. The preferred **Time Zone**.

This **Time Zone** will be shown from now on in all the date-related fields in Administration Console.

The default **Time Zone** is **GMT**.

5. Click **Save**.

Security Recommendations While Using Administration Console

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

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

Quick Administration

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

- [For Simple Deployments](#)
- [For Complex Deployments](#)

For Simple Deployments

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

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

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

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

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

1. Ensure that RA is installed and configured properly and that you have deployed the WAR files for the Administration Console.
2. Log in to the Administration Console as MA and follow the steps in the Bootstrap wizard to initialize the system.
3. The MA must create the first GA account(s).
4. As a GA, create the required GA, OA, and UA accounts.
5. As a GA or OA, configure the required RA rulesets and rules to meet your business requirements.

6. Create and deploy additional (custom) rules if the out-of-the-box rules do not match your business requirements.
7. As a UA, create users in RA.

With this, your system is set for risk evaluation. You can now manage the system, rules, and administrators and users.

For Complex Deployments

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

Note: See Planning the Deployment for more information about this type of deployment.

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

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

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

1. Ensure that RA is installed and configured properly and that you have deployed the WAR files for the Administration Console.
2. Log in to the Administration Console as MA and follow the steps in the Bootstrap wizard to initialize the system.
3. Configure the Administration Console settings, which include UDS settings, global organization settings, Administration Console cache settings, and the basic username-password authentication policy for logging in to the console.
4. Set up Transaction Server instances on different systems.
5. Configure the protocols that Administration Console, SDKs, and Web Services use to communicate to Transaction Server.
6. Plan and create organizations. The organization architecture is flat and each organization that you create can map to a business unit in your enterprise.

7. The MA must create the first GA account(s).
8. If required, configure Secure Sockets Layer (SSL)-based communication between Transaction Server and its clients.
9. Plan and create the required custom roles, if any.
10. As a GA, create the required GA, OA, and UA accounts.
11. As a GA or OA, configure the appropriate rules and rulesets to meet your business requirements, and assign these configurations.
12. Create and deploy additional (custom) rules if the out-of-the-box rules do not match your business requirements.
13. If you are planning to extend the RA functionality by the use of callouts, then define and configure the required configurations.
14. As a UA, create users in RA.

With this, your system is set for risk evaluation. You can now manage the system, rules, and administrators and users.

Configuring Administration Console Settings

Before you configure any RA-specific settings, it is recommended for security purpose that you configure the out-of-the-box settings for Administration Console. This article covers the following topics:

- [How to Create a Global Administrator Account](#)
- [How to Specify Basic Authentication Policy Settings](#)
- [How to Configure the Master Administrator Authentication Policy](#)
- [How to Change the Default Organization](#)
- [How to Update UDS Configurations](#)
- [How to Refresh the Cache](#)
- [How to Configure Custom Locales](#)
- [How to Configure Attribute Encryption](#)
- [How to Configure Web Services Authentication and Authorization](#)
- [Other Miscellaneous Optional Tasks](#)

How to Create a Global Administrator Account

To create a GA account:

1. Ensure that you are logged in with the required privileges and scope to create the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create Administrator** link to display the Create Administrator page.
4. In the **Administrator Details** section, enter the details of the administrator. The following table explains the fields on this page.

Input	Description
User Name	The unique user name for the administrator.
Organization	The display name of the organization to which the administrator belongs. Note: This is <i>not</i> the organization that this administrator will manage.
First Name	The first name of the administrator.
Middle Name	The middle name, if any, of the administrator.

Input	Description
(optional)	
Last Name	The last name of the administrator.

5. In the **Email Address(es)** section, enter the email address of the administrator for the email types configured for the organization.

6. In the **Telephone Number(s)** section, enter the phone number to contact the administrator.

If multiple telephone types are configured, you *must* enter values for all the mandatory telephone types.

7. In the **Custom Attributes** section, enter the **Name** and **Value** of any attributes you want to add, such as office location.

8. Click **Next** to proceed.

The next page appears.

9. On this page:

Specify the role of the new administrator from the **Role** drop-down list.

- In the **Set Password** section, set and confirm the password for the administrator.
- In the **Manages** section, select the organizations that the administrator will have scope on, and perform one of the following:
 - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.
or
 - Select the required organizations from the **Available Organizations** list and click the > button to add these organization to the **Selected Organizations** list.

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

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

11. Communicate the new password to the administrator.

How to Specify Basic Authentication Policy Settings

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

- If you select the **Basic User Password** option while creating an organization, then you can use the default authentication policy, as discussed in "How to Configure the Basic Authentication Password Policy" (for global level).

- If you select the **LDAP User Password** option, the password stored in LDAP is used by the administrator to log in. The authentication policy is defined in the LDAP system.
- If you select the **WebFort User Password** option, then ensure that Arcot WebFort 7.0 is deployed and accessible.

Note: See the *CA Arcot WebFort 7.0* documentation for detailed information to install and configure WebFort in your environment.

Configuring Basic Authentication Policy

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

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

To configure Basic Authentication policy for the Administration Console:

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

Parameter	Default Value	Description
Minimum Password Length	6	The minimum number of characters that the password must contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The maximum number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.

Parameter	Default Value	Description
Maximum Password History Count	3	The maximum number of previously used passwords that cannot be reused.
Validity Period	180 days	The maximum number of days for which a password is valid.
Allow Multi-Byte Characters		Select this option if you want to allow multi-byte characters in the password.
The following options are disabled if you select this check box.		
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#\$%^&*()_+	The list of special characters that the password can contain.

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

7. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure the Master Administrator Authentication Policy

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

You can use the Master Administrator Authentication Policy page to strengthen the MA'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.

To configure the MA authentication policy:

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

Parameter	Default Value	Description
Minimum Password Length	6	The minimum number of characters that the password must contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The maximum number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.
Maximum Password History Count	3	The maximum number of previously used passwords that cannot be reused.
Validity Period	180 days	The maximum number of days for which a password is valid.
Allow Multi-Byte Characters		Select this option if you want to allow multi-byte characters in the password.
The following options are disabled if you select this check box.		
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#\$%^&*()_+	The list of special characters that the password can contain.

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

How to Change the Default Organization

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

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

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

To change your default organization:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **UDS Configuration** section on the side-bar menu, click the **Set Default Organization** link to display the page.
5. Under **Default Organization**, select the organization that you want to set as the Default Organization from the **Organization Name** list.
6. Click **Save** to save the changes you made on this page.
7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Update UDS Configurations

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

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

- **If you are using a relational database**, then you just need to seed the database with Arcot schema as a part of the post-installation configurations.
- **If you are using an LDAP directory server** and you want Transaction Server, Case Management Server, and Administration Console to seamlessly access it, then you must deploy User Data Service as a part of the post-installation configurations.

How to Change the Default UDS Connectivity Configuration

To update the default UDS connectivity settings, you must use the UDS Connectivity Configuration page.

To change the default UDS Connectivity configuration:

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

Parameter	Default Value	Description
Protocol	TCP	<p>The protocol to connect to the UDS service by using Administration Console. The available options are:</p> <p>TCP: If you want to implement unencrypted information exchange between UDS and Administration Console, Transaction Server, and the RA Database.</p> <p>One-Way SSL: If you want to implement SSL communication between UDS and RA components, and RA components must present their certificates when accessing UDS.</p> <p>Two-Way SSL: If you want to implement SSL communication between UDS and RA components, and both UDS and RA components must present their certificates during information exchange.</p>
Host	localhost	The IP address or host name where the UDS service is available.
Port	8080	The port at which the UDS service is available.
Application Context Root	arcotuds	The application context that is specified when UDS is deployed on the application server.
Connection Timeout (in milliseconds)	30000	Maximum time in milliseconds before the UDS service is considered unreachable.
Read Timeout (in milliseconds)	10000	

Parameter	Default Value	Description
		The maximum time in milliseconds to wait for a response from UDS.
Idle Timeout (in milliseconds)	30000	The time (in milliseconds) after which an idle connection not serving requests will be closed.
Server Root Certificate		<p>The path to the Certificate Authority (CA) certificate file of the UDS server. The file must be in PEM format.</p> <p>Note: This field will <i>not</i> be enabled if you selected the TCP option in the Protocol field.</p>
Client Certificate		<p>The path to the CA certificate file of Administration Console. The file must be in PEM format.</p> <p>Note: This field will <i>not</i> be enabled if you selected the TCP or One-Way SSL option in the Protocol field.</p>
Client Private Key		<p>The location of the file that contains the CA's private key. The path can be an absolute path or relative to ARCOT_HOME.</p> <p>Note: This field will <i>not</i> be enabled if you selected the TCP or One-Way SSL option in the Protocol field.</p>
Minimum Connections	4	The minimum number of connections that will be created between Transaction Server and the UDS server.
Maximum Connections	32	The maximum number of connections that can be created between Transaction Server and the UDS server.

6. Click **Save** to save the changes you made.

7. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Change the Default UDS Parameters

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

To change the default UDS parameters:

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

Parameter	Default Value	Description
Search Configuration		
Maximum Search Return Count	500	The maximum number of records that will be returned for all Search operations in Administration Console.
LDAP Configuration		
Note: These fields cannot be edited using Administration Console.		
LDAP Connection Pool Initial Size	NA	The initial number of connections between UDS and LDAP that will be created in the pool.
LDAP Connection Pool Maximum Size	NA	The maximum number of connections allowed between UDS and LDAP.
LDAP Connection Pool Preferred Size	NA	The preferred number of connections between UDS and LDAP.
LDAP Connection Pool Timeout (in milliseconds)	NA	The period for which UDS waits for a response from LDAP, when a new connection is requested.
Authentication and Authorization Token Validity Configuration		
Purge Interval (in seconds)	3600	The maximum interval after which an authentication token is purged from the database, <i>after</i> the token expires.
Validity Period (in seconds)	86400	The maximum period (default is one day) after which an issued authentication token expires.

6. Click **Save** to save the changes you made.
7. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Refresh the Cache

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

Data Cached at the System Level

The following data is cached at the system level:

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

Data Cached at the Organization Level

The following data is cached at the organization level:

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

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

Cache Refresh Order Example

Account type details and global account types are cached at the system level. Whenever you create a new account type, irrespective of whether it is global or organization-specific, you must refresh the system cache. In addition, if the account type is organization-specific, you must refresh the cache of all the organizations involved in the scope. For more information about account types, see [How to Configure Account Types](#).

How to Refresh the Administration Console Cache

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

Note: The Master Administrator (MA) and Global Administrator (GA) can refresh the cache of Administration Console and all instances of Transaction Server and Case Management Server. The MA, GA, and Organization Administrator (OA) can refresh the cache of the organizations within their scope.

To refresh the Administration Console cache:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **System Configuration** section on the side-bar menu, click the **Refresh Cache** link to display the page.
5. Select one or both of the following:
 - Select **Refresh System Configuration** to refresh the cache configuration of Administration Console, User Data Service, and all Transaction Server and Case Management Server instances.
 - Select **Refresh Organization Configuration** to refresh the cache configuration of all organizations in your purview.
6. Click **OK**.
7. Click OK in the confirmation dialog box that appears.
A message with a Request ID for the current cache refresh request is displayed.

Note: See [When to Perform Server Refresh and Restart Tasks](#) for at-a-glance information on tasks after which you need to refresh the server cache.

How to View the Status of Cache Refresh Requests

You can view the status of a cache refresh request either by selecting a Request ID that was generated for the cache refresh request or by selecting a specific status, such as In Progress, Failure, Successful, or All.

To view the status of a cache refresh request:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **System Configuration** section on the side-bar menu, click the **Check Cache Refresh Status** link to display the page.
5. Enter a **Request ID** or select a **Status** and click **Search** to check the status of the cache refresh request.
The cache refresh details are displayed. You can see the status of the cache refresh operation for the different server instances.
The search result lists the following:
 - The unique identifier of the cache refresh request
 - Organizations that were affected by cache refresh request
 - Time when the request was received
 - The event type
 - Transaction Server instances that were affected by cache refresh request. The following table describes the Transaction Server instance details.

Parameter	Description
Resource	<p>The RA resource that was refreshed. Possible values are:</p> <p>AdminConsole For Administration Console and User Data Service</p> <p>Risk Analytics For Transaction Server</p>
Server Instance ID	<p>Specifies the unique identifier of the server instance that was refreshed.</p> <p>For Administration Console and User Data Server, this value is fetched from the InstanceID parameter set in arcotcommon.ini file.</p> <p>For Transaction Server, it is the instance name of Transaction Server. By default, it is a combination of host name and a unique identifier.</p>
Server Instance Name	<p>Specifies the instance name of the Risk Analytics component that was refreshed. Possible values are:</p> <p>Arcot Administration Console</p> <p>User Data Service</p>

Parameter	Description
	Instance name of Transaction Server
Host Name	Specifies the name of the system on which the refreshed component is installed.
Status	Specifies the status of the cache refresh request.


How to Configure Custom Locales

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

Before you configure the available locales, you can add additional locales that will appear in the **Available** list for you to choose.

To configure a custom locale:

1. Ensure that you are logged in as the MA.
 2. Activate the **Services and Server Configurations** tab.
 3. Click the **Administration Console** option on the submenu of the tab.
 4. Under the **System Configuration** section on the side-bar menu, click the **Localization Configuration** link to display the page.
 5. In the **Configure Supported Locales** section, select the locales that you want to add from the **Available** list, and use the > or < buttons to move them to the **Selected** list.
You can also click the >> or << buttons to move all locales to the desired lists.
 6. In the **Configure Default Locale** section, select the **Default Locale** from the drop-down list.
 7. In the **Configure Default Date Time Format** section, specify the **Date Time Format** you want to use.

Move your cursor over the  icon to determine the **Date Time Format** that you want to use.
- Note:** The Administrator can change the **Locale** and **Date Time Format** at the organization level and also on the My Profile page.
8. Click **Save** to save your changes.
 9. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure Attribute Encryption

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

To ensure that user data is stored in database in encrypted format:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **System Configuration** section on the side-bar menu, click the **Attribute Encryption Configuration** link to display the page.

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

- User ID
- Account ID
- Account ID attributes

5. In the **Select Attribute(s) for Encryption** section, select the attributes that you want to encrypt from the **Available Attributes for encryption** list to the **Attributes Selected for encryption** list.
Click the > or < buttons to move selected attributes to the desired list. You can also click the >> or << buttons to move all attributes to the desired lists.

6. In the **Data Masking Configuration** section, specify the parameters described in the following table.

Note: Data masking is the process of hiding specific elements within the actual data string. It ensures that sensitive data is replaced with some data other than the real one.

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

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

8. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

Examples of Masking and Unmasking

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

If you want to unmask a user name that has been configured for encryption, and the **Start Length**, **End Length**, and **Masking Character** are 2, 2, and x, then the user name "mparker" is unmasked as "mpxxxer".

How to Configure Web Services Authentication and Authorization

RA provides Web services to programmatically perform the operations that are supported by Administration Console. You can secure these Web services calls by enabling authentication and authorization. You can use Administration Console to select the Web services for which you want to enable authentication and authorization.

To configure Web Services A&A:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **Web Services** section on the side-bar menu, click the **Authentication and Authorization** link to display the page.
5. In the **Web Services** section, select and move the Web services from the **Disabled** list to the **Enabled** list.
Click the > or < buttons to move selected Web services to the desired list. You can also click the >> or << buttons to move all Web services to the desired lists.
6. Click **Save** to save your changes.
7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Other Miscellaneous Optional Tasks

This section covers:

- [How to Configure Account Types](#)
- [How to Configure Email and Telephone Types](#)

How to Configure Account Types

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

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

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

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

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

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

- BNG02132457678
- FIXED_DEPOSITS/000203876544
- ONLINE_BANKING/rlaurie

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

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

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

Creating a New Account Type

To create a new account type:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **UDS Configuration** section on the side-bar menu, click the **Configure Account Type** link to display the page.
5. (If this is the first account type you are adding) In the **Add New Account Type** section:

- a. Enter the **Name** of the account type.
 - b. Enter a **Display Name** for the account type.
 - c. If required, expand the **Custom Attributes** section by clicking the + sign and specify the **Name** and **Value** of any custom attributes that you want to add for this account type.
6. In the **Assign to Organizations** section:
- Select **Apply to all Organizations** if you want to use this account type for all existing organizations and any organizations that might be created in future.
- Note:** Such accounts appear under **Global Accounts** on the Configure Account Type page at the organization level.
- or
- Select the organization to which you want to assign the account type from the **Available** list and move it to the **Selected** list.
- Note:** The accounts assigned to specific organizations appear under **Organization-Specific Accounts** on the Configure Account Type page at the organization level.
- Click the > or < buttons to move selected organizations to the desired list. You can also click the >> or << buttons to move all organizations to the desired lists.
7. Click **Create** to create the account type.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Updating an Account Type

To update an account type:

1. Select the account type from the **Select Account Type** drop-down list.
2. Modify the required fields, and click **Update**.

Note: Once you have created an account type, you cannot change the **Name** of the account type.

3. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Deleting an Account Type

To delete an account type:

1. Select the account type from the **Select Account Type** drop-down list.
2. Click **Delete**.

Important! You cannot delete an account type if you have created user accounts for that type.

3. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure Email and Telephone Types

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

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

Email and Telephone Type Example

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

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

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

Configuring Email and Telephone Types

To configure multiple email and telephone types:

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

- **Display Name** of the Email Type.
- Whether the Email Type is **Mandatory**.

For example, you can configure work email with a higher priority than your personal email so that work email gets displayed first.

5. In the **Configure Telephone Type** section, specify:

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

Note: You can add multiple Email and Telephone types by clicking the + icon.

6. Click **Save** to save your changes.

7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Working with Custom Roles

Risk Analytics is shipped with out-of-the-box roles that are associated with pre-defined privileges. However, RA also provides you the capability to manipulate these pre-defined roles if:

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

This article explores the ability to create and apply custom roles in RA, which are a major benefit. This article guides you through the following topics:

- [Understanding Custom Roles](#)
- [How to Create a Custom Role](#)
- [How to Update a Custom Role Information](#)
- [How to Delete a Custom Role](#)

Understanding Custom Roles

As an MA, you can create *new administrative roles* that inherit a subset of privileges from one of the following pre-defined parent roles, as discussed in [Getting Started with the Administration Console](#):

- Global Administrator
- Organization Administrator
- User Administrator

These roles are called *custom roles*, and are derived by **disabling** some of the default privileges associated with the parent role. For example if you need to disable the privilege to create organizations for a GA, then you can create a custom role by disabling this privilege, and assign the same to the GA.

Things That You Should Know About Custom Roles

Only the MA can create custom roles.

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

For example, you *cannot* create a custom UA role that has privileges to manage users (UA privilege) and create organizations (OA privilege.)

You cannot assign new privileges to a custom role, if the parent role does not have these privileges.

For example, if the pre-defined OA role does not have the privilege to create an organization, then the custom role based on this OA role cannot have that privilege either.

When you create a custom role, a task representing one or more privileges will continue to be visible, as long as at least one of the privileges is *still* available.

For example, the **Search Organizations** link will appear if the Update privilege is still available, even though the Activate, Deactivate, and Delete privileges are disabled.

A new custom role is available to other instances of Administration Console *only after* you refresh the Administration Console server cache.

Pre-Defined Custom Roles

In addition to the custom roles that you can create, RA has three pre-defined custom roles that are required for Case Management. These roles include:

- **QM:** The **Queue Manager** role has the required privileges to supervise cases. This role is derived from the default Organization Administrator role.
- **CSR:** The **Customer Support Representative** role has the required privileges to work on cases and handle end-user calls. This role is derived from the default User Administrator role.
- **FA:** The **Fraud Analyst** role has the required privileges to analyze cases to find hidden trends and patterns. This role is also derived from the default User Administrator role.

Note: See [Managing Cases](#) for detailed information about Case Management and the Queue Manager, Customer Support Representative, and Fraud Analyst roles.

You can see these out-of-the-box custom roles on the Update Custom Role page.

How to Create a Custom Role

When you create a custom role, it becomes available as a role option when you create or update an administrator. A new custom role is available only after refreshing the Transaction Server cache.

To create a new role:

1. Ensure that you are logged in as the MA.
2. Activate the **Users and Administrators** tab.
3. Click the **Manage Roles** link on the submenu of the tab.
4. Under the **Manage Roles** section, click the **Create Custom Role** link. The Create Custom Role page appears.
5. In the **Role Details** section, specify the following information:
 - **Role Name:** The unique name to identify the new role. This name is used internally by RA by authenticating and authorizing this new role.

- **Role Display Name:** The descriptive name of the role that appears on all other Administration Console pages and reports.
 - **Role Description:** The useful information related to the role for later reference.
 - **Role Based On:** The pre-existing role from which this custom role should be derived.
6. In the **Set Privileges** section, specify the roles that will *not* be available to the new role:
 - a. In the **Available Privileges** list, select all the privileges that you need to *disable* for the custom role.
This list displays all the privileges available to the administrative role that you selected in the **Role Based On** field.
 - b. Click the > button to move the selected privileges to the **Unavailable Privileges** list.
 7. Click **Create** to create the custom role.
 8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Update a Custom Role Information

You can update custom roles by enabling or disabling the privileges available to the role.

To update a custom role you created:

1. Ensure that you are logged in as the MA.
2. Activate the **Users and Administrators** tab.
3. Click the **Manage Roles** link on the submenu of the tab.
4. Under the **Manage Roles** section, click the **Update Custom Role** link.
The Update Custom Role page appears.
5. Select the **Role Name** that you want to update.
6. In the **Role Details** section, change the **Role Display Name** and **Role Description**, if required.
7. In the **Set Privileges** section, if required, specify the list of privileges that will *not* be available to the role:
 - a. In the **Available Privileges** list, select all the privileges that you need to *disable* for the new role.
This list displays all the privileges available to the administrative role that you selected in the **Role Based On** field.
 - b. Click the > button to move the selected privileges to the **Unavailable Privileges** list.
8. In the **Set Privileges** section, if required, specify the list of privileges that *will be* available to the role:

- a. In the **Unavailable Privileges** list, select the privileges that you want to *enable* for the new role.
This list displays all the privileges that are not available to the administrative role that you selected in the **Role Based On** field.
 - b. Click the < button to move the selected privileges to the **Available Privileges** list.
9. Click **Update** to update the Custom role definition.
 10. Refresh *all* deployed RA Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Delete a Custom Role

Important! If you need to delete a custom role that is currently assigned to an administrator, then you must first change the role of all administrators who have been assigned this role by using the Update Administrator page and then follow the instructions in this topic.

To delete a custom role you created:

1. Ensure that you are logged in as the MA.
2. Ensure that no active administrator is assigned this role.
3. Activate the **Users and Administrators** tab.
4. Click the **Manage Roles** link on the submenu of the tab.
5. Under the **Manage Roles** section, click the **Delete Custom Role** link.
The Delete Custom Role page appears.
6. In the **Role Details** section, select the custom role that you need to delete from the **Role Name** list.
7. Click **Delete** to delete the selected custom role.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Managing Server Instances

As a Master Administrator, you will need to manage a Transaction Server instance locally. However, before you can manage a server instance, you must configure the connectivity parameters to connect to the instance. For more information about this, see [How to Configure Server Connectivity](#).

Only after you configure the connectivity parameters, you can manage the Transaction Server instance. The tasks for managing an instance include:

- [How to Configure Server Connectivity](#)
- [How to Create Trust Stores](#)
- [How to Configure Communication Protocols for Server Instances](#)
- [How to Refresh a Server Instance](#)
- [How to Update Server Instance Configurations](#)
- [How to Shut Down a Server Instance](#)
- [How to Restart a Server Instance](#)

Note: [Shutting Down a Server Instance](#) can also be performed by using system tools, as discussed in [Tools for Administrators](#).

How to Configure Server Connectivity

RA comprises two server components:

- **Transaction Server**, which is the core engine for risk evaluations.
- **Case Management Server**, which is responsible for building, prioritizing, and dispatching cases to administrators according to the Queue definitions.

The following table lists the four sections on the Risk Analytics Connectivity page and describes the components that you can connect using each section.

Configuration Section	Description
Risk Analytics Transaction Server Management Connectivity	Used by Administration Console to connect to the Transaction Server Management port. For example, cache refresh and shutdown requests to Transaction Server.
Case Management Server Management Connectivity	Used by Administration Console to connect to the Case Management Server Management port. For example, cache refresh and shutdown requests to Transaction Server.
Risk Analytics Administration Connectivity	

Configuration Section	Description
	Used by Administration Console to connect to the Transaction Server Administration web service port. For example, the Rules and Scoring Management screen and Model Configuration screen.
Case Management Server Connectivity	Used by Administration Console to connect to the Case Management Server instance. For example, to issue Queue rebuild requests and to fetch the next case in the Queue.

For Transaction Server Management

You must use the Risk Analytics Transaction Server Management Connectivity section to configure the connection settings that will be used by Administration Console to connect to your Transaction Server Management instance.

To specify the connectivity parameters used by Administration Console to connect to the Transaction Server Management instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Risk Analytics** link on the submenu of the tab.
4. If not already displayed, click the **Risk Analytics Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the RA connectivity parameters.

Field	Description
Server	Enter the IP address or host name of the system where you installed the required Transaction Server Management instance. Note: Ensure that the system where Transaction Server is installed is accessible by its hostname on the network.
Server Management Port	Enter the port on which the Risk Evaluation service is exposed.
Transport	Specify the transport mode (TCP or SSL) for the following components to connect to the specified Transaction Server Management instance: Server Management Web Services Administration Web Services Transaction Web Services

Field	Description
	Authentication Native
Server CA Root Certificate	Browse to and upload the server CA root certificate. Note: This server certificate must be in PEM format.
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

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

For Case Management Server Management

You must use the Case Management Server Management Connectivity section to configure the connection settings that will be used by Administration Console to connect to your Case Management Server Management instance.

To specify the connectivity parameters used by Administration Console to connect to the Case Management Server Management instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Risk Analytics** link on the submenu of the tab.
4. If not already displayed, click the **Risk Analytics Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the Case Management Server connectivity parameters.

Field	Description
Server	Enter the IP address or host name of the system where you installed the required Case Management Server Management instance.
Server Management Port	Enter the port on which the Case Management service is exposed.
Transport	Specify the transport mode (TCP or SSL) for the corresponding component to connect to the specified Case Management Server Management instance: Server Management Web Services Administration Web Services

Field	Description
	Transaction Web Services
	Authentication Native
Server CA Root Certificate	Browse to and upload the server CA root certificate. Note: This server certificate must be in PEM format.
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

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

For Risk Analytics Administration

You must use the Risk Analytics Administration Connectivity section to configure the connection settings that will be used by Administration Console to connect to your Transaction Server Administration instance.

To specify the connectivity parameters used by Administration Console to connect to the Transaction Server Administration instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Risk Analytics** link on the submenu of the tab.
4. If not already displayed, click the **Risk Analytics Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the RA connectivity parameters.

Field	Description
Server	Enter the IP address or host name of the system where you installed the required Transaction Server Administration instance. Note: Ensure that the system where Transaction Server is installed is accessible by its hostname on the network.
Server Management Port	Enter the port on which the Risk Evaluation service is exposed.
Transport	Specify the transport mode (TCP or SSL) for the following components to connect to the specified Transaction Server Administration instance:

Field	Description
	Server Management Web Services
	Administration Web Services
	Transaction Web Services
	Authentication Native
Server CA Root Certificate	Browse to and upload the server CA root certificate. Note: This server certificate must be in PEM format.
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

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

For Case Management Server

You must use the Case Management Server Connectivity section to configure the connection settings that will be used by Administration Console to connect to your Case Management Server instance.

To specify the connectivity parameters used by Administration Console to connect to the Case Management Server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Risk Analytics** link on the submenu of the tab.
4. If not already displayed, click the **Risk Analytics Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the Case Management Server connectivity parameters.

Field	Description
Host	Enter the IP address or host name of the system where you installed the Case Management Server instance. Note: Ensure that the system where Case Management Server is installed is accessible by its hostname on the network.
Backup Host	

Field	Description
	<p>If installed, enter the IP address of the system where the backup Case Management Server instance is available.</p> <p>Important! You must configure this Backup Host parameter <i>before</i> you start the backup Case Management Server.</p>
Port	Enter the port on which the Case Management service is exposed.
Transport	<p>Specify the transport mode (TCP or SSL) for the corresponding component to connect to the specified Case Management instance:</p> <p>Server Management Web Services</p> <p>Administration Web Services</p> <p>Transaction Web Services</p> <p>Authentication Native</p>
Server CA Root Certificate	<p>Browse to and upload the server CA root certificate.</p> <p>Note: This server certificate must be in PEM format.</p>
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

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

How to Create Trust Stores

You can create a trust store to authenticate RA components (that include Administration Console and Java SDKs) or other clients to a Transaction Server instance during SSL-based communications. A *trust store* contains a set of CA root certificates trusted by Transaction Server and the Case Management Server instances.

You can use the Trusted Certificate Authorities page to create trust stores and to add new root certificates to your trust stores.

Follow these steps:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **Risk Analytics** tab in the submenu is active.

3. Under the **System Configuration** section, click the **Trusted Certificate Authorities** link to display the Trusted Certificate Authorities page.
4. In the **Name** field, enter the name for the new trust store that you want to create.
5. Click the corresponding **Browse** buttons to upload one or more root certificates of the trusted CAs. You can click **Add More** to display additional fields for uploading certificates.
6. Click **Save** when you finish uploading all certificates.

How to Configure Communication Protocols for Server Instances

The Protocol Configuration page allows you to configure protocols for the Transaction Server instance or the Case Management Server instance.

By selecting the Transaction Server instance from the drop-down list, you can configure the protocols that Administration Console, SDKs, and Web Services use to communicate with your Transaction Server instance for authentication and administration purposes. In addition to the port on which the server listens to each of these enabled components, you can also specify the transport security mechanism (TCP or SSL). In case you specify this mechanism as SSL, then you must also specify the valid and trusted client component's certificate and private key that are required for establishing a secure connection.

The following table explains the protocols that you see in the **List of Protocols** table for the Transaction Server instance and lists their default port numbers.

Protocol	Default Port Number	Description
Native (TCP)	7680	<p>This is the protocol to enable communication between the Transaction Server instance and the RA Java SDKs, which include Risk Evaluation and Issuance (deprecated).</p> <p>Note: The Web service interface is available for Issuance as part of the user management Web Service Definition Language (WSDL).</p>
Administration Web Service	7777	<p>This is the protocol for communication between Transaction Server and Administration Web services.</p> <p>Transaction Server listens to the Administration Web service calls on this port.</p> <p>Note: These calls do <i>not</i> include the RA Issuance (deprecated) or Risk Evaluation calls.</p>
Transaction Web Service	7778	

Protocol	Default Port Number	Description
		<p>This protocol is used by the Risk Evaluation and the Issuance (deprecated) Web services to connect to the Transaction Server instance. This protocol receives Web services requests that are sent by Authentication and Issuance Web services.</p> <p>Note: These calls do <i>not</i> include the Administration service calls.</p>
Native (SSL)	7681	<p>This is a binary protocol to enable SSL-based communication between the Transaction Server instance and the RA Java SDKs, which include Risk Evaluation and Issuance (deprecated).</p>
Server Management	7980	<p>The arrfclient tool communicates with the Transaction Server instance for server management activities (graceful shutdown and server cache refresh) by using this protocol.</p> <p>See Tools for Administrators for detailed information about this Administration Console tool.</p>
ISO8583 Native (TCP)	7690	<p>This is the protocol used by RA to support transactions originating from ATM or POS channels. RA receives ATM or POS transaction data over this TCP port as an asynchronous ISO 8583 message and returns the Risk Advice as an ISO 8583 message.</p> <p>Note: Transaction data for ATM or POS channels is received as ISO 8583 protocol messages that might be compliant with one of the following ISO 8583 versions or their variants:</p> <p>ISO 8583:1987</p> <p>ISO 8583:1993</p>

Similarly, by selecting the Case Management Server instance from the drop-down list, you can configure the protocols that Administration Console and the Case Management Server use to communicate with your Transaction Server instance for authentication and administration purposes. In addition to the port on which the server listens to each of these enabled

components, you can also specify the transport security mechanism (TCP or SSL). In case you specify this mechanism as SSL, then you must also specify the valid and trusted client component's certificate and private key that are required for establishing a secure connection.

The following table explains the protocols that you see in the **List of Protocols** table for the Case Management Server instance and lists their default port numbers.

Protocol	Default Port Number	Description
Case Management Server	7779	This protocol is used by the Case Management Server module to listen to the Case Management requests from the Administration Console on the specified port.
Case Management Administration	7780	This is the protocol for communication with Case Management Server for administrative operations.
Case Management Transaction Web Service	7781	This protocol is used by the Case Management Server module to listen to the Case Management Web service requests received from external clients on the specified port.

To configure Transaction Server and the Case Management Server network protocols:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **Risk Analytics** tab in the submenu is displayed.
3. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
4. Select the Transaction Server instance or Case Management Server instance from the drop-down list.
The **List of Protocols** appears.
5. In the **List of Protocols** table, click the link corresponding to the protocol that you want to configure.
The corresponding Protocol page appears.
6. Edit the fields on the page, as required. The following table explains these fields.

Column	Action Description
Change Protocol Status	Select this check box to enable the Action drop-down list and change the status of the protocol.
Action	Select Enable to enable the required protocols.
Port	Enter the port number where the corresponding service is available. Following are the default port numbers for RA protocols:

Column	Action Description
	Native (TCP): 7680
	Native (SSL): 7681
	Administration Web Services: 7777
	Transaction Web Services: 7778
	Case Management Server: 7779
	Case Management Administration: 7780
	Case Management Transaction Web Service: 7781
	Server Management: 7980
	ISO8583 Native (TCP): 7690
Minimum Threads	Minimum number of threads processed on the port.
Maximum Threads	Maximum number of threads processed on the port.
Transport	<p>Specify one of the following modes that are supported for data transfer:</p> <p>TCP: Transmission Control Protocol (TCP) mode is the default mode that is supported by both RA protocols. It sends data in the clear.</p> <p>SSL: Secure Sockets Layer (SSL) provides higher security for transactions, because it encrypts and decrypts data that is transmitted.</p>
Key in HSM	<p>Enable this check box if the private key for the SSL communication needs to be in the HSM device. In this case, Transaction Server and Case Management Server will find the private key based on the certificate chain provided.</p> <p>This check box is enabled only if you select SSL in "Transport".</p>
Server Certificate Chain	<p>Specify the certificate chain that is used by the SSL transport security mode. Use the Browse button to upload the Server Certificate Chain.</p> <p>Important! Ensure that the certificates in the chain that you upload here follow the Leaf certificate > Intermediate CA certificates > Root certificate hierarchy. The certificate and the key must be in PEM format.</p>
Server Private Key	Use the Browse button to upload the Server Private Key .

Column	Action Description
	Note: This field will be enabled only if you did not select the Key in HSM check box.
Select Client Store	Select the trust store that contains the root certificates of the trusted CAs. See How to Create Trust Stores for more information about configuring trust stores.
Channel-Header Configuration (Applicable only to ISO 8583 ports)	Contains the channel and header information required to parse incoming transactions for ATM and POS channels.

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

Configuring SSL Communication

By default, Administration Console uses Transmission Control Protocol (TCP) to communicate with Transaction Server. However, TCP is vulnerable to spoofing and man-in-the-middle attacks. By using Administration Console, you can configure SSL to ensure secure communication between different components of RA.

If you have configured SSL for secure communication, you can see the corresponding entries in the startup log files. The following table lists the log file entries when SSL is configured for Transaction Server and Case Management Server protocols.

Protocol	Entry in Log File
Risk Analytics	
Server Management	Started listener for [Server Management] [7980] [SSL] [srvmgrwsprotocol]
Transaction Web Service	Started listener for [Risk Analytics Trans WS] [7778] [SSL] [transwsprotocol]
Administration Web Service	Started listener for [Risk Analytics Admin WS] [7777] [SSL] [aradminwsprotocol]
Native (SSL)	Started listener for [Risk Analytics Native (SSL)] [7681] [SSL] [RiskAnalytics]
Case Management Server	
Case Management Administration	Started listener for [Case Management Admin] [7780] [SSL] [srvmgrwsprotocol]
Case Management Server	Started listener for [Case Management Server] [7779] [SSL] [RiskAnalyticsCaseManagement]
Case Management Transaction Web Service	Started listener for [Case Management WS] [7781] [SSL] [casewsprotocol]

How to Refresh a Server Instance

You can refresh Transaction Server and the Case Management Server instances either through Administration Console or by using the arrfclient tool. This topic covers the following:

- [By Using Administration Console](#)
- [By Using the arrfclient Tool](#)

By Using Administration Console

You can refresh specific Transaction Server and the Case Management Server instances by selecting the instance on the Instance Management page.

Follow these steps:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **Risk Analytics** tab in the submenu is displayed.
Under the **Instance Configuration** section, click the **Instance Management** link to display the page.
The following table describes the columns on the Instance Management page.

Column	Description
Instance Name	Name of Transaction Server or the Case Management Server instance.
Last Startup Time	The time the instance was last started.
Last Shut Down Time	The time the instance was last shut down.
Last Refresh Time	The time the instance was last refreshed.
Uptime	The duration for which the instance has been running.
Status	The status of the instance.
Organization List To Refresh	The list of organizations to refresh. Choose Select in the drop-down list to select the organizations that you want to refresh. or Select All in the drop-down list to refresh all organizations.
System Cache Refresh	Select this check box to refresh the system cache.

3. In the **Risk Analytics Instances** section:

Select the instance of Transaction Server that you want to refresh.

1. Select the organizations to refresh from the **Organization List to Refresh** drop-down list.
2. Select **System Cache Refresh** if you want to refresh the system cache configuration.
3. Click **Refresh**.
4. In the **Case Management Instances** section:

Select the instance of the Case Management Server that you want to refresh.

1. Select the organizations to refresh from the **Organization List to Refresh** drop-down list.
2. Select **System Cache Refresh** if you want to refresh the system cache configuration.
3. Click **Refresh**.

By Using the arrfclient Tool

You can use the **arrfclient** tool to refresh both Transaction Server and the Case Management Server instances.

Before you run the arrfclient tool for Transaction Server as directed in the following topics, set the Host and Port values in riskfortadminclient.ini. See [Tools for Administrators](#) for more information.

On Windows

Run the arrfclient tool to refresh the Transaction Server cache as follows:

1. Open the Command Prompt window.
2. Navigate to the following directory:

`<install_location>\Arcot Systems\bin\`
3. Run the following command to refresh:

- **Transaction Server instance:**

```
arrfclient -cr
```

- **Case Management Server instance:**

```
arrfclient <host_name> <port_number> -cr
```

On UNIX-Based Platforms

Run the arrfclient tool to refresh the Transaction Server cache as follows:

1. Open the terminal window.
2. Navigate to the following directory:

```
<install_location>/arcot/bin/
```

3. Run the following command to refresh:

▪ **Transaction Server instance:**

```
arrfclient -cr
```

▪ **Case Management Server instance:**

```
arrfclient <host_name> <port_number> -cr
```

How to Update Server Instance Configurations

You can update the instance attributes, logging configurations, and database configurations for the Transaction Server and Case Management Server instances.

Follow these steps:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **Risk Analytics** tab in the submenu is active.
3. Under the **Instance Configuration** section, click the **Instance Management** link to display the page.
4. Click the link corresponding to the instance whose configuration you want to update. The page to update the instance-specific configuration appears.
5. In the **Instance Attributes** section:
 - a. Select the check box to **Change the Instance Name** of your Transaction Server or Case Management Server instance.
 - b. Specify name for the instance in the **New Instance Name** field.
6. In the **Logging Configuration** section, specify values as described in the following table.

Field	Description
Transaction Log Directory	The directory to store the transaction log files. The path can be an absolute path or relative to ARCOT_HOME.
Rollover After (in Bytes)	The maximum number of bytes the log file can contain. When the log files reach this size, a new file with the specified name is created and the old file is moved to the backup directory.
Transaction Log Backup Directory	The backup directory to store the older transaction log files. The path can be an absolute path or relative to ARCOT_HOME.
Log Level	The severity level of the logged entry. Fatal, WARNING, INFO, and DETAIL are the supported levels in decreasing order of severity.
Log Timestamps in GMT	

Field	Description
	Select this option if you want to time stamp the logged information using GMT.
	RA enables you to either use the local time zone or GMT to timestamp the logged information.
Enable Trace Logging	An additional logging flag that logs the Entering and Exiting log for each function called during processing. By default, this flag is disabled. Enabling this flag logs huge amount of data for debugging. You must not enable this flag in production unless advised by CA Support.

7. In the **Database Configurations** section, specify values as described in the following table.

Field	Description
Minimum Connections	The minimum number of connections that will be created between Transaction Server and the database.
Maximum Connections	The maximum number of connections that can be created between Transaction Server and the database.
Increment Connections by	The value by which to increment the connections when all database connections in the pool are exhausted and used by the existing threads, and if any of the threads requests for a new database connection.
Monitor Thread Sleep Time (in Seconds)	The time interval after which the database monitor thread polls the database to check if the database is active and functional.
Monitor Thread Sleep Time in Fault Conditions (in Seconds)	Same as Monitor Thread Sleep Time. But this value is used only when the database monitor thread detects any failure. This value <i>must</i> be less than the Monitor Thread Sleep Time because polling must be done at frequent intervals in the case of any failure.
Log Query Details	When enabled, this option logs all the Oracle or MS SQL database queries executed by the Server. By default, this option is disabled and must be enabled <i>only</i> when debugging is required as in the case of Enable Trace Logging.
Monitor Database Connectivity	If this option is enabled, the Server creates the database monitor thread. Else, database monitoring is disabled.
Auto-Revert to Primary	When the connection to the primary database fails, the Server falls back to the backup database. If this option is enabled, the Server automatically reverts to the primary database when it is up and running.

8. Click **Save** to save your changes.

9. Refresh or restart your server instance depending on the parameters that you have updated.

For instructions on how to do this, see [How to Refresh a Server Instance](#) and [How to Restart a Server Instance](#).

How to Shut Down a Server Instance

To shut down a Transaction Server or Case Management Server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **Risk Analytics** tab in the submenu is displayed.
3. Under the **Instance Configuration** section, click the **Instance Management** link to display the page.
4. Select a Transaction Server instance or a Case Management Server instance that you want to shut down.
5. Click **Shut Down** to shut down the selected server instances.

Note: When a shutdown request is received by Transaction Server, all the ongoing transactions are processed, and then the shutdown request is processed.

How to Restart a Server Instance

The following topics walk you through the steps for restarting the Transaction Server and the Case Management Server instances.

On Windows

To start a server instance on Windows:

1. Log in to the computer where the instance has stopped.
2. Click the **Start** button on the desktop.
3. Navigate to **Settings > Control Panel > Administrative Tools > Services**.
4. To restart:
 - **Transaction Server instance:** Double-click **CA Risk Analytics Transaction Server** from the listed services.
 - **Case Management Server instance:** Double-click **CA Risk Analytics Case Management Server** from the listed services.
5. Click **Start** to start the service.

On UNIX-Based Platforms

To start a server instance on UNIX-based platforms:

1. Log in to the computer where the instance must be started.
2. Navigate to the following directory:

```
<install_location>/arcot/bin/
```

3. Run the following command to restart:

- **Transaction Server instance:**

```
./riskanalyticsserver start
```

- **Case Management Server instance:**

```
./casemanagementserver start
```

Managing Model and Other Server Configurations

This article covers the following topics:

- [How to Update the Risk Analytics Predictive Model](#)
- [How to Configure the Default Card Issuer Organization](#)
- [How to Configure the Default Transaction Acquirer Organization](#)
- [How to Configure Default NBIN Mapping](#)

How to Update the Risk Analytics Predictive Model

Risk Analytics offers an advanced fraud modeling capability. Based on the historical data, this modelling capability can be built and created in Risk Analytics. By using the available transaction data and system data, the model generates a score that describes the extent to which the model suspects a transaction's genuineness. This score typically ranges from 0 through 100, where the higher the number, the greater the possibility of fraud. RA can be configured to send different responses to your calling application based on this model score.

The model score is available as a part of the system parameters (as Score) while configuring out-of-the-box rules. This score can be used in conjunction with other data elements to arrive at a risk advice.

Configuring the Predictive Model

You can configure the URL and timeout parameters for the RA Predictive Model by using Administration Console.

To configure the RA Predictive Model:

1. Ensure that you are logged in as a MA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Model Configuration** section on the side-bar menu, click the **Model Configuration** link.
The Model Configuration page appears.
5. In the **Proposed Value** column, specify the parameters as described in the following table.

Parameter	Description
Predictive Model URL (primary)	The primary URL of the RA Predictive Model.
Predictive Model URL (backup)	The backup URL of the RA Predictive Model.
Connection Timeout (in milliseconds)	

Parameter	Description
	The time for which RA tries to establish a connection to the Model before timing out.
Read Timeout (in milliseconds)	The time in which Transaction Server expects a response back from the Model.
Minimum Connections	The minimum number of connections in the connection pool to connect to the Model Server.
Maximum Connections	The maximum number of connections in the connection pool to connect to the Model Server.
Score Multiplication Factor (rational number allowed)	The value by which the score returned by Model is multiplied before being used for rule evaluation.
Protocol Type	The protocol used by RA to communicate with the Model.
Server Authentication SSL	If you want to configure SSL-based communication between Transaction Server and your Model, then you must select this option.
Callout Server Root Certificate	<p>Click Browse to navigate to the location where the Callout Server Root Certificate is located. Callout Server Root Certificate must be in PEM (Base64-encoded) format.</p> <p>Note: If Server Authentication SSL is selected, then you must specify the Callout Server Root Certificate.</p>
Client Authentication SSL	<p>If you want to configure two-way SSL connection between Transaction Server and your Model, then you must select this option and ensure that the Server Authentication SSL is also selected.</p> <p>If you want to configure one-way SSL connection between Transaction Server and your model, then you must not select this option. In this case, you must ensure that the Server Authentication SSL is selected.</p> <p>If you do not want to configure any SSL-based connection, then you must not select either this option or the Server Authentication SSL option.</p>
Risk Analytics Transaction Server Certificate and Private Key	<p>Click Browse to navigate to the location where the Transaction Server Certificate and Private Key are located. Transaction Server Certificate and Private Key must be in PEM (Base64-encoded) format.</p> <p>Note: If Client Authentication SSL is selected, then you must specify the RA Transaction Server Certificate and Private Key.</p>

6. Click **Upload Model Configuration** to save the changes.

7. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure the Default Card Issuer Organization

The first six digits of the card number are known as the *Issuer Identification Number (IIN)* or *Bank Identification Number (BIN)*, and these digits identify the Card Issuer. During a transaction, RA checks whether the BIN prefix of the card used in the transaction matches the configured Issuer BIN prefixes for any organization. If a match is found, then the corresponding organization's active ruleset is used for rule evaluation. If no match is found, then the default Card Issuer organization's active ruleset is used for rule evaluation. The Master Administrator can configure the default Card Issuer organization.

Follow these steps:

1. Ensure that you are logged in as a MA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Additional Configuration** section on the side-bar menu, click the **Default Card Issuer Mapping** link.
The Default Card Issuer Mapping page appears.
5. Select the **Default Card Issuer Organization** from the drop-down list.
6. Enter values for the fields, as described in the following table:

Field	Description
Duration	Maximum time period to consider for transaction history. The duration is specified in minutes or hours, depending on how it is configured in the rule. Note: Transaction history is defined as the list of transactions for the same account (Card Number or PAN) over ATM and POS channels in reverse chronological sequence.
Threshold Amount	Maximum limit on the transaction amount for a card, defined in the organizations' base currency.
Transaction Count	Total number of transactions to consider for transaction history.

7. Click **Save** to save your configuration changes.

8. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure the Default Transaction Acquirer Organization

An *Institution Identification Code (IIC)*, also referred to as *Acquirer ID*, is assigned to each Acquirer institution that participates in the global financial network. During a transaction, RA checks whether the Acquirer ID of the Transaction Acquirer involved in the financial transaction matches the configured Acquirer IDs for any organization. If a match is found, then the corresponding organization's active ruleset is used for rule evaluation. If no match is found, then the default Transaction Acquirer organization's active ruleset is used for rule evaluation. The Master Administrator can configure the default Transaction Acquirer organization.

To configure the default Transaction Acquirer organization:

1. Ensure that you are logged in as a MA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Additional Configuration** section on the side-bar menu, click the **Default Transaction Acquirer Mapping** link.
The Default Transaction Acquirer Mapping page appears.
5. Select the **Default Transaction Acquirer Organization** from the drop-down list.
6. Click **Save** to save your configuration changes.
7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure Default NBIN Mapping

National Bank Identification Number (NBIN) is used to identify banks in the context of Mobile Remittances for routing transactions by Interbank Payment Service (IMPS). A 4-digit unique identification number is assigned to the member banks participating in IMPS. The 4-digit NBIN and 3-digit Mobile Account Selector (MAS) together make the 7-digit Mobile Money Identifier (MMID), which is issued by the bank to customers availing IMPS.

During a transaction, RA checks whether the NBIN of the organization participating in the transaction matches the configured NBIN for any organization. If a match is found, then the corresponding organization's active ruleset is used for rule evaluation. If no match is found, then the default NBIN organization's active ruleset is used for rule evaluation. The Master Administrator can configure the default NBIN organization.

To configure the default NBIN organization:

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

4. Under the **Additional Configuration** section on the side-bar menu, click the **Default NBIN Mapping** link.
The NBIN to Organization Mapping page appears.
5. Select the **Default NBIN Organization** from the drop-down list.
6. Click **Save** to save your configuration changes.
7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Managing Global Configurations

RA configurations are of two types:

- **System-level configurations:** These configurations are applicable to *all* organizations, unless overridden for a specific organization by configuring the same under the **Organizations** tab. These configurations are made under the **Services and Server Configurations** tab, and any changes made under this tab are available to all organizations.
- **Organization-level configurations:** These configurations are made to a specific organization, but can be used by other organizations in the scope of the administrator who made these changes. However, they are not automatically available; they need to be specifically applied to other organizations. An example of this type of configuration is a Ruleset template created at the global level. The rulesets can optionally be used as a starting point when creating a ruleset for an organizations.

Notes on System- and Organization-Level Configurations

- Although system-level configurations are available to all organizations, they cannot be used as-is at the organization level. For example, even if you configure a Untrusted IP Check rule at the global level, individual organizations need to configure this rule either by copying from the global rule.
- Although you can change the default rule configurations individually for every organization in the system, most of the organizations might be using the same configuration settings repeatedly. Also, setting rule configurations for individual organizations can be a cumbersome task if a large number of organizations are configured. In this case, you might want to set the global configurations for the rules so that Organization Administrators (OAs) do not need to specify the same setting every time.
- The changes you make to the configuration globally or at the organization level are *not* applied automatically. You need to refresh all server instances to apply these configuration changes.

This article covers the following topics:

- [How to Configure Global Settings](#)
- [How to Configure Organization-Level Settings](#)

How to Configure Global Settings

To configure settings at global-level:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Risk Analytics** option on the submenu of the tab.
4. Configure the required setting.

How to Configure Organization-Level Settings

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

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the `<ORGANIZATION_NAME>` link for the required organization.
The Organization Information page appears.
6. Activate the **Risk Engine** tab.
The organization-specific configuration links are displayed in the tasks pane.
7. Configure the required setting.

Managing Organizations

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

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

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

- [How to Create and Activate an Organization](#)
- [How to Create an Org Family](#)
- [How to Search for an Organization](#)
- [How to Update an Organization](#)
- [How to Upload Users and User Accounts in Bulk to an Organization](#)

- [How to View the Status of the Bulk Data Upload Request](#)
- [How to Refresh the Organization Cache](#)
- [How to Deactivate an Organization](#)
- [How to Activate an Organization](#)
- [How to Activate an Organization that is in Initial State](#)
- [How to Delete an Organization](#)

Note: In addition to the preceding list of tasks related to organization management, OAs can also manage organization-specific configurations.

How to Create and Activate an Organization

You can create an organization either in the RA repository or in your existing LDAP-based directory server implementations, such as Microsoft Active Directory, SunOne Directory Server, or CA Directory Server.

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

Based on your implementation, this topic guides you through the procedure used for:

- [How to Create an Organization in Arcot Repository](#)
- [How to Create an Organization in LDAP Repository](#)

Privileges Required

To create and activate an organization, you must ensure that you have the appropriate privileges to do so. Only MA and GAs with scope can create and activate all organizations.

How to Create an Organization in Arcot Repository

To create an organization in the Arcot repository:

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

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create.

Field	Description
	<p>NOTE: You have to specify this value to log in to this organization, <i>not</i> the Display Name of the organization.</p>
Display Name	<p>Enter a unique descriptive name for the organization.</p> <p>NOTE: This name appears on all other Administration Console pages and reports.</p>
Description	<p>Provide a description for the administrators who will manage this organization.</p> <p>NOTE: You can provide additional details for later reference for the organization by using this field.</p>
Administrator Authentication Mechanism	<p>Select the mechanism that will be used to authenticate administrators who belong to this organization.</p> <p>Administration Console supports the following types of authentication mechanisms:</p> <p>Basic User Password This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators can log in to the console by specifying their user ID and password.</p> <p>LDAP User Password This 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 console.</p> <p>WebFort User Password This is the WebFort user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by the WebFort Server. To use this mechanism, you must have CA Arcot WebFort 7.0 installed and configured. Refer to the <i>CA Arcot WebFort 7.0 Installation and Deployment Guide</i> for detailed information about how to deploy WebFort.</p>
Key Label Configuration	
<p>RA enables you to use hardware- or software-based encryption of your sensitive data. You can choose the encryption mode by using the <code>arcotcommon.ini</code> configuration file. For more information, see "HSM Encryption Settings" in "Configuration Files and Options" in the <i>CA Risk Analytics Installation and Deployment Guide</i>.</p>	

Field	Description
<p>Irrespective of hardware or software encryption, all CA Arcot products use Global Key Label for encrypting user and organization data.</p> <p>If you are using hardware encryption, then this label serves only as a reference (or pointer) to the actual 3DES key stored in the HSM device. In this case, the key label that you specify must match the HSM key label. However, in the case of software-based encryption, this label acts as the key.</p>	
Use Global Key	This option is selected by default. Deselect this option if you want to override the Global Key Label you specified in the bootstrap process and specify a new key label that will be used for encrypting organization-specific data.
Key Label	If you deselected the Use Global Key option, then specify the new key label that you want to use for the organization.
Storage Type	This option indicates whether the encryption key is stored in the database (Software) or the HSM (Hardware).
Localization Configuration	
Use Global Configuration	Select this option to use the localization parameters that are configured at the global level.
Date Time Format	If you deselected the Use Global Configuration option, then specify the Date Time format that you want to use for this organization.
Preferred Locale	If you deselected the Use Global Configuration option, then select a preferred locale for this organization.
User Data Location	
Repository Type	Select Arcot Database . By specifying this option, the user and administrator details for the new organization will be stored in the RDBMS repository supported by RA.
Custom Attributes	
Use this section to provide additional information specific to the organization you are creating.	
Name	Name of the custom attribute.
Value	Value of the custom attribute.

From this release, risk evaluation on an incoming transaction is performed based on multiple perspectives, such as Issuer, Acquirer, and Beneficiary. To achieve this, an organization-level flag is used to determine whether the organization is an Issuer, Acquirer, or Beneficiary. To identify an organization as an Acquirer, set the custom attribute **SUPPORTED_PERSPECTIVES** to **2**.

An organization is identified as a Beneficiary organization if it has the IMPS channel associated with it.

Note: If no attribute value is specified, the organization is considered an Issuer Organization. All existing organizations are assumed to be Issuer organizations.

5. Click **Next**.

The Select Attribute(s) for Encryption page appears.

6. In the **Attribute(s) for Encryption** section, do one of the following:

- Select **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration.
- Select the attributes that you want to encrypt from the **Available Attributes for Encryption** list and move them to the **Attributes Selected for Encryption** list.
Click the > or < buttons to move selected attributes to the desired list. You can also click the >> or << buttons to move all attributes to the desired lists.

7. Click **Next**.

The Add Administrators page appears.

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

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

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

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

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

9. Click **Next** to proceed.

The Configure Account Type page appears.

Note:

- This page is not displayed if you have not created any account types.
- Global account types will be selected by default.

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

11. Click **Next** to proceed.

The Configure Account Custom Attributes page appears.

Note: This page is not displayed if you did not select any account types on the previous page.

12. Provide **Custom Attributes** for your **Account Type**, and click **Next**.

The Configure Email/Telephone Type page appears.

13. Specify the mandatory and optional email address and telephone numbers the user must provide.

14. Click **Skip** to use the email and telephone types configured at the system level and move to the next page, or click **Save** to save your changes.

The Activate Organization page appears.

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

A message box appears.

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

Note: If you do not choose to activate the organization, the organization is created in Initial state. You can activate the organization later. For instructions to do so, see ["How to Activate an Organization That is in Initial State"](#).

17. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

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

How to Create an Organization in LDAP Repository

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

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

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. NOTE: You can use Administration Console to log in to this organization, by specifying this value, <i>not</i> the Display Name of the organization.
Display Name	Enter a unique descriptive name for the organization. NOTE: This name appears on all other Administration Console pages and reports.
Description	Provide a description for the administrators who will manage this organization.

Field	Description
	<p>NOTE: You can provide additional details for later reference for the organization by using this field.</p>
Administrator Authentication Mechanism	<p>Select the mechanism that will be used to authenticate administrators who belong to this organization.</p> <p>Administration Console supports the following two types of authentication mechanisms:</p> <p>Basic User Password This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators can log in to the console by specifying their ID and plain text password.</p> <p>LDAP User Password This 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 console.</p> <p>WebFort User Password This is the WebFort user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by WebFort Server. To use this mechanism, you must have Arcot WebFort 7.0 installed and configured. Refer to the <i>CA Arcot WebFort 7.0 Installation and Deployment Guide</i> for detailed information about how to deploy WebFort.</p>
Key Label Configuration	
Use Global Key	This option is selected by default. Deselect this option if you want to override the Global Key Label you specified in the bootstrap process and specify a new key label to encrypt organization-specific data.
Key Label	If you deselected the Use Global Key option, then specify the new key label that you want to use for the organization.
Storage Type	This option indicates whether the encryption key is stored in the database (Software) or the HSM (Hardware).
Localization Configuration	
Use Global Configuration	Select this option to use the localization parameters that are configured at the global level.
Date Time Format	

Field	Description
	If you deselected the Use Global Configuration option, then specify the Date Time format that you want to use for this organization.
Preferred Locale	If you deselected the Use Global Configuration option, then select a preferred locale for this organization.
User Data Location	
Repository Type	Select Enterprise LDAP . By specifying this option, the user details for the new organization will be stored in the LDAP repository that you will specify on the next page.
Custom Attributes	
Name	Name of the custom attribute.
Value	Value of the custom attribute.

From this release, risk evaluation on an incoming transaction is performed based on multiple perspectives, such as Issuer, Acquirer, and Beneficiary. To achieve this, an organization-level flag is used to determine whether the organization is an Issuer, Acquirer, or Beneficiary. To identify an organization as an Acquirer, set the custom attribute **SUPPORTED_PERSPECTIVES** to **2**.

An organization is identified as a Beneficiary organization if it has the IMPS channel associated with it.

Note: If no attribute value is specified, the organization is considered an Issuer Organization. All existing organizations are assumed to be Issuer organizations.

5. Click **Next**.

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

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

Field	Description
Host Name	Enter the host name of the system where the LDAP repository is available.
Port Number	Enter the port number on which the LDAP repository service is listening.
Schema Name	Specify the LDAP schema used by the LDAP repository. This schema specifies the types of objects that an LDAP repository can contain, and specifies the mandatory and optional attributes of each object type. Typically, the schema name for Active Directory is user and for SunOne Directory and CA Directory Server, it is inetorgperson.
Base Distinguished Name	Enter the base Distinguished Name of the LDAP repository. This value indicates the starting node in the LDAP hierarchy to search in the LDAP repository.

Field	Description
	<p>For example, to search or retrieve a user with a DN of cn=rob laurie, ou=sunnyvale, o=arcot, c=us, you must specify the base DN as the following:</p> <p>ou=sunnyvale, o=arcot, c=us</p> <p>Note: Typically, this field is case sensitive and searches all subnodes under the provided base DN.</p>
Redirect Schema Name	<p>Specify the name of the schema that provides the definition of the "<i>member</i>" attribute. You can search for users in the LDAP repository by using the Base DN defined for an organization. But this search returns only the users who belong to a specific Organization Unit (OU). An LDAP administrator might want to create a group of users who belong to different Organization Units for controlling access to an entire group, and might want to search for users from different groups. When the administrator creates groups, user node DNs are stored in a "member" attribute within the group node. By default, UDS does not allow search and DN resolution based on attribute values. Redirection enables you to search for users who belong to different groups within LDAP, based on specific attribute values for a particular node.</p> <p>Typically, the redirect schema names are as follows:</p> <p>Active Directory: group</p> <p>SunOne Directory: groupofuniquenames</p> <p>CA Directory Server: groupOfUniqueNames</p>
Connection Type	<p>Select the type of connection that you want to use between Administration Console and the LDAP repository. Supported types are:</p> <p>TCP</p> <p>One-way SSL</p> <p>Two-way SSL</p>
Login Name	<p>Enter the complete distinguished name of the LDAP repository user who has the privilege to log in to repository sever and manage the Base Distinguished Name.</p> <p>For example,</p> <p>uid=gt,dc=arcot,dc=com</p>

Field	Description
Login Password	Enter the password of the user provided in the Login Name.
Server Trusted Root Certificate	Enter the path for the trusted root certificate who issued the SSL certificate to the LDAP server by using the Browse button, if One-way SSL or Two-way SSL option is selected.
Client Key Store Path	Enter the path for the key store that contains the client certificate and the corresponding key by using the Browse button, if the Two-way SSL option is selected. Note: You must upload either PKCS#12 or JKS key store type.
Client Key Store Password	Enter the password for the client key store, if the Two-way SSL option is selected.

7. Click **Next** to proceed.

The page to map the repository attributes appears.

8. On this page:

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

Important! Mapping of the *UserName* attribute is compulsory. Ensure that you map the *UserName* attribute to an LDAP attribute that uniquely identifies the user. If you are using Active Directory, then map *UserName* to *sAMAccountName*. If you are using SunOne Directory Server, then map *UserName* to *uid*. If you are using CA Directory Server, then map *UserName* to *cn*.

For Active Directory, you must map *STATUS* to *userAccountControl*.

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

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

The attributes that you have mapped will be moved to the **Mapped Attributes** list. If required, you can unmap the attributes. If you want to unmap a single attribute at a time, then select the attribute and click **Unmap**. However, if you want to clear the **Mapped Attribute** list, then click **Reset** to unmap all the mapped attributes. You cannot unmap the *UserName* attribute after you have activated the organization.

- If you specified the **Redirect Schema Name** in the previous page, you must select the search attribute from the **Redirect Search Attribute** list. Typically, the attributes are as follows:
 - Active Directory: *member*
 - SunOne Directory: *uniquemember*
 - CA Directory Server: *uniqueMember*

9. Click **Next** to proceed.

The Select Attribute(s) for Encryption page appears.

10. In the **Attribute(s) for Encryption** section, do one of the following:

- Select **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration.
- Select the attributes that you want to encrypt from the **Attributes Available for encryption** list and move them to the **Attributes Selected for encryption** list.
Click the > or < buttons to move selected attributes to the desired list. You can also click the >> or << buttons to move all attributes to the desired lists.

11. Click **Next**.

The Add Administrators page appears.

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

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

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

13. Click **Next** to proceed.

The Configure Account Type page appears.

Note: This page is not displayed if you have not created any account types.

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

15. Click **Next** to proceed.

The Configure Account Custom Attributes page appears.

Note: This page is not displayed if you did not select any account types on the previous page.

16. Provide **Custom Attributes** for your **Account Type**, and click **Next**.

The Activate Organization page appears.

Note: The UserName mapping *cannot* be changed or updated after the organization is activated.

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

The warning message appears.

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

19. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

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

How to Create an Org Family

From this release, you can group organizations under a portfolio referred to as an Org Family. This enables organizations to share list data and rules run across the family of organizations.

To create an Org Family, run the following statement:

```
INSERT INTO ARRFORGFAMILY (ORGNAME, ORGFAMILYNAME) VALUES (<ORGNAME>, <FAMILYNAME>);
```

Example:

```
INSERT INTO ARRFORGFAMILY (ORGNAME, ORGFAMILYNAME) VALUES ('FAMILYORG1', 'FAMILY1');
INSERT INTO ARRFORGFAMILY (ORGNAME, ORGFAMILYNAME) VALUES ('FAMILYORG2', 'FAMILY1');
COMMIT;
```

How to Search for an Organization

You can search for organizations by their display name and status. To search for the organization:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Enter the partial or complete information of the required organization. You can select the following options to broaden your search:

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

4. Click **Search** to display the page with all the matches for the specified criteria.

Privileges Required

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

How to Update an Organization

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

- **Organization information** that includes organization display name, description, and status, the administrators that manage the organization, account types assigned to the organization, email/telephone types configured, and attribute encryption set ("[For Basic Organization Configurations](#)")
- **RA-specific configurations** for the organization that include credential profiles, authentication policies, extensible configurations, and the assigned default configurations.

Privileges Required

To update an organization, you must ensure that you have the appropriate privileges and scope. The MA can update all organizations. GAs and OAs can update the information for all organizations in their scope.

For Basic Organization Configurations

To update the basic organization information:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
5. In the **Organization Details** section, edit the required fields (**Display Name** and **Description**).
6. Edit the **Administrator Authentication Mechanism**, if required.
You can edit the authentication mechanism only if there no administrators exist for this organization.
7. In the **Localization Configuration** section, you can do one of the following:
 - a. Choose to **Use Global Configuration**.
 - b. Edit the **Date Time Format** and **Preferred Locale**.
8. In the **Custom Attributes** section, edit the **Name** and **Value** fields, if required.
9. Click **Next** to proceed with additional configurations:
 - If the organization was created in the **Arcot Repository**, then do the following:

- a. On the Select Attribute(s) for Encryption page, **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration, or select the attributes that you want to encrypt from the **Available Attributes for Encryption** list to the **Attributes Selected for Encryption** list, and click **Next**. You cannot update attributes if users have already been created in the organization.
 - b. On the Update Administrators page, update the administrators who will manage the organization, and click **Next**.
 - c. On the Configure Account Type page, configure the account types by moving them from the **Available** list to the **Selected** list and click **Next**. You cannot deselect global account types.
 - d. On the Configure Account Custom Attributes page, add custom attributes for the accounts and click **Next**.
 - e. On the Configure Email/Telephone Type page, configure the mandatory and optional Email address and Telephone Type for the users, and click **Save** to complete the process.
- If the organization was created **in the LDAP repository**, then Edit Organization page appears. To update the organization details:
 - a. Update the fields, as required, and click **Next** to display the page to edit the Repository Attribute Mappings.
 - b. Except for the UserName mapping, you can edit the other mappings. Click **Next** to display the Select Attribute(s) for Encryption page.
 - c. On the Select Attribute(s) for Encryption page, **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration, or select the attributes that you want to encrypt from the **Available Attributes for Encryption** list to the **Attributes Selected for encryption** list, and click **Next**.
 - d. You cannot update the attributes if users have already been created in the organization. In the case of LDAP, even a simple search operation for users in the LDAP repository registers the users in the database. So, you cannot update the attributes if you have searched for users in the LDAP repository.
 - e. On the Update Administrators page, update the administrators who will manage the organization and click **Next**.
 - f. On the Configure Account Type page, configure the account types by moving them from the **Available** list to the **Selected** list and click **Update** to save your changes and complete the process. You cannot deselect global account types.
10. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

For Risk Analytics-Specific Configurations

To update the RA configurations of an organization:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.

3. Enter the complete or partial information of the organization you want to search and click the **Search** button to display a list of organizations matching the search criteria.
4. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization to display the Organization Information page appears.
5. Activate the **Risk Engine** tab to display the links for RA configurations in the task panel.

How to Upload Users and User Accounts in Bulk to an Organization

RA allows you to upload users and user accounts in bulk using the Administration Console. For this purpose, you need a comma-separated value (CSV) input file that contains the information for the multiple users and accounts that you want to upload.

Information Required for Uploading Users in Bulk

The first line in the CSV input file to upload users *must* be as follows:

```
#UserID,fName,mName,lName,status,pam,pamURL,EmailAddr,telephoneNumber,INFOLIST#
```

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

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

- The csv file should have one header starting and ending with #. All the other field names should be provided between these # symbols.
- Only the UserID entry is mandatory. The other entries are optional.
- If the user you are trying to upload already exists, the user details are updated.
- You can provide up to five email addresses and five telephone numbers. In this case, you must specify the header, as follows:

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

The entries in the file are described in the following table

Entry	Description
UserID	The unique ID of the user.
fName	The first name of the user.
mName	The middle name of the user.
lName	The last name of the user.
status	The status of the user. Possible values are: INITIAL ACTIVE
pam	The personal authentication message

Entry	Description
pamURL	The URL where the user's personal authentication message image is available
EmailAddr	The contact email ID of the user.
telephoneNumber	The complete phone number of the user with the international code. For example, US phone numbers should start with 1.
INFOLIST	Additional information about the user. Values must be separated by semi-colons. For example: age=25;favsport=cricket

A sample file, for example, can contain:

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

Information Required for Uploading User Accounts in Bulk

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

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,accountIDAttribute3,customAttr1,customAttr2,customAttr3,customAttr4,customAttr5,customAttr6,customAttr7,customAttr8,customAttr9,customAttr10#
```

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

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

- Only the UserID, accountType, and accountID entries are mandatory. The other entries are optional.
- You must have created the user in the system.
- You must have created the account type and assigned it to the organization.
- You must have created custom attributes for the account type.
- You can provide up to 10 custom attributes for an account type.

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

Entry	Description
UserID	The unique ID of the user.
accountType	The account type associated with the accountID.
accountID	The alternate ID of the user.
status	The status of the account ID. Possible values are: [0-9]: INITIAL

Entry	Description
	[10-19]: ACTIVE
	[20-29]: INACTIVE
accountIDAttribute1	Attribute of the accountID. You can provide up to a maximum of three account ID attributes.
customAttr1	Custom attribute for the user account.

Sample File Entry

A sample file, for example, can contain:

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,accountIDAttribute3,customAttr1,customAttr2#
prush,ONLINE_BANKING,OB_ID1,10,login,password,image,chicago,music
jhume,SAVINGS,SA_ID1,10,interest,deposit,check,florida,soccer
```

How to Upload Users and Accounts in Bulk

To upload multiple users and user accounts in the RA database:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Select the organization to which you want to upload users and user accounts in bulk.
5. Under the **Basic Organization Information** section, click the **Bulk Upload** link to display the Bulk Data Upload page.
6. In the **Bulk Upload** section:
 - a. Select **Upload User Accounts** or **Upload Users** from the **Bulk Upload Operation** drop-down list.
 - b. Click **Browse** to navigate to the required csv file that contains the user account or user entries.
 - c. Provide a **Description** for the operation.
7. Click **Upload** to upload user accounts or users in bulk.
8. After the operation completes, you will see a Request ID in the message.
9. **(IMPORTANT)** Carefully note the Request ID.
You will need it to view the status of the bulk data upload operation.

Privileges Required

To upload multiple users and user accounts to an organization, you must ensure that you have the appropriate privileges and scope. The MA can do this for all organizations. GAs and OAs can perform this task for all organizations in their scope.

How to View the Status of the Bulk Data Upload Request

To view the status of the bulk data upload request:

1. Ensure that you are logged in with the required privileges and scope to perform this operation.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Select the organization for which you want to view the status of the bulk upload request.
5. Under the **Basic Organization Information** section, click the **View Bulk Requests** link to display the Search Bulk Requests page.
6. In the Search Bulk Requests page:
 - a. Enter the Request ID that you noted down earlier in Step 10 in "[How to Upload Users and User Accounts in Bulk to an Organization](#)".
or
 - b. Select a **Status** based on which you want to view the bulk request.
or
 - c. Select an **Operation**, depending on whether you want to view **Upload Users** or **Upload User Accounts** requests.
7. Click **Search** to display the table.
8. In case of failure, click the **Request ID** link to get more information about the bulk request.
9. Click the **No. of failed operations** link to view the reason why the operation failed.

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

Privileges Required

To view the status of the bulk data upload request for an organization, you must ensure that you have the appropriate privileges and scope. The MA can do this for all organizations. GAs and OAs can perform this task for all organizations in their scope.

How to Refresh the Organization Cache

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

To refresh the organization cache:

1. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Select the organizations whose cache you want to refresh.
5. Click **Refresh Cache**.
6. Click **OK** in the dialog box to confirm your cache refresh request.
A message with a Request ID for the current cache refresh request is displayed. You can check the status of your cache refresh request by clicking the **Check Cache Refresh Status** link and selecting this **Request ID**.

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

Privileges Required

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

How to Deactivate an Organization

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

To deactivate an organization:

1. Ensure that you are logged in with the required privileges and scope to deactivate the organization.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Select one or more organizations that you want to deactivate.

5. Click **Deactivate** to disable the selected organizations.
A message box appears.
6. Click **OK** to confirm the deactivation.
7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Privileges Required

To deactivate an organization, you must ensure that you have the appropriate privileges and scope. The MA can deactivate all organizations. GAs and OAs can deactivate all organizations in their scope.

How to Activate an Organization

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

To activate a deactivated organization:

1. Ensure that you are logged in with the required privileges and scope to activate the organization.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Select one or more organizations that you want to activate again.
5. Click **Activate** to activate the selected organizations.
A message box appears.
6. Click **OK** to confirm the activation.
7. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Privileges Required

To activate an organization, you must ensure that you have the appropriate privileges and scope. The MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

How to Activate an Organization that is in Initial State

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

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

To activate an organization in Initial state:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Enter the partial or complete information of the required organization and select the **Initial** option.
4. Click **Search** to display the page with all the matches for the specified criteria.
5. Select the organizations that you want to activate.
6. Click **Activate** to enable the selected organizations. A message box appears.
7. Click **OK** to confirm the activation.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

Privileges Required

To activate an organization in Initial state, you must ensure that you have the appropriate privileges and scope. MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

How to Delete an Organization

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

To delete an organization:

1. Ensure that you are logged in with the required privileges and scope to delete the organization.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Select one or more organizations that you want to delete, and click **Delete**.
A message box appears.
5. Click **OK** to confirm the deletion.

Privileges Required

To delete an organization, you must ensure that you have the appropriate privileges and scope. The MA can delete all organizations. GAs and OAs can delete all organizations in their scope.

Managing Administrators

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

See [Supported Roles](#) for information about supported administrative roles. This article covers the following administrator management operations:

- [How to Create an Administrator](#)
- [How to Change Profile Information for an Administrator](#)
- [How to Search for an Administrator](#)
- [How to Update Administrator Information](#)
- [How to Demote an Administrator to User Role](#)
- [How to Configure Account IDs for Administrators](#)
- [How to Deactivate an Administrator Account](#)
- [How to Temporarily Deactivate an Administrator](#)
- [How to Activate an Administrator Account](#)
- [How to Delete an Administrator Account](#)

Note: In addition to the operations discussed in this article, the Master Administrator has the privilege to create "Custom Roles" that are derived from the existing default roles supported by RA.

How to Create an Administrator

To create an administrator:

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

4. In the **Administrator Details** section, enter the details of the administrator. The following table explains the fields on this page.

Input	Description
User Name	The unique user name for the administrator.
Organization	The display name of the organization to which the administrator belongs. Note: This is <i>not</i> the organization that this administrator will manage.
First Name	The first name of the administrator.
Middle Name	The middle name, if any, of the administrator.
(optional)	
Last Name	The last name of the administrator.

5. In the **Email Address(es)** section, enter the email address of the administrator for the email types configured for the organization.

6. In the **Telephone Number(s)** section, enter the phone number to contact the administrator.

If multiple telephone types are configured, you *must* enter values for all the mandatory telephone types.

7. In the **Custom Attributes** section, enter the **Name** and **Value** of any attributes you want to add, such as office location.

8. Click **Next** to proceed.

The next page appears.

9. On this page:

Specify the role of the new administrator from the **Role** drop-down list.

- In the **Set Password** section, set and confirm the password for the administrator.
- In the **Manages** section, select the organizations that the administrator will have scope on, and perform one of the following:
 - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.
or
 - Select the required organizations from the **Available Organizations** list and click the > button to add these organization to the **Selected Organizations** list.

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

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

11. Communicate the new password to the administrator.

Privileges Required

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

- The MA can create all other types of administrators.
- GAs can create the following *within* their scope:
 - Other GAs
 - OAs
 - UAs
- OAs can create the following *within* their scope:
 - Other OAs
 - UAs

How to Change Profile Information for an Administrator

The profile information for an account includes:

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

Note: An administrator can change their account's profile information at any time. To change the information for any other administrative account, see [How to Update Administrator Information](#).

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

1. Ensure that you are logged in to *your account*.
2. In the **Header** frame, click the <ADMINISTRATORNAME> link to display the My Profile page.
3. Edit the required settings in the sections on this page:
 - a. Edit the fields in the **Personal Information** section, as needed.
 - b. If you want to change the current password, then in the **Change Password** section, enter the **Current Password**, and specify a new password in the **New Password** and **Confirm Password** fields.
 - c. In the **Administrator Preferences** section:

- Select the **Enable Preferred Organization** option, and select an organization from the **Preferred Organization** list. This organization will be selected for all administrator-related tasks that you perform from now on.
- Specify the preferred **Date Time Format**.
- Select the preferred **Locale** for your instance of Administration Console.
- Select the required option from the **Time Zone** list.

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

Privileges Required

Only the administrator whose account information is being updated can change this information.

How to Search for an Administrator

To search for an administrator:

1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Users and Administrators** tab.
3. Specify the search criteria to display the list of administrators. You can:
 - Search for administrators by specifying the partial or complete information of the administrator in the fields on this page.
 - Search for administrators by specifying the organization's Display Name.
 - Search for administrators by not specifying any criteria and just clicking **Search**.
 - Click the **Advanced Search** link to display the Advanced Search page to search for the required administrators by specifying their Status or Role.

Note: In the **User Status** section, you can search for **Current Users** based on the user status (Active, Inactive, or Initial) or you can search for **Deleted Users**.

4. Select **Enable search by Accounts** if you want to search for administrators based on account IDs also.
5. Specify the required details of the administrators and click **Search**.
A list of administrators matching the search criteria appears.

Privileges Required

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

How to Update Administrator Information

To update administrator information:

1. Ensure that you are logged in with the required privileges to update the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the corresponding page.
4. Enter the partial or complete information of the administrator whose account you want to update and click **Search**.
A list of administrators matching the search criteria appears.
5. Click the *<user name>* link of the administrator whose account you want to edit.
The Basic User Information page appears.

Note: This page also displays the **User Account Information (Account Type, AccountID, and Status)** if any account type was configured.

6. Click **Edit** to change the administrator information on this page.
In the **User Details** section, edit the required fields (**First Name**, **Middle Name**, and **Last Name**).
7. In the **Email Address(es)** section, edit the email addresses for the email types configured for the organization.
8. In the **Telephone Number(s)** section, edit the telephone numbers for the telephone types configured for the organization.
9. In the **Custom Attributes** section, edit the **Name** and **Value** of the custom attributes.
10. You can either click **Save** to save the changes made and return to the User Information page, *or* you can click **Next** to proceed with additional configurations.

Note: If you don't see a **Next** button, it means that no account type has been configured for the organization. In this case, click **Update Administrator Details** and go to Step 14.

If you click **Next**, then the User Account page appears.

11. In the **User Account** section:
 - Edit the **Account Type** and **Status** fields.
 - Expand **Advanced Attributes** to add **AccountID Attributes** for the account ID.

Note: If this is the first account ID you are creating, you must click **Add** to add an account ID before you can update it. For more information about adding an account ID, see [Create Account IDs](#).

12. Click **Update Administrator Details**.
The **Update Administrator** page appears.

13. In the **Role** section on this page, change the role of the administrator by using the **Role** drop-down list.
14. In the **Set Password** section:
 - Set the **Password** and **Confirm Password** for the administrator.
 - Select **Lock** to lock the administrator's credentials for the **Credential Lock Period**, which you can specify in the **From** and **To** fields.
15. In the **Manages** section, select the organizations that the administrator will manage. You can also remove the organization from the administrator's scope by moving the specific organization from **Selected Organizations** to **Available Organizations**.
16. Click **Save** to save the updates.

Privileges Required

To update administrator information, you must ensure that you have the appropriate privileges and scope. The MA can update any administrator. The GAs can update all the administrators (including other GAs) in their scope, *except* the MA account. The OAs can update all other OAs and UAs in their purview, while UAs can only update their peers within their scope.

How to Demote an Administrator to User Role

You can change the role of an administrator to an user. For example, an administrator in the IT department might have moved to the Engineering department. In this case, we would want to retain the user details, but remove the administrative privileges for the user.

To demote an administrator to a user:

1. Perform Step 1 to Step 13, as described [How to Update Administrator Information](#). The Update Administrator page appears.
2. On the Update Administrator page, click **Change Role to User**.
3. Click **OK** in the confirmation dialog box that appears.
4. You get the following message:
Successfully demoted the administrator to user.

Privileges Required

To update administrator information, you must ensure that you have the appropriate privileges and scope. The MA can update any administrator. The GAs can update all the administrators (including other GAs) in their scope, *except* the MA account. The OAs can update all other OAs and UAs in their purview, while UAs can only update their peers within their scope.

How to Configure Account IDs for Administrators

In addition to the user name, an *account ID* is an alternate method to uniquely identify a user in RA system. After you have configured the account types that your organization will use, you can associate one account ID per user for any of these account types. For more information about account types, see [Configuring the Account Type](#).

Privileges Required

To configure an account ID for an account type, you must ensure that you have the appropriate privileges and scope to update the user account. The MA can update any user account. The GAs can update all user accounts in their scope. The OAs and UAs can update the user accounts in their purview.

How to Create Account IDs

To create an account ID:

1. Ensure that you are logged in with the required privileges and scope to update the administrator information.
 2. Activate the **Users and Administrators** tab.
 3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
 4. Enter the partial or complete information of the administrator whose account you want to update and click **Search**.
A list of administrators matching the search criteria appears.
 5. Click the *<user name>* link of the administrator whose account you want to edit.
The Basic User Information page appears.
 6. Click **Edit** to open the Update Administrator page.
 7. Click **Next** to display the User Account page.
 8. Select the **Account Type** for which you want to add the account ID.
 9. Specify the unique **AccountID** in the text box.
This combination of account type and account ID will be used to identify the user in addition to the user name.
 10. Select the **Status** of the user account from the drop-down list.
 11. If required, expand the **Advanced Attributes** section, and do the following:
 - Provide attributes for the account ID you are creating.
- Note:** You can specify up to a maximum of three account ID attributes for any account ID.
12. Click **Add** to add the account ID.

How to Update Account IDs

Note: You cannot change the account ID once it is created. You can only change the status of the user account and add or delete account ID attributes and custom attributes.

To update an account ID:

1. Complete Step 1 through Step 7 in [Create Account IDs](#) to display the User Account page.

2. Select the **Account Type** for which you want to update the account ID information.
3. If required, change the **Status** of the user account from the drop-down list.
4. If required, expand the **Advanced Attributes** section, and provide attributes for the account ID you are creating and custom attributes, if any.
5. Click **Update** to save your changes.

How to Delete Account IDs

To delete an account ID:

1. Complete Step 1 through Step 7 in [Create Account IDs](#) to display the User Account page.
2. Select the **Account Type** for which you want to delete the account ID.
3. Click **Delete** to delete the account ID.

How to Deactivate an Administrator Account

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

To deactivate an administrative account:

1. Ensure that you are logged in with the required privileges to deactivate the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator whose account you want to deactivate and click **Search**.
You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).
The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators you want to deactivate.
6. Click **Deactivate** to deactivate the selected administrator.

Privileges Required

To deactivate an administrator, you must ensure that you have the appropriate privileges and scope. The MA can deactivate any administrator, while GAs can deactivate all administrators (including other GAs) in their scope, *except* the MA account. The OAs can deactivate all other OAs and the UAs in their purview, while UAs can only deactivate their peers within their scope.

How to Temporarily Deactivate an Administrator

Temporarily deactivating the administrator differs from *deactivating* the administrator (See [How to Deactivate an Administrator](#)). When you temporarily deactivate the administrator, the administrator is automatically activated when the end of the lock period is reached. But when you deactivate an administrator, you must manually activate them again whenever you want to provide access to them.

To temporarily deactivate an administrator, you must specify the **Start Lock Date** and **End Lock Date** for the period that you want the administrator to be locked. When the **End Lock Date** is reached, the administrator is automatically activated.

To temporarily deactivate an administrator:

1. Ensure that you are logged in with the required privileges to deactivate the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator whose account you want to deactivate and click **Search**.
You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).
The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators you want to deactivate temporarily.
6. Click **Deactivate Temporarily**.
The Deactivate User Temporarily dialog box appears.
7. In the **Starting From** section, select the start lock **Date** and the **Time**.
8. In the **To** section, select the end lock **Date** and the **Time**.
9. Click **Save** to save your changes.

Note: If you do not specify any value for the **Starting From** fields, the account is locked from the current time. If you do not specify an end lock **Date**, the account is locked forever.

Privileges Required

To temporarily deactivate an administrator, you must ensure that you have the appropriate privileges and scope. The MA can deactivate any administrator, while GAs can deactivate all administrators (including other GAs) in their scope, *except* the MA account. The OAs can deactivate all other OAs and the UAs in their purview, while UAs can only deactivate their peers within their scope.

How to Activate an Administrator Account

You might need to activate a deactivated administrator. For example, you might deactivate an administrator if the administrator is on long vacation. This helps prevent unauthorized access to that administrator information.

You cannot search directly for the deactivated administrators by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You *must* perform an **Advanced Search** for such administrators and use the **Inactive** option in the **Current Users** section to search.

To activate an administrator account:

1. Ensure that you are logged in with the required privileges to activate the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).
The Advanced Search page appears.
5. Enter the partial or complete information of the administrator in the **User Details** section.
6. In the **User Status** section, for **Current Users**, select the **Inactive** and **Initial** options to search for all inactive or initial administrators.
7. Click **Search** to display the list of all administrators matching the search criteria.
8. Select the administrators you want to activate.
9. Click **Activate** to activate the administrator.

Privileges Required

To activate an administrator, you must ensure that you have the appropriate privileges and scope. The MA can activate any administrator, while the GAs can activate all administrators (including other GAs) in their scope, *except* the MA. The OAs can activate all other OAs and UAs in their purview, while the UAs can only activate their peers within their scope.

How to Delete an Administrator Account

Administrator information in RA includes personal information (first name, middle name, last name, email address, and telephone number), credentials, and accounts. When you delete an administrator from Administration Console, the credential and account information must also be deleted along with the personal information. RA supports the cascaded user deletion feature by which all credential, account, and risk-related information for an administrator is also deleted when the administrator is deleted.

If you create a new administrator with the same name as a previously deleted administrator, then 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.

To delete an administrator account:

1. Ensure that you are logged in with the required privileges to delete the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator you want to delete and click **Search**.
You can also click the **Advanced Search** link to search for **Current Users** based on their status (active, inactive, or initial) or their roles (GA, OA, or UA).
The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators you want to delete.
6. Click **Delete**.

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

Privileges Required

To delete an administrator, you must ensure that you have the appropriate privileges and scope. The MA can delete any administrator, while the GAs can delete all administrators (including other GAs) in their scope, *except* the MA account. The OAs can delete all other OAs and UAs in their purview. However, the UAs *cannot* delete their peers within their scope.

Working with Models

Risk Analytics offers an advanced fraud modeling capability. Based on the historical data, this modeling capability can be built and created in RA. By using the available transaction data and system data, the model generates a score that describes the extent to which the model suspects a transaction's genuineness. This score typically ranges from 0 through 100, where the higher the number, the greater the possibility of fraud. RA can be configured to send different responses to your calling application based on this model score.

The model score is available as a part of the system parameters (as **ModelScore**) while configuring rules on the Rules and Scoring Management page in Administration Console. This score can be used in conjunction with other data elements to arrive at a risk advice.

RA publishes an interface specification called **Predictive Model Integration Interface**, and can support any Model platform that conforms to the same. Currently, the following Model platforms are supported:

- Global Decisioning Platform (GDP) v2.7.4
- Data Science Platform (DSP) v1.0

This article briefly explains about how RA uses the Predictive Model and guides you through the process of configuring it and enabling it for use by RA. It covers following topics:

- [How the Rule Engine Uses Model](#)
- [How to Configure Predictive Model Parameters](#)
- [How to Enable the Predictive Model for an Organization](#)
- [How to Configure DSP Model for Organizations with no Existing Models](#)
- [How to Configure DSP Model for Organizations with Existing Models](#)
- [How to Validate DSP Model Configuration](#)
- [Error Codes When RA is Configured to Use DSP Model](#)

How the Rule Engine Uses Model

RA allows for an organization-level (or tenant-level) usage of the DSP Model through the **Model Callout** feature. The Model Callout is executed, if the Model is configured for the specified organization. It is executed *after* all the system rules are executed and *before* the execution of any custom rules you might have deployed. The output of the Model is made available as **Predictive_Score** for the Rule Engine. This value can be used to create other rules, if required.

DSP Model Score

RA expects a numerical value between 0 and 1 as the Predictive Score from the Model, representing the probability of the transaction being a fraudulent. Because this score is multiplied by a factor (generally, **1000**) prior to making the same available to the Rule Engine for risk evaluation, the Score received from the Model is referred to as **Raw Model Score**. The multiplication factor is called **Score Multiplication Factor**.

Valid Raw Model Score: All score output values between 0 and 1 (both inclusive)

Invalid Raw Model Score: Any score output values less than 0 or greater than 1

GDP Model Score

RA expects a numerical value between 0 and 1 as the Predictive Score from the Model, representing the probability of the transaction being a fraudulent. Because this score is multiplied by a factor (generally, **100**) prior to making the same available to the Rule Engine for risk evaluation, the Score received from the Model is referred to as **Raw Model Score**. The multiplication factor is called **Score Multiplication Factor**.

Valid Raw Model Score: All score output values between 0 and 1 (both inclusive)

Invalid Raw Model Score: Any score output values less than 0 or greater than 1

How it Works

DSP: When a valid Raw Model Score is received, the RA system multiplies the same by the configured Score Multiplication Factor, rounds it up to the nearest integer, and finally, presents the same as PREDICTIVE_SCORE to the Rule Engine for risk evaluation. In case of GDP, the rounded up value is presented to the Rule Engine as MODEL_SCORE. The multiplied value is also persisted as PREDICTIVE_SCORE as part of the transaction audit logs.

GDP: When a valid Raw Model Score is received, the RA system multiplies the same by the configured Score Multiplication Factor, rounds it up to the nearest integer, and finally, presents the same as MODEL_SCORE to the Rule Engine for risk evaluation. The multiplied value is also persisted as MODEL_SCORE as part of the transaction audit logs.

When an invalid Raw Model Score is received, then the RA system persists a corresponding negative value. The actual received invalid value is stored in the debug log files.

If any error message or error code is received along with the Raw Model Score, then the same is logged in the Transaction Server's debug logs. This information is not available in the database.

If for some reason, no Raw Model Score is received, then the Risk Analytics system persists a negative value.

Deployment Options

- RA can connect simultaneously to one or more types of Model platforms or to one or more instances of the Model platform.
- Each organization can either have their own Model setup or share the same model setup, as long as one organization has exactly one model setup.

How to Configure Predictive Model Parameters

Note: The RA Predictive Model is an optional component. If you are interested in using a predictive model, contact your Account Manager and initiate a statement of work.

You can configure the URL and timeout parameters for the RA Predictive Model using Administration Console.

Follow these steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Model Configuration** section on the side-bar menu, click the **Model Configuration** link.
The Model Configuration page appears.
5. In the **Proposed Value** column, specify the parameters as described in the following table.

Parameter	Description
Predictive Model URL (primary)	The primary URL of the RA Predictive Model.
Predictive Model URL (backup)	The backup URL of the RA Predictive Model.

Parameter	Description
Connection Timeout (in milliseconds)	The time for which RA tries to establish a connection to the Model before timing out.
Read Timeout (in milliseconds)	The time in which Transaction Server expects a response back from the Model.
Minimum Connections	The minimum number of connections in the connection pool to connect to the Model Server.
Maximum Connections	The maximum number of connections in the connection pool to connect to the Model Server.
Score Multiplication Factor (rational number allowed)	The value by which the score returned by Model is multiplied before being used for rule evaluation.
Protocol Type	The protocol used by RA to communicate with the Model.
Server Authentication SSL	If you want to configure SSL-based communication between Transaction Server and your Model, then you must select this option.
Callout Server Root Certificate	<p>Click Browse to navigate to the location where the Callout Server Root Certificate is located. Callout Server Root Certificate must be in PEM (Base64-encoded) format.</p> <p>Note: If Server Authentication SSL is selected, then you must specify the Callout Server Root Certificate.</p>
Client Authentication SSL	<p>If you want to configure two-way SSL connection between Transaction Server and your Model, then you must select this option and ensure that the Server Authentication SSL is also selected.</p> <p>If you want to configure one-way SSL connection between Transaction Server and your Model, then you must not select this option. In this case, you must ensure that the Server Authentication SSL is selected.</p> <p>If you do not want to configure any SSL-based connection, then you must not select either this option or the Server Authentication SSL option.</p>
Risk Analytics Transaction Server Certificate and Private Key	<p>Click Browse to navigate to the location where the Transaction Server Certificate and Private Key are located. Transaction Server Certificate and Private Key must be in PEM (Base64-encoded) format.</p> <p>Note: If Client Authentication SSL is selected, then you must specify the RA Transaction Server Certificate and Private Key.</p>

6. Click **Upload Model Configuration** to save the changes.

The changes are not yet active and are not available to your end users.

7. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Enable the Predictive Model for an Organization

To enable the RA Model for your organization:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **Rules Management** section, click the **Model Configuration** link.
7. Do one of the following:
 - Enable or Disable the Model:
 - a. Expand the **Enable / Disable Model** option.
 - b. From the **Ruleset** list, select the ruleset for which this configuration is applicable.
 - c. Select **Enable Model** to enable the model.
 - d. Click **Save** to save your changes.
 - e. To make the changes active, you must migrate them to production.
Refer to [How to Migrate to Production](#) for instructions to do so.
 - f. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.
 - Upload model configuration information at the organization level:
 - a. Expand the **Upload Org Level Model Configuration** option.
 - b. In the **Proposed Value** column, specify the parameters as described in the following table:

Parameter	Description
Predictive Model URL (primary)	The primary URL of the RA Predictive Model.
Predictive Model URL (backup)	The backup URL of the RA Predictive Model.
Connection Timeout (in milliseconds)	

Parameter	Description
	The time for which RA tries to establish a connection to the Model before timing out.
Read Timeout (in milliseconds)	The time in which Transaction Server expects a response back from the Model.
Minimum Connections	The minimum number of connections in the connection pool to connect to the Model Server.
Maximum Connections	The maximum number of connections in the connection pool to connect to the Model Server.
Score Multiplication Factor (rational number allowed)	The value by which the score returned by Model is multiplied before being used for rule evaluation.
Protocol Type	The protocol used by RA to communicate with the Model.
Server Authentication SSL	If you want to configure SSL-based communication between Transaction Server and your Model, then you must select this option.
Callout Server Root Certificate	<p>Click Browse to navigate to the location where the Callout Server Root Certificate is located. Callout Server Root Certificate must be in PEM (Base64-encoded) format.</p> <p>Note: If Server Authentication SSL is selected, then you must specify the Callout Server Root Certificate.</p>
Client Authentication SSL	<p>If you want to configure two-way SSL connection between Transaction Server and your Model, then you must select this option and ensure that the Server Authentication SSL is also selected.</p> <p>If you want to configure one-way SSL connection between Transaction Server and your Model, then you must not select this option. In this case, you must ensure that the Server Authentication SSL is selected.</p> <p>If you do not want to configure any SSL-based connection, then you must not select either this option or the Server Authentication SSL option.</p>
Risk Analytics Transaction Server Certificate and Private Key	<p>Click Browse to navigate to the location where the Transaction Server Certificate and Private Key are located. Transaction Server Certificate and Private Key must be in PEM (Base64-encoded) format.</p> <p>Note: If Client Authentication SSL is selected, then you must specify the RA Transaction Server Certificate and Private Key.</p>

c. Click **Upload Model Configuration** to save the changes.

How to Configure DSP Model for Organizations with no Existing Models

DSP Model configuration for an organization with no existing Model (GDP or DSP) requires following steps:

- [Step 1: How to Create Organization-Level Model Configuration](#)
- [Step 2: How to Set the Model as the Referenced Model](#)
- [Step 3: How to Enable the Model](#)

Step 1 How to Create Organization-Level Model Configuration

To create an organization-level DSP Model configuration:

1. Identify the following data points:
 - Destination DSP deployment's Primary URL
 - Destination DSP deployment's Backup URL

2. Execute the following queries:

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP', 'PRIMARYURL', '<dsp-primary-url>', 'Default URL of primary DSP
server', 'Default URL of primary DSP server', 0, 0, 0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP', 'BACKUPURL', '<dsp-backup-url>', 'Default URL of backup DSP
server', 'Default URL of backup DSP server', 0, 0, 0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP', 'READTIMEOUT', '10000', 'Read timeout for DSP server', 'Read timeout
for DSP
server', 0, 0, 0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
```

```
'ADDONDSP','CONNECTIONTIMEOUT','10000','Connection timeout for DSP
server','Connection timeout for DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORGNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','MINCONNECTION','16','Minimum number of connection to DSP
server','Minimum number of connection to DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORGNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','MAXCONNECTION','64','Maximum number of connection to DSP
server','Maximum number of connection to DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORGNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','SCOREMULFACTOR','1000','Score Multiplication Factor on
DSP','Score
Multiplication Factor on DSP',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORGNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','POPULATESCOREAS','PREDICTIVE_SCORE','Destination rule element
for model
score', 'Destination rule element for model score',0,0,0);
```

Note: Replace *<dsp-primary-url>*, *<dsp-backup-url>*, *<specific-org-name>* with the specific URL and Organization name.

Step 2 How to Set the Model as the Referenced Model

To set the Model to be used:

1. Execute the following query:

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORGNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONMODEL','ACTIVEMODELS','ADDONDSP', 'Model settings to use', 'Model
```

```
settings to  
use',0,0,0);
```

Note: Replace *<specific-org-name>* with the specific Organization name.

2. Restart the Transaction Server (either immediately or as part of the regular rolling scheduled restarts). This change will only take effect after the server has been restarted.

Step 3 How to Enable the Model

To enable the new Model:

1. Log in to the Administration Console as an administrator with access to the required organization.
2. Under **Organizations** tab, search for the desired organization and then navigate to **Risk Engine** tab.
3. Under the **Rules Management** section, click the **Model Configuration** link.
4. For each of the rulesets where the Model is required, explicitly check the **Enable Model** option and save the same.
Repeat this step for each ruleset where Model will be used.
5. Restart the Transaction Server to make the change effective.

Important! Create rules using the Model Score only after all the Transaction Servers have been restarted.

See [How to Enable the Predictive Model for an Organization](#) for detailed steps for enabling a Model.

How to Configure DSP Model for Organizations with Existing Models

The following table provides an at-a-glance overview of the process of switching over from an older GDP Model to a newer DSP Model.

Activity Phase	Activity Details	Impact	Dependency
Deployment of RA Patch and Configuration of DSP Model URLs		No change as transactions would continue with being relayed to GDP Model only	
Phase I - Priming of the DSP Model <i>(Generally expected to be around 3 weeks)</i>	Change Model Relay mode from 'Model GDP' to 'Both GDP and DSP Models' Note: No rule changes required; current Rules continue to work as-is	No change as rules would consume the model score of the GDP Model only	When Customer and DS team are ready to initiate Model Priming
Phase II - Enabling of the DSP Model	Creation of Rules to use DSP Model Score		

<i>(Generally expected to be around 3 weeks)</i>	Disabling of the Rules using GDP model score	Transactions would be evaluated using the Rules configured with DSP Model score thresholds	When DS Team confirms that Model priming is completed
Phase III - Disabling of the GDP Model	Change Model Relay mode from 'Both GDP and DSP Models' to 'Model DSP' Deletion of GDP Rules	No impact as transactions would continue with being relayed to DSP Model only	When Customer Admin and DS team find DSP Model scoring as acceptable

Notes on Model Score Monitoring

- Rollback from the DSP to GDP model is possible in Phase I and Phase II. Any further action plan needs be worked out on a case-by-case basis.
- Both GDP and DSP scores can be monitored either through exporting from the Analyze Transaction screen or through offline SQL report, because both scores will be available as separate columns within the **SysAuditLog** table.
- The scores can be displayed on the user interface (UI) and as part of desired reports, whenever required.
- GDP and DSP scores can also be monitored through the respective system's file logs.

The following steps walk you through the process to configure DSP Model for organizations that already have GDP Model configured:

- [Step 1: How to Create an Organization-Level Model Configuration](#)
- [Step 2: How to Enable the DSP Model as the Secondary Model to Initiate Priming](#)
- [Step 3: How to Switch Over from the GDP Model to DSP Model for Use in Rules](#)
- [Step 4: How to Remove the GDP Model](#)
- [Step 5: How to Display the DSP Model Score in UI and Reports](#)

Step 1 How to Create an Organization-Level Model Configuration

To create an organization-level DSP Model configuration:

1. Identify the following data points:

- Destination DSP deployment's Primary URL
- Destination DSP deployment's Backup URL

2. Execute the following queries:

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,
```

```
'<specific-org-name>', -1,
'ADDONDSP','PRIMARYURL', '<dsp-primary-url>','Default URL of primary DSP
server','Default URL of primary DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','BACKUPURL', '<dsp-backup-url>','Default URL of backup DSP
server','Default URL of backup DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','READTIMEOUT','10000','Read timeout for DSP server','Read timeout
for DSP
server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','CONNECTIONTIMEOUT','10000','Connection timeout for DSP
server','Connection timeout for DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','MINCONNECTION','16','Minimum number of connection to DSP
server','Minimum number of connection to DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','MAXCONNECTION','64','Maximum number of connection to DSP
server','Maximum number of connection to DSP server',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID,ORNAME,CHANNELID,CATEGORY,NAME,VALUE,DESCRIPTION,DISPLAYNAME,TYPE,SHOWI
NUI,DISPLAYORDERID) VALUES (ARRFCFIGSEQUENCE.NEXTVAL,
'<specific-org-name>', -1,
'ADDONDSP','SCOREMULFACTOR','1000','Score Multiplication Factor on
DSP','Score
```

```
Multiplication Factor on DSP',0,0,0);
```

```
INSERT INTO ARRFCONFIGURATION  
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI  
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,  
'<specific-org-name>', -1,  
'ADDONDSP', 'POPULATESCOREAS', 'PREDICTIVE_SCORE', 'Destination rule element  
for model  
score', 'Destination rule element for model score', 0, 0, 0);
```

```
INSERT INTO ARRFCONFIGURATION  
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWI  
NUI, DISPLAYORDERID) VALUES (ARRFCONFIGSEQUENCE.NEXTVAL,  
'<specific-org-name>', -1,  
'ADDONMODEL', 'ACTIVEMODELS', 'ADDONGDP', 'Model settings to use', 'Model  
settings to  
use', 0, 0, 0);
```

Note: Replace *<dsp-primary-url>*, *<dsp-backup-url>*, *<specific-org-name>* with the specific URL and Organization name.

3. Restart the Transaction Server (either immediately or as part of the regular rolling scheduled restarts). This change will only take effect after the server has been restarted.

Step 2 How to Enable the DSP Model as the Secondary Model to Initiate Priming

To prime the DSP Model as secondary Model:

1. Execute the following query:

```
UPDATE ARRFCONFIGURATION  
SET VALUE = 'ADDONGDP;ADDONDSP'  
WHERE ORGNAME = '<specific-org-name>' AND CATEGORY = 'ADDONMODEL' AND NAME =  
'ACTIVEMODELS'
```

Note: Replace *<specific-org-name>* with the specific organization's name.

2. Restart the Transaction Server (either immediately or as part of the regular rolling scheduled restarts).
This change will only take effect after the server has been restarted.

At this stage, both the GDP and DSP models will be called and the Model Score will be available as follows:

Model Number	Rule element for the model score
Model #1 - GDP model	MODEL_SCORE
Model #2 - DSP model	PREDICTIVE_SCORE

Important! At this point, rules should be created **ONLY** using the **MODEL_SCORE** element.

Step 3 How to Switch Over from the GDP Model to DSP Model for Use in Rules

Important! Switchover of rules from using the GDP model score to the DSP model score **must be undertaken only when the DSP model priming is completed**. This can be ensured based on Data Science team's monitoring reports.

Option I

To switch over from GDP to DSP Model:

1. For each rule created that is using the MODEL_SCORE rule element:
 - a. Create a new rule using the PREDICTIVE_SCORE rule element and keeping the remaining rule criteria as the same.
 - b. Disable the rule using the MODEL_SCORE element.
2. At this stage:
 - (Optional) You can change the rule's risk advice, if required.
 - You can deprecate some existing model score rules in favour of new rules using the model score.
3. Migrate to Production.
4. Restart the Transaction Server.

Note: A regular scheduled transaction server refresh is also sufficient

Model score ranges are as follows:

Model Number	Rule Element for The Model Score	Output Score Range
Model #1 - GDP model	MODEL_SCORE	1 through 100
Model #2 - DSP model	PREDICTIVE_SCORE	1 through 1000

Note: Model score thresholds for GDP model and DSP model have no direct correlation, and therefore the rule thresholds must be specified with due consideration.

Option II

To switch over from GDP to DSP Model:

1. Create a new Ruleset based on the existing ruleset being used.
2. For each rule that is using the MODEL_SCORE rule element:
 - a. Edit the existing model score rules to now use the PREDICTIVE_SCORE element, while keeping the remaining rule criteria as the same.
3. At this stage,
 - (Optional) You can change the rule's risk advice, if required.
 - You can deprecate some existing model score rules in favour of new rules using the model score.

4. Migrate to Production the new ruleset.
5. Change the assigned ruleset to refer to the new ruleset.

Model score ranges are as follows:

Model Number	Rule Element for The Model Score	Output Score Range
Model #1 - GDP model	MODEL_SCORE	1 through 100
Model #2 - DSP model	PREDICTIVE_SCORE	1 through 1000

Note: Model score thresholds for GDP model and DSP model have no direct correlation, and therefore, the rule thresholds must be specified with due consideration.

Step 4 How to Remove the GDP Model

To remove the older GDP Model:

1. Execute the following query:

```
UPDATE ARRFCONFIGURATION
SET VALUE = 'ADDONDSP'
WHERE ORGNAME = '<specific-org-name>' AND CATEGORY = 'ADDONMODEL' AND NAME =
'ACTIVEMODELS'
```

Note: Replace *<specific-org-name>* with the specific organization's name.

2. Restart the Transaction Server (either immediately or as part of the regular rolling scheduled restarts).
This change will only take effect after the server has been restarted.

Important! At this stage, only the DSP model will be called and the Model Score will be available as PREDICTIVE_SCORE. Therefore, rules must be created **ONLY** using the PREDICTIVE_SCORE element.

When Is Roll Back from DSP to GDP Model Possible

Phase	Rollback Options And Procedure
Phase I	Rollback not applicable because only GDP Model score is being used within rules. Relay of transactions to DSP can be stopped, if required.
Phase II	<p>Model Scores from both GDP and DSP Models available, because two different Data Elements are available and both can be individually used by rules.</p> <p>To use DSP Model Score, rules will use the DSP Model Score element, while to use GDP Model Score, rules will need to use the GDP Model Score element.</p> <p>Rolling back depends on the option used as part of the Phase II:</p>

Phase	Rollback Options And Procedure
	<p>If Option I was used, then simply changing of the rules by inactivating the DSP Model Score rules in favor of GDP Model Score rules is required.</p> <p>If Option II was used, then simply changing the Assigned Ruleset from the one using DSP Model Score to the earlier one what used the GDP Model Score is required.</p>
Phase III	Rollback is not applicable.

Step 5 How to Display the DSP Model Score in UI and Reports

Important! DSP model scores (enabled post-Risk Analytics 4.0 SP4 HF1) are stored within **SysAuditLog** table's PREDICTIVE_SCORE column, as against MODEL_SCORE column earlier. This field will not be visible or included as part of the default product deployment or upgrade. In due course, all Model Scores will be sourced from this new column instead of the older MODEL_SCORE column.

Query to Display the DSP Model Score as the Last Column in UI and Reports

Run the following query to make PREDICTIVE_SCORE column appear as the last column in Analyze Transaction screen and other screens and reports:

```
UPDATE ARRFCHANNELEMENTS
SET SHOW_IN_DETAIL = 1, SHOW_IN_EXPORT = 1, SHOW_IN_FA_SUMMARY = 1,
SHOW_IN_SUMMARY = 1, ORDER_DETAIL = 1000, ORDER_EXPORT = 1000,
ORDER_FA_SUMMARY = 1000, ORDER_SUMMARY = 1000
WHERE ELEMENTNAME = 'PREDICTIVE_SCORE';
```

Query to Display the DSP Model Score Next to GDP Model Score in UI and Reports

Run the following query to make PREDICTIVE_SCORE column appear as the column next to MODEL_SCORE in Analyze Transaction screen and other screens and reports:

```
UPDATE ARRFCHANNELEMENTS
SET SHOW_IN_DETAIL = 1, SHOW_IN_EXPORT = 1, SHOW_IN_FA_SUMMARY = 1,
SHOW_IN_SUMMARY = 1, ORDER_DETAIL = 106, ORDER_EXPORT = 106,
ORDER_FA_SUMMARY = 106, ORDER_SUMMARY = 106
WHERE ELEMENTNAME = 'PREDICTIVE_SCORE';
```

How to Validate DSP Model Configuration

This section guides you how to validate if your DSP Model was correctly deployed. It covers the following topics:

- [How to Validate the Model Configuration at Organization-Level](#)
- [How to Validate the Model State at Ruleset-Level](#)

How to Validate the Model Configuration at Organization-Level

For Risk Analytics version 4.x, execute the following database queries for the specified organization:

Note: As of Risk Analytics 4.x, this cannot be validated through the UI.

▪ Query for Model #1

```
SELECT NAME, DESCRIPTION, VALUE
FROM ARRFCONFIGURATION
WHERE ORGNAME = '<specific-org-name>' AND CATEGORY = 'ADDONGDP'
ORDER BY NAME;
```

Note: Replace *<specific-org-name>* with the specific organization's name.

▪ Query for Model #2

```
SELECT NAME, DESCRIPTION, VALUE
FROM ARRFCONFIGURATION
WHERE ORGNAME = '<specific-org-name>' AND CATEGORY = 'ADDONDSP'
ORDER BY NAME;
```

Note: Replace *<specific-org-name>* with the specific organization's name.

The following table lists the expected record output (to be validated independently for each Model):

Parameter	Output Value	Example output value
PRIMARYURL	Valid URL of the primary GDP/DSP deployment. URL must contain protocol (HTTP or HTTPS), machine name or IP address, port number, URI	http://dsp.arcot.com:8080/dsp
BACKUPURL	Valid URL of the HA GDP/DSP deployment. URL must contain protocol (HTTP or HTTPS), machine name or IP address, port number, URI	http://dsp.arcot.com:8080/dsp
READTIMEOUT	Integer value Min value = 10 Max value = 20000	10000
CONNECTIONTIMEOUT	Integer value Min value = 10 Max value = 20000	10000
MINCONNECTION	Integer value	16

Parameter	Output Value	Example output value
MAXCONNECTION	Min value = '1'	
	Max value = '64'	
	Integer value	64
	Value should be greater than MINCONNECTION	
SCOREMULFACTOR	Min value = '4'	
	Max value = '64'	
	Integer value	1000
	Value should be either '100' for GDP models and it should be '1000' for DSP models	
POPULATESCOREAS	Field name	PREDICTIVE_SCORE
	Value should be either 'MODEL_SCORE' for GDP models and it should be 'PREDICTIVE_SCORE' for DSP models	

Notes:

- This is an ORG-level setting, and therefore, needs to be done once when the organization is being enabled for GDP or DSP Models.
- Changes will be required only if one or more parameters are to be tweaked.

How to Validate the Model State at Ruleset-Level

To validate if the DS Model was correctly de[ployed:

1. Log in to the Administration Console as an administrator with access to the required organization.
2. Under **Organizations** tab, search for the desired organization and then navigate to **Risk Engine** tab.
3. Under the **Rules Management** section, click the **Model Configuration** link.
4. For each of the rulesets where the Model is required, ensure that the **Enable Model** option is selected.
Repeat this step for each ruleset where Model will be used.

Error Codes When RA is Configured to Use DSP Model

The following table lists the error codes logged by Risk Analytics during its interaction with DSP Model. In case of errors, these are the values that you will see in the **Model Score** column instead of the actual score (which is expected to be between 0 and 1000).

ERROR	ERROR_CODE
UNKNOWN_FAILURE	-1
READ_TIMEOUT	-2
READ_GDPRESPONSE_FAILURE	-3
WRITE_GDPREQUEST_FAILURE	-4
XML_PARSE_FAILURE	-5
MODEL_SCORE_NOT_RECEIVED	-6
MODEL_SCORE_NEGATIVE	-7
MODEL_SCORE_INVALID	-8
TRANSACTIONID_INVALID	-9
ARCOT_EXCEPTION	-10
TRANSPORT_EXCEPTION	-11
TRANSPORT_READ_EXCEPTION	-12
TRANSPORT_WRITE_EXCEPTION	-13
UNKNOWN_EXCEPTION	-14
UN_TRANSPORT_WRITE_EXCEPTION	-15
UN_TRANSPORT_READ_EXCEPTION	-16
UN_GDPREQ_EXCEPTION	-17
UN_GDPREQ_POSEVAL_EXCEPTION	-18
UN_CONN_SNDRCV_EXCEPTION	-19
UN_CONN_SNDRCV_FAILURE	-20
UN_CONN_EXCEPTION	-21
LOGGING_EXCEPTION	-22
HTML_REPONSE_ERROR	-23
MODEL_NOT_CALLED	-999

Important! If DSP Model returns any specific error code and/or error details, the same will be logged to the Transaction Server debug logs. However, this information will not be available in the database.

Configuring RA Properties and Related Configurations

This topic covers the following sub-topics:

- [How to Configure Channels and Accounts Associations](#)

- [How to Configure a Card Issuer](#)
- [How to Delete the Card Issuer Mapping](#)
- [How to Configure the NBIN Mapping](#)
- [How to Delete the NBIN Mapping](#)
- [How to Configure the Transaction Acquirer](#)
- [How to Delete the Transaction Acquirer Mapping](#)
- [How to Configure Miscellaneous Risk Analytics Properties at the Organization Level](#)
- [How to Configure Miscellaneous Risk Analytics Properties at the System Level](#)
- [How to Upload Compromised Card Information](#)

How to Configure Channels and Accounts Associations

An end user can perform a transaction in many ways. Some of these include:

- Online (Transactions that originate when the user uses a credit card or a debit card online, but the transaction is not governed by 3D Secure protocol.)
- 3D Secure (Transactions that originate when the user uses a credit card or a debit card online.)
- Online banking (Transactions that originate when the user logs into their banking site, without using a credit card.)
- Online wire transfers (Transactions that originate when the user transfers money.)
- App (Transactions that originate when the user uses a smartphone app.)
- SMS (Transactions that originate using SMS messaging.)
- ATM (Transactions that originate at an ATM machine.)
- POS (Transactions that originate at a store's or shop's point of sale.)

These different origins of transactions are referred to as *channels* in RA terminology.

RA can be configured to evaluate risk for any of these channels. It can also be configured to evaluate transactions from each channel differently to generate a risk score. It can also be configured to evaluate transactions from each channel differently to generate a risk score. In addition, an RA rule can be evaluated across different channels to arrive at a score. This is known as *cross-channel* configuration.

The following table describes the channels that are available out-of-the-box in RA.

Channel	Description
DEFAULT	

Channel	Description
	Transactions that are initiated using a Web browser. This may be either a computer, smart phone, tablet, or set-top box. The default channel is the Web channel.
3D Secure	Online transactions initiated using credit card or debit card.
ATM	<p>Transactions initiated through ATM.</p> <p>ATMs are terminals primarily used as an alternate channel for availing banking services, such as account balance inquiry or cash withdrawal.</p>
POS	<p>Transactions initiated at physical Point of Sale (POS).</p> <p>POS terminals are primarily used as channels for recording a financial payment made by the card holder to a merchant for goods or services purchased by the card holder from the merchant</p>
IMPS	<p>Transactions initiated using Immediate Payment Service (IMPS), a channel-agnostic payment service.</p> <p>Using IMPS, bank customers can transfer money instantly within any of the IMPS-enabled member banks across India. IMPS is accessible through mobile banking, net banking, and ATM channel.</p> <p>IMPS can be used for funds transfer and merchant payments. It supports the following services:</p> <p>P2P: Person to Person</p> <p>P2A: Person to Account</p> <p>P2M (Push): Person to Merchant initiated by Customer</p> <p>P2M (Pull): Person to Merchant initiated by Merchant</p>
ECOM	Ecommerce transactions received as ISO 8583 messages.

To configure channel and account associations:

Note: Typically, configuring channels is a one-time activity. If you want to change these settings in a production environment, contact CA Arcot Support to understand the implications. You can add a channel to your existing deployment, but removing support for a channel or account type and changing the default channel or default account type requires careful consideration.

- Ensure that you are logged in as a GA.
- Activate the **Organizations** tab.
- Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
- Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
- Activate the **Risk Engine** tab.
- Under the **General Risk Analytics Configurations** section, click the **Assign Channels and Configure Default Account Types** link.
The Assign Channels and Configure Default Account Types page appears.
- Select the channels that are supported by the organization by selecting the **Select Channels to Associate** check box.
- Select the default account type for each channel:
 - Select **User Name** as **Default Account Type** if requests from the calling application on the specific channel send the username in the Risk Evaluation APIs.
 - If requests from the calling application contain the account IDs in the user name field, select the relevant <**Default Account Type**> for the channel.
- Select the option under **Select Default Channel** to make the channel the default one to be used for risk evaluation purposes.
- Click **Save** to save your changes.
- Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure a Card Issuer

A *Card Issuer* is the institution that issues the card, which is involved in a financial transaction. The first six digits of the card number are known as the **Issuer Identification Number (IIN)** or **Bank Identification Number (BIN)**, and these digits identify the Card Issuer. To correctly identify the organization representing the Card Issuer, you must map the card numbers to Issuers by creating BINs, and then associate the BIN with an organization. This mapping represents that card numbers with the specified BIN prefix string are issued by the associated organization. You must configure the Card Issuer because the incoming transaction metadata for ATM and POS channels does not contain organization information. RA determines this information from the card number.

Note: An organization can have several BINs associated with it, but a single BIN can be associated with exactly one organization.

To configure a card issuer:

1. Ensure that you are logged in as a GA.

2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the Organization column, click the **<ORGANIZATION_NAME>** link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **General Risk Analytics Configurations** section, click the **Card Issuer Mapping** link.
The Card Issuer Mapping page appears.
7. Enter values for the fields on this page, as described in the following table.

Field	Description
BIN Data to Organization Mapping	
BIN Name	Name of the Issuer BIN
BIN Prefix	Prefix of the card number that will be used to identify the Issuer
Card Length	The total length of the card number
Note: Expected values are 15, 16, or 19.	
BIN Parameters	
<p>The Card BIN parameters enable you to set business thresholds, which are different from rule thresholds. For example, you can create a rule that detects and restricts consecutive withdrawals of the daily maximum withdrawal amount for three consecutive days for a given card, where the daily maximum cash withdrawal limit might be USD1,000 for a Silver-level card and USD10,000 for a Platinum-level card. In this case, the limits of 1,000 and 10,000 are business thresholds rather than rule thresholds. You can set these thresholds as part of the appropriate Card BIN configuration.</p>	
Duration	<p>Maximum time period to consider for transaction history. The duration is specified in minutes or hours, depending on how it is configured in the rule.</p> <p>Note: Transaction history is defined as the list of transactions for the same account (Card Number or PAN) over ATM and POS channels in reverse chronological sequence.</p>
Threshold Amount	Maximum limit on the transaction amount for a card, defined in the organizations' base currency.
Transaction Count	Total number of transactions to consider for transaction history.

8. Click **Add**.
9. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Delete the Card Issuer Mapping

To delete the mapping between the BIN and Card Issuer,:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the Organization column, click the **<ORGANIZATION_NAME>** link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **General Risk Analytics Configurations** section, click the **Card Issuer Mapping** link.
The Card Issuer Mapping page appears.
7. Select the row in the **Card Issuer to Organization** table that corresponds to the mapping that you want to delete, and click **Delete**.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure the NBIN Mapping

National Bank Identification Number (NBIN) is used to identify banks in the context of Mobile Remittances for routing transactions by IMPS. You must configure the NBIN because the incoming transaction metadata for IMPS channels does not contain organization information.

Important! NBIN values must be unique across organizations.

To configure NBIN mapping:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the Organization column, click the **<ORGANIZATION_NAME>** link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.

6. Under the **General Risk Analytics Configurations** section, click the **NBIN Mapping** link.
The NBIN to Organization page appears.
7. Enter values for the **NBIN Name** and **NBIN**, and click **Add**.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Delete the NBIN Mapping

To delete the mapping between the NBIN and an organization:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the Organization column, click the **<ORGANIZATION_NAME>** link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **General Risk Analytics Configurations** section, click the **NBIN Mapping** link.
The NBIN to Organization page appears.
7. Select the row in the **NBIN to Organization** table that corresponds to the mapping that you want to delete, and click **Delete**.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure the Transaction Acquirer

A *Transaction Acquirer* is the institution that manages the network of ATM or POS terminals from where the financial transaction originates. An Institution Identification Code (IIC) is assigned to each Acquirer institution that participates in the global financial network. You can map Acquiring IICs (hereafter referred to as Acquirer IDs) to Acquirers by associating Acquirer IDs with a specific organization.

Note: An organization may have more than one Acquirer ID associated with it, but a single Acquirer ID can be associated with exactly one organization.

To configure a Transactions Acquirer:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.

3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the Organization column, click the **<ORGANIZATION_NAME>** link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **General Risk Analytics Configurations** section, click the **Transaction Acquirer Mapping** link.
The Transaction Acquirer Mapping page appears.
7. Enter values for the **Acquirer Name** and **Acquirer ID**, and click **Add**.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Delete the Transaction Acquirer Mapping

To delete the mapping between the Transaction Acquirer and an organization:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the Organization column, click the **<ORGANIZATION_NAME>** link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **General Risk Analytics Configurations** section, click the **Transaction Acquirer Mapping** link.
The Transaction Acquirer Mapping page appears.
7. Select the row in the **Transaction Acquirer to Organization** table that corresponds to the mapping that you want to delete, and click **Delete**.
8. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure Miscellaneous Risk Analytics Properties at the Organization Level

To configure RA properties:

1. Ensure that you are logged in as a GA.

2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click the **Search** button.
A list of organizations matching the search criteria appears.
4. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **General Risk Analytics Configurations** section, click the **Miscellaneous Configurations** link. The Miscellaneous Configurations page appears.
7. From the **Select Channel** list, select the channel for which you want to configure these parameters.
8. Specify values for the parameters, as described in the following table.

Property	Default Value	Description
User Enrollment Mode	Implicit	<p>The mode in which the user is created in the RA database:</p> <p>Implicit: If you select Implicit, then you do not need to invoke the createUser() Web service for creating users in RA. In this case, when you call the evaluateRisk()API for a transaction, RA will automatically create users (if not already present) in RA.</p> <p>Explicit: If you select Explicit, you would need to explicitly call the createUser()Web service to create the users in RA before you can do a risk evaluation (by calling the evaluateRisk()API) for their transactions.</p>
Base Currency Code	USD	Currency Code in which the organization does business. This parameter is used for amount-based rules and for display purposes in Case Management.
Enable Reverse Lookup for Device Identification	No	Enable Reverse Lookup to identify the device. Select No if this parameter is not applicable for the channel, for example, ATM.
Use IP Address for Reverse Lookup	No	Use the IP address for reverse lookup method of device identification.

Property	Default Value	Description
Number of Case Notes to Display When Working on Cases	1	Number of case notes to display when the CSR views the case on the Case Management screen.
Additional Number of Case Notes to Display on Clicking "More"	3	Number of case notes to display when the CSR clicks the More link under Case Notes.
Default Number of Days a User Gets Added to Exception List Through Case Management Screen	10	The number of days for which a user is added to the Exception List through the Case Management screen.
Default Transaction Display Duration (in Days)	30	Duration for which transactions are displayed to the CSR on the Case Management screen by default.
Max Transaction Display Duration (in Days)	90	The maximum duration for which CSRs can view the transaction history.
Maximum Duration for Which the Case is Exclusively Assigned to a CSR Before it is Available for Reassignment (in Seconds)	3600	The maximum duration for which a case remains exclusively assigned to a CSR viewing the case in the console.
Number of Records on Each Page of Analyze Transactions Screen	10	Number of records to display on each page of the Analyze Transactions screen in Case Management.
Queue Rebuild Schedule Time Interval(Format: HHMM-HHMM=DURATION(seconds)) GMT	-1	The time interval during which the Queue Rebuild is scheduled. For example, 0900-2000=1800 schedules the Queue Rebuild every 30 minutes from 9AM to 8PM.
Frequency of Automatic Queue Rebuild Schedule (in Seconds)	1800	Frequency at which the case scheduler automatically rebuilds Queues.
Generate Cases For Advice(s)	DENY ALERT	The RA advice(s) for which cases are to be generated. The possible values are: NONE DENY ALERT INCREASEAUTH ALLOW

9. Click **Update** to save your changes.

10. Refresh the organization cache for the changes to take effect.

See [How to Refresh the Organization Cache](#) for detailed information about how to do this.

How to Configure Miscellaneous Risk Analytics Properties at the System Level

To configure miscellaneous Risk Analytics properties at the system level:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Risk Analytics** option on the submenu of the tab.
4. Under **General Risk Analytics Configurations** section on the side-bar menu, click the **Miscellaneous Configurations** link to display the page.
5. Specify the parameters that the GA can configure at the system level, as described in the following table.

Property	Default Value	Description
Next Action Date Cut-Off for Including a Case in Queue Rebuild (in Seconds)	1800	The duration before a case is added to the Queue rebuild.
Number of Records to Be Fetched in One Chunk From Database When Exporting Analyze Transactions Report (Configure this according to the maximum heap memory available on the application server.)	5000	If the number of records to export is very high, the RA application fetches datasets in chunks of small sizes to ensure that the application server does not run out of memory. If the application server has sufficient heap memory available, you can increase this value so that the RA application makes fewer number of queries to the database. This results in improved performance.
Maximum Duration for Search on Analyze Transaction And Search Cases Screen (in Days)	180	Maximum duration for which search is allowed in the Analyze Transaction screen and Search Cases screen.
Enable Risk Analytics Statistics Monitoring (Risk Analytics Server Restart Required)	Yes	Enables statistics collection at the server so that the arrfstatsmonitor tool can monitor the health of the system in real-time.
ISO8583 Transaction Identification Look-Back Duration for Repeat Transactions (in mins)	10	Maximum time period (in minutes) to consider for transaction history to identify the original transaction in the case of repeat transactions.
	30	

Property	Default Value	Description
ISO8583 Transaction Identification Look-Back Duration for Reversal Transactions (in mins)		Maximum time period (in minutes) to consider for transaction history to identify the original transaction in the case of reversal transactions.
ISO8583 Transaction Identification Look-Back Duration for Advice Transactions (in mins)	2880	Maximum time period (in minutes) to consider for transaction history to identify the original transaction in the case of financial advice transactions.

Note: The other parameters are described in the table in [How to Configure Risk Analytics Properties at the Organization Level](#).

6. Click **Update** to make your changes effective.

7. Refresh *all* deployed Transaction Server instances.

See [Refreshing the Cache](#) for instructions on how to do this.

How to Upload Compromised Card Information

Common Point of Compromise (CPC) for multiple cards is a potential terminal where multiple cards are skimmed and subsequently, details of more than one of those cards get used in fraudulent transactions. You can upload a file containing the compromised card information.

To upload a list of compromised cards:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Compromised Card Configuration** section, click the **Upload Card Details** link to display the **Compromised Card Configuration** page.
5. Browse to the file containing the compromised card numbers.

Note: Click the help icon to see the data format that you should use in your file.

6. Click **Upload** to upload the file.

Configuring RA Callouts

Important! All the configurations and tasks discussed in this article can be performed by **Global Administrators** to apply the rules globally or by **Organization Administrators** to apply the rules for an organization.

A *Callout* is a custom component (which can be written in a programming language of your choice) to modify or augment the standard functionality of RA. A Callout, typically, is an external process. As a result, it resides "outside" the Transaction Server context and is hosted on a separate HTTPS-based server. Being an external process, you must configure a Callout by using the Administration Console, so that it is invoked when required.

This article describes the types of Callouts that RA supports and how to configure these Callouts to meet your business requirements. In addition, this article also walks you through the deployment, configuration, and use of the Sample Callout that is shipped in the RA package:

- [What are Callouts and How they Work](#)
- [How to Configure an Evaluation Callout](#)
- [How to Configure a Scoring Callout](#)
- [How to Work with the Sample Callout](#)

Note: Ensure that the administrator performing configuration-related activities has the required privileges to perform these operations. For more information about the privileges available to administrators at each level, see [Summary of Administrative Privileges](#).

After you configure a Callout, the changes are not immediately **active** (available to your end users.) You *must* use the **Migrate to Production** link in the side-bar menu of Administration Console to "move" all **proposed** configuration changes to your production database. Refer to [How to Migrate to Production](#) for instructions to do so.

What are Callouts and How they Work

Based on your business requirements, you can write your own custom Evaluation logic and Scoring logic, which if implemented, will run at your application-end, independent of Transaction Server. These custom Evaluation or Scoring programs are known as *Callouts* that can also be implemented to interact with your application's back-end system.

Note: RA is shipped with a basic Sample Callouts WAR file (**riskfort-5.0-sample-callouts.war**) that demonstrates how you can write and implement simple Evaluation and Scoring Callouts. See [How to Work with the Sample Callout](#) for more information about deploying and configuring this file.

For example, in addition to tracking the origin of each transaction, a banking institution would also like to assess the risk of regular bank transactions and wire transfers based on the transaction amount. Say, the bank would like to evaluate all transactions more than \$30,000 for risk, irrespective of whether they are regular transactions or wire transfers. In this case, in addition to using RA's Negative Country, Untrusted IP, Zone Hopping, and Velocity checks, the institution can write an Evaluation Callout (within the scope of their application) to track this behavior.

Note: After a Callout is deployed, you *must* enable it by using the Callout Configuration page for it to take effect.

What Different Types of Callouts are Available

RA supports the following types of Callouts:

- Evaluation Callouts

- Scoring Callout

Evaluation Callouts

An *Evaluation Callout* is executed as part of risk evaluation. If an Evaluation Callout is implemented, then:

1. RA executes all Standalone and Combination rules and invokes the Callout framework.
2. The RA Callout framework formats the data in XML format.
3. The RA Callout framework performs an HTTP or HTTPS POST of the following information to your Evaluation Callout:
 - **Context information** (such as User name, IP address, and Device ID) that is passed to each RA Evaluation rule.
 - **Rule results** for each Evaluation rule that was executed.
 - **Additional Inputs**, if any, that are provided by the RA SDK to Transaction Server as input data.
4. Your Callout uses the data passed by RA to process its custom logic.
5. Your Callout then returns the following information to RA:
 - **Rule result** in the form of Y (SUCCESS) or N (FAILURE).
 - **Modifier string** with additional information, if any, to be used by the Scoring Callout (if implemented.)

Note: Transaction Server does not process the modifier string at all. If a Scoring Callout also has been implemented, then Transaction Server POSTs this data to the Scoring Callout. This information is used for logging (in the database), reporting, and auditing purposes.

6. Transaction Server logs the information returned by your Callout.

Scoring Callout

A *Scoring Callout* is executed *after* the standard RA Scoring logic has executed. If a Scoring Callout is implemented, then:

1. Transaction Server executes the standard Scoring program and invokes the Callout framework.
2. The RA Callout framework formats the data in XML format.
3. The RA Callout framework performs an HTTP or HTTPS POST of the following information to your Scoring Callout:
 - **Overall Score** computed by the standard RA built-in Scoring Engine.
 - **Rule results** for each Evaluation rule that was executed.
 - **Additional Inputs**, if any, that are provided by the calling application as part of the `evaluateRisk()` API call.

- **Modifier string** originally returned by the Evaluation Callout.
4. Your Callout uses the data passed by RA to process its custom logic.
 5. Your Callout then returns the following information to RA:
 - **Final Score** in the form of an integer in the range [0 - 100].

Note: The score returned by the Scoring Callout always overrides the Score computed by the RA Scoring Engine. If you want to retain the score computed by the RA standard Scoring Engine, then you will need to pass that same Score as the return value in your response. This information is used for logging (in the database), reporting, and auditing purposes.

6. Transaction Server logs the information returned by your Callout.

How are Callouts Implemented

Note: Implementation of Callouts is optional.

If you have implemented a Callout, then Transaction Server reads all configurations related to the Callout from the database and caches the information on startup. During a transaction:

1. Transaction Server calls the Callout framework *after* executing all pre-defined and new rules (in case of Evaluation Callout) or the standard Scoring Engine (in case of Scoring Callout.)

Note: The Callout framework is a part of Transaction Server and just like any other RA Evaluation rule, is loaded during the Server startup. It is implemented as a .dll or .so file.

2. Depending on the type of Callout (**Evaluation** or **Scoring**), the framework collects all the required data from Transaction Server and prepares the HTTP or HTTPS data.

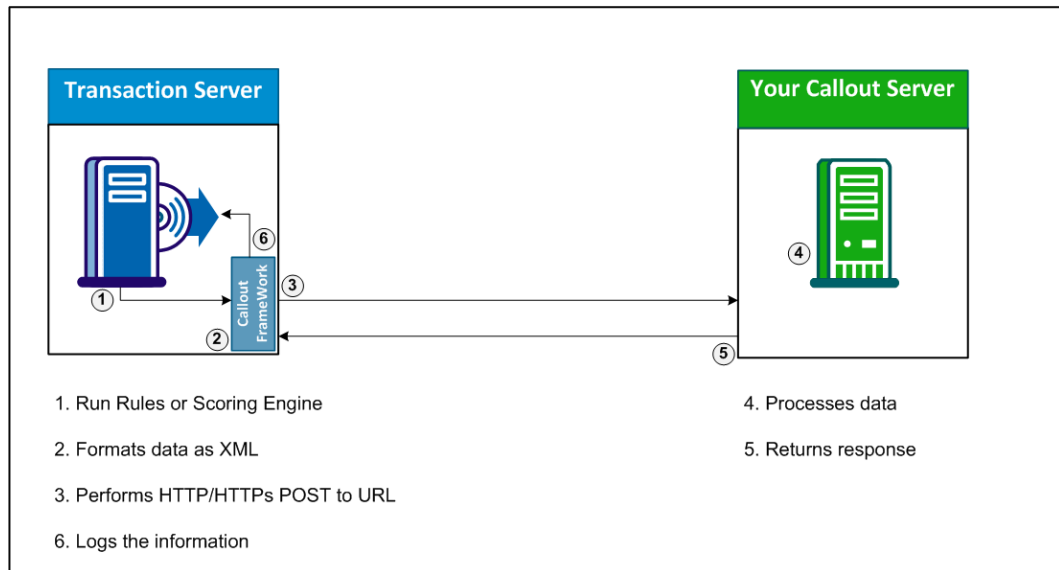
Note: RA supports both one-way and two-way SSL-based connections between Transaction Server and your Callout in case of HTTPS data.

3. This data is then posted (HTTP or HTTPS) to the (configured) URL of your Callout. The Callout framework now waits for a response from the Callout. If the response from your Evaluation Callout is received within a specified time-out period, then the framework parses the response and sends the result to Transaction Server. If the response is not received within the specified time-out period, then the framework returns FAILURE as the rule result and empty strings ("") for the modifier and annotation.

Note: The time-out period can be configured by using Administration Console.

4. Your Callout processes the data by using custom logic.
5. Your Callout then returns an appropriate response to the Callout framework, which forwards the same to Transaction Server.
6. Transaction Server logs all the information returned by the framework for reporting and auditing purposes.

The following figure illustrates the interaction between Transaction Server, Callout Framework, and your Callout.



CAPMRA--9_ca0001

Note: If you are implementing an Evaluation as well as a Scoring Callout, then you can either implement them on the same server or on separate servers.

How to Configure an Evaluation Callout

To configure an Evaluation Callout, perform the following steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Rules Management** section on the side-bar menu, click the **Callout Configuration** link.
The Callout Configuration page appears.
5. Ensure that the **Evaluation Callout** option is selected and click **Next**.
The Evaluation Callout Configuration page appears.
6. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.
The updated Evaluation Callout Configuration page is displayed.
7. In the table, under the **Proposed** column:
 - a. Select the appropriate SSL option for **Server Authentication SSL**.

Important! If you want to configure SSL-based communication between Transaction Server and your Callout, then you must select **YES**.

- b. Select the appropriate SSL option for **Client Authentication SSL**.

Note: The client here is your Callout.

- c. Specify the URL at which the Callout is available against **Callout URL**.
 - If **Server Authentication SSL** is set to **YES** or **Client Authentication SSL** is set to **YES**, then the URL of Evaluation Callout *must* begin with *https://*.
 - If both **Server Authentication SSL** is set to **NO** and **Client Authentication SSL** is set to **NO**, then the URL of Evaluation Callout *must* begin with *http://*.
 - d. Specify the value of **Connection Timeout** in milliseconds.
Connection Timeout indicates the time in which connection between Transaction Server and your Callout will expire.
 - e. Specify the value of **Read Timeout** in milliseconds.
Read Timeout indicates the time in which Transaction Server expects a response back from your Callout.
 - f. Click **Browse** to navigate to the location where the **Callout Server Root Certificate** is located.

Note:

 - If **Server Authentication SSL** is set to YES or **Client Authentication SSL** is set to YES, then you *must* specify the **Callout Server Root Certificate**.
 - **Callout Server Root Certificate** *must* be in PEM (Base64-encoded) format.
 - g. Click **Browse** to navigate to the location where the **Transaction Server Certificate and Private Key** are located.

Note:

 - If **Client Authentication SSL** is set to YES, then you *must* specify the **Callout Server Root Certificate** and **Transaction Server Certificate and Private Key**.
 - **Transaction Server Certificate and Private Key** *must* be in PEM (Base64-encoded) format.
 - h. Specify useful details about the Callout against **Callout Description**.
8. Click **Save** to save the changes that you just made.
 The changes are not yet active, and not available to your end users.
 9. To make the changes active, you must migrate them to production.
 Refer to [How to Migrate to Production](#) for instructions to do so.
 10. Refresh *all* deployed Transaction Server instances.
 See [Refreshing the Cache](#) for instructions on how to do this.

How to Configure a Scoring Callout

To configure a Scoring Callout, perform the following steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.

4. Under the **Rules Management** section on the side-bar menu, click the **Callout Configuration** link.
The Callout Configuration page appears.
5. Select the **Scoring Callout** option and click **Next**.
The Scoring Callout Configuration page appears.
6. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.
The updated Scoring Callout Configuration page is displayed.
7. In the table, under the **Proposed** column:

- a. Select the appropriate SSL option for **Server Authentication SSL**.

Important! If you want to configure SSL-based communication between Transaction Server and your Callout, then you must select **YES**.

- b. Select the appropriate SSL option for **Client Authentication SSL**:

Note: The client here is your Callout.

- c. Specify the URL at which the Callout is available against **Callout URL**.

- If **Server Authentication SSL** is set to **YES** or **Client Authentication SSL** is set to **YES**, then the URL of Evaluation Callout *must* begin with *https://*.
- If both **Server Authentication SSL** is set to **NO** and **Client Authentication SSL** is set to **NO**, then the URL of Evaluation Callout *must* begin with *http://*.

- d. Specify the value of **Connection Timeout** in milliseconds.
Connection Timeout indicates the time in which connection between Transaction Server and your Callout will expire.

- e. Specify the value of **Read Timeout** in milliseconds.
Read Timeout indicates the time in which Transaction Server expects a response back from your Callout.

- f. Click **Browse** to navigate to the location where the **Callout Server Root Certificate** is located.

Note: That:

- If **Server Authentication SSL** is set to **YES** or **Client Authentication SSL** is set to **YES**, then you *must* specify the **Callout Server Root Certificate**.
- **Callout Server Root Certificate** *must* be in PEM (Base64-encoded) format.

- g. Click **Browse** to navigate to the location where the **Transaction Server Certificate and Private Key** are located.

Note: That:

- If **Client Authentication SSL** is set to **YES**, then you *must* specify the **Callout Server Root Certificate** and **Transaction Server Certificate and Private Key**.
- **Transaction Server Certificate and Private Key** *must* be in PEM (Base64-encoded) format.

- h. Specify useful details about the Callout against **Callout Description**.

8. Click **Save** to save the changes that you just made.
The changes are not yet active, and not available to your end users.
9. To make the changes active, you must migrate them to production.
Refer to [How to Migrate to Production](#) for instructions to do so.
10. Refresh *all* deployed Transaction Server instances.
See [Refreshing the Cache](#) for instructions on how to do this.

How to Work with the Sample Callout

RA is shipped with a basic and non-GUI Sample Callouts WAR file (**riskfort-5.0-sample-callouts.war**) that demonstrates:

- The basic operations (invocation and post-processing) of Transaction Server from your custom program.
- The integration of your Callout with RA.

This Sample Callouts WAR file is automatically installed as a part of **Complete** installation of RA. As a part of **Custom** installation, you *must* select the **Transaction Server** component to access this WAR file.

Important! Sample Callouts *must* be deployed on the same application server where Transaction Server is installed.

This topic covers:

- [How to Deploy the Sample Callout](#)
- [How to Configure Transaction Server to Communicate with Sample Callout](#)

How to Deploy the Sample Callout

This topic walks you through the steps for deploying Sample Callouts:

- On Windows
- On UNIX-Based Platforms

On Windows

To deploy the Sample Callouts shipped with RA on your application server:

1. Navigate to **Settings > Control Panel > Administrative Tools > Services**.
2. Stop the application server services.
3. Deploy the **riskfort-5.0-sample-callouts.war** file from the following location:

<install_location>\Arcot Systems\samples\java\

Note: Although you will also see riskfort-5.0-sample-callouts.war in the package, you must deploy the Sample Application WAR file from the preceding location.

4. Navigate to **Settings > Control Panel > Administrative Tools > Services**.
5. Restart the application server services.

On UNIX-Based Platforms

To deploy the Sample Callouts shipped with RA on your application server:

1. Stop the application server services.
2. Deploy the **riskfort-5.0-sample-callout.war** file from the following location:

`<install_location>/arcot/samples/java/`

3. Restart the application server services.

How to Configure the Transaction Server to Communicate with Sample Callout

Note: The XSD for the request and response XML is available in the `<install_location>\Arcot Systems\docs\riskfort\Arcot-RiskFort-5.0-CallOutInterface-xsds.zip` file.

Follow these steps:

1. Perform the tasks listed from Step 1 through Step 5 in [How to Configure an Evaluation Callout](#) to display the **Evaluation Callout Configuration** page.
2. Under the **Proposed** column of the table:

- a. Select **NO** for **Server Authentication SSL**.
- b. Select **NO** for **Client Authentication SSL**.

Note: The client here is the Sample Callout.

- c. Specify the following against the **Callout URL** option:
`http://<host>:<port_number>/riskfort-5.0-sample-callouts/SampleEvalCalloutServe`

Here, `<host>` refers to the host name or IP address of the server where your Callouts WAR is deployed and `<port_number>` refers to the port on which this server is available.

- d. Specify the value of **Connection Timeout** in milliseconds. The default value is 30000 milliseconds.
 - e. Specify the value of **Read Timeout** in milliseconds. The default value is 30000 milliseconds.
 - f. Specify useful details about the Callout against **Callout Description**.
 - g. Click **Save** to save the changes that you just made.
3. Perform the tasks listed from Step 1 through Step 5 in [How to Configure a Scoring Callout](#) to display the **Scoring Callout Configuration** table.
 4. Under the **Proposed** column of the table:

a. Select **NO** for **Server Authentication SSL**.

b. Select **NO** for Client Authentication SSL.

Note: The client here is the Sample Callout.

c. Specify the following against the **Callout URL** option:

http://<host>:<port_number>/riskfort-5.0-sample-callouts/SampleScoringCalloutSei

Here, <host> refers to the host name or IP address of the server where your Callouts WAR is deployed and <port_number> refers to the port on which this server is available.

d. Specify the value of **Connection Timeout** in milliseconds. The default value is 30000 milliseconds.

e. Specify the value of **Read Timeout** in milliseconds. The default value is 30000 milliseconds.

f. Specify useful details about the Callout against **Callout Description**.

g. Click **Save** to save the changes that you just made.

All the changes that you made until now are not yet active, and not available to your end users.

5. To make the changes active, you must migrate them to production. Refer to [How to Migrate to Production](#) for instructions to do so.

Managing Users

RA works with your application to manage strong authentication for administrators and end users. RA allows you to create users directly through Administration Console. Managing user information is a critical part of maintaining a secure system. The end user management operations supported by RA for this purpose include:

- [How to Create a User](#)
- [How to Search for Users](#)
- [How to Update User Information](#)
- [How to Promote a User to Administrator](#)
- [How to Configure Account IDs for Users](#)
- [How to Deactivate a User Account](#)
- [How to Temporarily Deactivate a User Account](#)
- [How to Activate a User Account](#)
- [How to Delete a User Account](#)

Note: In RA, it is highly recommended that user management tasks discussed in this article be performed by a User Administrator (UA).

How to Create a User

Every end user of your online application system is referred to as a user in Administration Console. Global Administrators (GAs), Organization Administrators (OAs), and User Administrators (UAs) can create users for organizations within their scope.

To create a user in the system:

1. Ensure that you are logged in with the required privileges and scope to create the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create User** link to display the Create User page.
4. In the **User Details** section, enter the details of the user. The following table explains the fields on this page.

Field	Description
User Name	The unique user name.
Organization	The display name of the organization to which the user belongs.
First Name (optional)	The first name of the user.
Middle Name (optional)	The middle name, if any, of the user.
Last Name (optional)	The last name of the user.

5. In the **Email Address(es)** section, enter the email address of the user.
6. In the **Telephone Number(s)** section, enter the phone number to contact the user.
7. Select whether you want the user to be in the **Initial** state or you want to make the user **Active**.
8. In the **Custom Attributes** section, enter the **Name** and **Value** of any attributes you want to add, such as office location.
9. Click **Create User** to create the user.

How to Search for Users

To search for users:

1. Ensure that you are logged in with the appropriate scope.

2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Specify the search criteria to display the list of users. You can:
 - Search for users by specifying the partial or complete information of the user in the fields on this page.

Note: Specifying partial information in the fields works only if the fields are *not* marked for encryption. If any of the fields on this page have been marked for encryption, then you *must* specify the complete value for the search to function properly.
 - Search for users by specifying the organization's Display Name.
 - Search for users by not specifying any criteria and just clicking **Search**.
 - Click the **Advanced Search** link to display the Advanced Search page to search for users by specifying their Status or Role.
5. Specify the required details of the users and click **Search**.
A list of users matching the search criteria appears.

Privileges Required

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

How to Update User Information

To update user information:

1. Ensure that you are logged in with the required privileges and scope to update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user whose account you want to update and click **Search**.
A list of administrators matching the search criteria appears.
5. Click the `<user name>` link of the user whose account you want to edit.
The Basic User Information page appears.

Note: The Basic User Information page also displays the **User Account Information (Account Type, AccountID, and Status)** if any account type was configured.
6. Click **Edit** to change the user information on this page.

7. In the **User Details** section, edit the required fields (**First Name, Middle Name, Last Name**).
8. In the **Email Address(es)** section, edit the email addresses for the email types configured for the organization.
9. In the **Telephone Number(s)** section, edit the telephone numbers for the telephone types configured for the organization.
10. Update the **User Status**, if required.
11. Edit the **Name** and **Value** of **Custom Attributes**, if required.
12. You can either click **Save** to save the changes made and return to the User Information page, *or* you can click **Next** to proceed with additional configurations.

Note: The **Next** button is available only if you have configured accounts for the organization.

If you click **Next**, then the User Account page appears.

13. In the **User Account** section:
 - Edit the **Status**, if required.
 - Expand **Advanced Attributes** to add **AccountID Attributes** and **Custom Attributes** for the account ID.
- Note:** If this is the first account ID you are creating, you must click **Add** to add an account ID before you can update it. For more information about adding an account ID, see [Create Account IDs](#).
14. Click **Update** to save your changes.

Privileges Required

To update a user's account settings, you must ensure that you have the appropriate privileges and scope. The MA can update information of any user. The GAs can update all users in their scope. The OAs and UAs can update information for users in their purview.

How to Promote a User to Administrator

To promote a user to an administrator:

1. Ensure that you are logged in with the required privileges and scope to create administrators and update the user information.
2. Activate the **Users and Administrators** tab.
3. Enter the partial or complete information of the user whose account you want to update and click **Search**.
A list of users matching the search criteria appears.
4. Click the *<user name>* link of the user whose account you want to edit.
The Basic User Information page appears.

5. Click **Edit** to open the Update User page.
6. If the user's **First Name**, **Last Name**, **Email address(es)**, **Telephone Number(s)** are not specified, enter the same. These attributes are mandatory for administrators.
7. Click **Next** to display the User Account page.

Note: If no account type is configured for the user's organization, then the **Change Role to Administrator** button is displayed in the Update User page itself.

8. On the User Account page, click **Change Role to Administrator** to display the Create Administrator page.
 9. On this page:
 - Specify the role of the new administrator from the **Role** drop-down list.
 - Enter the password for the administrator in the **Password** and **Confirm Password** fields.
 - In the **Manages** section, select the organizations that the administrator will have scope on, and perform the following:
 - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.
or
 - Select the required organizations from the **Available Organizations** list and click the > button to add these organization to the **Selected Organizations** list.
- The **Available Organizations** list displays *all* the organizations that are available in the scope of the logged in administrator. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.
10. Click **Create** to save the changes and create and activate the administrator.

Privileges Required

To promote a user to an administrator, you must ensure that you have the appropriate privileges and scope. The MA can promote any user. The GAs can promote users to OA, UA, or GA for organizations within their administrative purview. The OAs can promote users to OA or UA for organizations within their administrative purview. The *UAs cannot* promote users to administrators.

How to Configure Account IDs for Users

In addition to the user name, an *account ID* is an alternate way to identify a user in the RA system. After you have configured the account types that your organization will use, you can associate one account ID per user for any of these account types. For more information about account types, see [Configuring the Account Type](#).

Privileges Required

To configure an account ID for an account type, you must ensure that you have the appropriate privileges and scope to update the user. The MA can update any user. The GAs can update all users in their scope. The OAs and UAs can update the users in their purview.

How to Create Account IDs

You can create an account ID for any of the account types that you have configured.

To create an Account ID:

1. Ensure that you are logged in with the required privileges and scope to update the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user for whom you want to create the account ID, and click **Search**.
You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).
The Search Results page appears, with all the matches for the specified criteria.
5. Click the *<user name>* link of the user whose account you want to edit.
The Basic User Information page appears.

Note: This page also displays the **User Account Information (Account Type, AccountID, and Status)** for the account types configured.

6. Click **Edit** to open the Update User page.
 7. Click **Next** to display the User Account page.
 8. Select the **Account Type** for which you want to add the account ID.
 9. Specify the unique **AccountID** in the text box.
This combination of account type and account ID will be used to identify the user in addition to the user name. You must ensure that the account type and account ID combination is unique for a particular organization.
 10. Select the **Status** of the user account from the drop-down list.
 11. If required, expand the **Advanced Attributes** section, and do the following:
 - a. Provide **AccountID Attributes** for the account ID.
 - b. Provide values for any **Custom Attributes** that are configured for the account type.
- Note:** You can specify up to a maximum of three **AccountID Attributes** for any account ID.
12. Click **Add** to add the account ID.

How to Update Account IDs

Note: You cannot change the account ID once it is created. You can only change the status of the user account and add account ID attributes.

To update an existing account ID:

1. Complete Step 1 through Step 7 in [Create Account IDs](#) to display the User Account page.
2. Select the **Account Type** for which you want to update the account ID.
3. If required, change the **Status** of the user account from the drop-down list.
4. If required, expand the **Advanced Attributes** section, and provide **AccountID Attributes** and **Custom Attributes** for the account ID you are updating.
5. Click **Update** to save your changes.

How to Delete Account IDs

To delete an account ID:

1. Complete Step 1 through Step 7 in [Create Account IDs](#) to display the User Account page.
2. Select the **Account Type** for which you want to delete the account ID.
3. Click **Delete** to delete the account ID.

How to Deactivate a User Account

To prevent a user from logging in to their account for security reasons, you can deactivate them instead of deleting them. If you deactivate users, then they are locked out of their account, and cannot log in unless they are activated again.

To deactivate a user account:

1. Ensure that you are logged in with the required privileges and scope to deactivate the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user whose account you want to disable and click **Search**.
You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).
The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users to deactivate.
6. Click **Deactivate** to deactivate the selected user.

Privileges Required

To deactivate a user, you must ensure that you have the appropriate privileges and scope. The MA can deactivate any user, while the GAs can deactivate all users (including other GAs) within their scope. The OAs and UAs can deactivate all users in their purview.

How to Temporarily Deactivate a User Account

Temporarily deactivating the user differs from *deactivating* the user (See [How to Deactivate a User Account](#)). When you temporarily deactivate the user, the user is automatically activated when the end of the lock period is reached. But when you deactivate a user, you must manually activate them again whenever you want to provide access to the user.

To temporarily deactivate a user, you specify the **Start Lock Date** and **End Lock Date** for which the user is locked. When the **End Lock Date** is reached, the user is automatically activated.

To temporarily deactivate a user account:

1. Ensure that you are logged in with the required privileges and scope to deactivate the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user to deactivate and click **Search**. You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive). The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users to deactivate temporarily.
6. Click **Deactivate Temporarily**.
7. The Deactivate User Temporarily page appears.
8. In the **Starting From** section, select the start lock **Date** and **Time**.
9. In the **To** section, select the end lock **Date** and **Time**.
10. Click **Save** to save your changes.

Note: If you do not specify any value for the **Starting From** fields, the user is locked from the current time. If you do not specify an end lock **Date**, the user is locked forever.

Privileges Required

To temporarily deactivate a user, you must ensure that you have the appropriate privileges and scope. The MA can deactivate any user, while the GAs can deactivate all users (including other GAs) within their scope. The OAs and UAs can deactivate all users in their purview.

How to Activate a User Account

You might need to activate a deactivated user. For example, you might deactivate an administrator if the administrator is on long vacation. This helps to prevent unauthorized access to that administrator's information.

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

To activate a deactivated user account:

1. Ensure that you are logged in with the required privileges to activate the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).
The Advanced Search page appears.
5. Enter the partial or complete information of the user in **User Details** section.
6. In the **User Status** section, for **Current Users**, select the **Inactive** and **Initial** options to search for all inactive or initial users.
7. Click **Search** to display the list of all users matching the search criteria.
8. Select the users you want to activate.
9. Click **Activate** to activate the user.

Privileges Required

To activate a user, you must ensure that you have the appropriate privileges and scope. The MA can activate any user, while the GAs can activate all users within their scope. The OAs and UAs can activate all users in their purview.

How to Delete a User Account

User information in RA includes personal information (first name, middle name, last name, email address, and telephone number), credentials, and accounts. When you delete a user from Administration Console, the credential and account information must also be deleted along with the personal information. RA supports the cascaded user deletion feature by which all credential, account, and risk-related information for a user is also deleted when the user is deleted.

If you create a new user with the same name as a previously deleted user, then 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.

To delete a user account:

1. Ensure that you are logged in with the required privileges to delete the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user you want to delete and click **Search**.
You can also click the **Advanced Search** link to search for users based on their status (active, inactive, or initial) or their roles (User).
The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users you want to delete.
6. Click **Delete**.

Note: After you delete a user, the user information is deleted from the database. However, the user history is archived for billing purposes.

Privileges Required

To delete a user, you must ensure that you have the appropriate privileges and scope. The MA can delete any user, while the GAs can delete all users (including other GAs), *except* the MA account, within their scope. The OAs and UAs can delete all users in their purview.

Managing Rules

This article discusses the basics of RA rules, rulesets, and the Rule Builder. It covers the following topics:

- [Understanding the Building Blocks of Rules](#)
- [Understanding the Data RA Uses](#)
- [Understanding RA Predictive Model](#)
- [Working with Rulesets](#)
- [Working with Out-of-the-Box Rules](#)
- [Creating Custom Rules by Using Rule Builder](#)
- [Understanding the Types of Operators Used by the Rule Builder](#)
- [Using Geolocation and Anonymizer Data in Rules](#)
- [Understanding Currency Conversion](#)
- [Understanding Data Elements](#)

Understanding the Building Blocks of Rules

This topic explains the basic concepts that you need to understand before you build any rules and covers the following sub-topics:

- [Basic Rule Concepts](#)
- [How Does Rule Engine Work](#)
- [State Diagrams](#)

Basic Rule Concepts

Before you build a rule, you must understand these basic concepts:

What Are Rules

Each *rule* is a pre-configured logic that returns a Boolean value. For a risk evaluation request from your application, this logic is applied to the incoming transaction data in the request. Each rule returns TRUE if the rule matched, and FALSE, if it did not.

Important! During scoring, Evaluation rules are scored in the order of priority until a match is detected.

Characteristics of a Rule

Every rule in RA has three specific characteristics that govern how the rule is processed:

- **Ruleset**
Each rule *must* belong to a Ruleset. This choice of the Ruleset determines the options that are available for a rule.
- **Rule Implementation** (at global or organization level)
This characteristic determines whether the rule is applicable at the global level (available as a template to organizations) or at the level of individual organizations.
- **Rule Type**
This characteristic determines the capability and scope of the rule, and is closely associated with [Custom Rules](#) added by using the Rule Builder.

Types of Rules Supported in RA

RA uses rules to evaluate the risk associated with each transaction. These rules can be broadly categorized into the following categories:

- [Out-of-the-Box Rules](#)
- [Custom Rules](#)

Out-of-the-Box Rules

These are *terminating rules*. In other words, if any Evaluation rule matches (returns True) during scoring, then the Risk Engine stops scoring the following rules in this category and generates a Risk Score corresponding to the matched rule.

The out-of-the-box rules can be categorized as:

- [Configurable Predefined Rules](#)
- [Non-Configurable Predefined Rules](#)

Configurable Predefined Rules

The following table lists the out-of-the-box rules that are installed and deployed by default when you install RA.

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
Exception User Check	EXCEPTION	An organization may choose to temporarily exclude a user from risk evaluation for a specified time interval. For example, a user might need to travel to a Negative Country. Such users are added to the <i>Exception User List</i> , and are referred to as <i>exception users</i> .

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
		If found in the Exception User List, by default, RA returns a low Score and the ALLOW advice for the transactions originating from exception users.
Untrusted IP Check	UNTRUSTEDIP	<p>This list constitutes the IP addresses that originate from anonymizer proxies or have been the origin of known fraudulent or malicious transactions in the past.</p> <p>Transactions originating from configured negative IP addresses receive a high score and the advice is Deny.</p>
Negative Country Check	NEGATIVECOUNTRY	<p>This list comprises the countries that have been known to be origins of significant number of frauds in the past.</p> <p>RA derives the country information based on the input IP address, and then uses this data to return a high risk score for online transactions originating from these "negative" countries.</p> <p>Transactions originating from configured negative countries receive a high score and the advice is Deny.</p>
Trusted IP/Aggregator Check	TRUSTEDIP	<p>Transactions originating from IP addresses "trusted" to the organization receive a low score, by default, and the advice is Allow.</p> <p>Many enterprises use the services of account and data aggregation service providers to expand their online reach. The originating IP addresses when users log in from a protected portal versus when they come in through such aggregators are different.</p>

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
		Transactions originating from aggregators "trusted" to the organization receive a low score, by default, and the advice is Allow.
Device MFP Match	SIGMATCH	<p>Checks if the match percentage between the input signature and the corresponding stored signature is GREATER_OR_EQUAL to a specified Signature Pass Threshold.</p> <p>Note: The short form of MFP must be passed along with long form of MFP for risk evaluation. The SIGMATCH rule does not trigger if only short form of MFP is passed.</p>
User Velocity Check	USERVELOCITY	<p>Frequent use of the same user ID could be an indication of risky behavior. For example, a fraudster might use the same user ID and password from different devices to watch a specific activity in a targeted account.</p> <p>Too many transactions originating from the same user within a short (configurable) interval receive a high score and the advice is Deny.</p>
Device Velocity Check	DEVICEVELOCITY	<p>Frequent use of the same device could also be an indication of risky behavior. For example, a fraudster might use the same device to test multiple combinations of user IDs and passwords. Administrators can now configure RA to track this behavior, as well.</p> <p>Too many transactions originating from the same user device within a short (configurable) interval receive a high score and the advice is Deny.</p>
Zone Hopping Check	ZONEHOPPING	

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
		<p>If a user logs in from two long-distance locations within a short time span by using the same user ID, this might be a strong indication of fraudulent activity.</p> <p>In addition, a User ID can also be shared, in which case, RA understands that the two people sharing the same User ID can be in geographically different locations and responds with an appropriate response.</p> <p>Transactions originating from the same user from locations that are far apart from each other within a short (configurable) interval receive a high score and the advice is Deny.</p>

Non-Configurable Predefined Rules

In addition to the preceding configurable rules, Risk Analytics also provides the following non-configurable rules. The following table lists the out-of-the-box non-configurable rules that are installed and deployed by default when you successfully install and configure RA.

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
User Known	USERKNOWN	<p>A known user is already registered in the RA database.</p> <p>If the user does not exist in the Risk Analytics database, then Risk Analytics returns ALERT. In this case, your application can either call the Risk Analytics API to create the user in Risk Analytics, or take an appropriate action.</p>
DeviceID Known	DEVICEIDCHECK	<p>The Device ID is a device identifier string that RA generates and stores as a cookie on the end user's system to identify and track the device that the end user uses for logging in to your online application to perform transactions.</p>

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
		RA returns a low risk score for transactions originating from known devices and the advice is typically ALLOW. In other words, if a device (whose transaction is being evaluated) exists in the Risk Analytics database.
		This information is used for Machine FingerPrint match.
User Associated with DeviceID	USERDEVICEASSOCIATED	Transactions originating from a known device (in other words, corresponding User-Device association exists in the RA database) that is associated with a user, and whose DeviceDNA matches, receive a low score, and the advice is ALLOW.
		Transactions originating from a known device that is not associated with a known user receive a medium score, and the advice is INCREASEAUTH.

Custom Rules

In RA, new customized rules and logic can be either built by using the Rule Builder or can be built using Callouts. This section walks you through the two ways you can build a new rule or logic in RA. It covers the following topics:

- [Custom Rules Built Using Rule Builder](#)
- [Custom Evaluations Built Using Callouts](#)

Custom Rules Built Using Rule Builder

The out-of-the-box rules in RA are generic and are configured for evaluating risk based on the rules that are applicable to all. If you need industry-specific rules that are significantly different from those that RA provides out-of-the-box, then you need to build and deploy your own rules by using the **Rule Builder**.

Important! Unlike the out-of-the-box rules, these rules are installed, but not deployed automatically. [Creating Custom Rules by Using Rule Builder](#) guides you through the process of building custom rules.

Custom Evaluations Built Using Callouts

Based on your business requirements, you can write your own custom Evaluation logic and Scoring logic, which if implemented, will run at your application-end, independent of RA Transaction Server. These custom Evaluation or Scoring programs are known as *Callouts* that can also be implemented to interact with your application's back-end system.

The Callout framework is a part of Transaction Server and just like any other RA Evaluation rule, is loaded during the Server startup. It is implemented as a **.dll** or **.so** file.

Note: RA is shipped with a basic **Sample Callouts WAR file (riskfort-5.0-sample-callouts.war)** that demonstrates how you can write and implement simple Evaluation and Scoring Callouts.

Example of Callout Implementation

For example, in addition to tracking the origin of each transaction, a banking institution would also like to assess the risk of regular bank transactions and wire transfers based on the transaction amount. Say, the bank would like to evaluate all transactions more than \$30,000 for risk, irrespective of whether they are regular transactions or wire transfers. In this case, in addition to using RA's Negative Country, Untrusted IP, Zone Hopping, and Velocity checks, the institution can write an Evaluation Callout (within the scope of their application) to track this behavior.

What are Evaluation Callouts

Based on your business requirements, you can also write your own custom Evaluation logic, which will run at your application-end, outside of the context of the Transaction Server. RA executes this custom Evaluation Callout *after* all the out-of-the-box rules and your new rules have been executed. This Callout accepts results of all previous rules and Additional Inputs as input and returns:

- A **response** (SUCCESS/FAILURE)
- A **modifier string** (extra information to be used by the [Scoring Callout](#))
- An **annotation string** (the reason or the description returned back to Transaction Server by your Callout implementation module).

Note: See [Configuring RA Callouts](#) for detailed information on working with Evaluation Callouts.

How Evaluation Callouts Work

An Evaluation Callout is executed as part of risk evaluation. If an Evaluation Callout is implemented, then:

1. RA executes all Standalone and Combination rules and invokes the Callout framework.
2. The RA Callout framework formats the data in XML format.
3. The RA Callout framework performs an HTTP or HTTPS POST of the following information to your Evaluation Callout:
 - **Context information** (such as User name, IP address, and Device ID) that is passed to each RA Evaluation rule.
 - **Rule results** for each Evaluation rule that was executed.

- **Additional Inputs**, if any, that are provided by the RA SDK to Transaction Server as input data.
4. Your Callout uses the data passed by RA to process its custom logic.
 5. Your Callout then returns the following information to RA:
 - **Rule result** in the form of Y (SUCCESS) or N (FAILURE).
 - **Modifier string** with additional information, if any, to be used by the Scoring Callout (if implemented.)

Note: Transaction Server does not process the modifier string at all. If a Scoring Callout also has been implemented, then Transaction Server POSTs this data to the Scoring Callout.

 - **Annotation string** that contains the reason or the description sent back to Transaction Server.

Note: This information is used for logging (in the database), reporting, and auditing purposes.
 6. Transaction Server logs the information returned by your Callout.

What are Scoring Callouts

Based on your business requirements, RA also provides you the flexibility to add your own custom scoring logic, in addition to RA's standard scoring logic. You can do so with the help of **Scoring Callout**. By implementing a Scoring Callout, you can write your own custom scoring logic to process the Score, Advice, and risk-evaluation results generated by RA's standard scoring program. The Scoring Callout then returns the final risk Score, which can differ and will override the Score computed by RA's standard Scoring Engine.

Like the [Evaluation Callout](#), Scoring Callout is a custom rule that executes *last*, after the standard RA scoring program is completed and returns a final Score and Advice.

Note: See [Configuring RA Callouts](#) for detailed information on working with Scoring Callouts.

How Scoring Callouts Work

A Scoring Callout is executed *after* the standard RA Scoring logic has executed. If a Scoring Callout is implemented, then:

1. Transaction Server executes the standard Scoring program and invokes the Callout framework.
2. The RA Callout framework formats the data in XML format.
3. The RA Callout framework performs an HTTP or HTTPS POST of the following information to your Scoring Callout:
 - **Overall Score** computed by the standard RA built-in Scoring Engine.
 - **Rule results** for each Evaluation rule that was executed.
 - **Additional Inputs**, if any, that are provided by the calling application as part of the `evaluateRisk()` API call.

- **Modifier string** originally returned by the Evaluation Callout.
4. Your Callout uses the data passed by RA to process its custom logic.
 5. Your Callout then returns the following information to RA:

- **Final Score** in the form of an integer in the range [0 - 100].

Note: The score returned by the Scoring Callout always overrides the Score computed by the RA Scoring Engine. If you want to retain the score computed by the RA standard Scoring Engine, then you will need to pass that same Score as the return value in your response. This information is used for logging (in the database), reporting, and auditing purposes.

6. Transaction Server logs the information returned by your Callout.

How Are Callouts Implemented

Note: Implementation of Callouts is optional.

If you have implemented a Callout, then Transaction Server reads all configurations related to the Callout from the database and caches the information on startup. During a transaction:

1. Transaction Server calls the Callout framework *after* executing all pre-defined and new rules (in case of Evaluation Callout) or the standard Scoring Engine (in case of Scoring Callout.)

Note: The Callout framework is a part of Transaction Server and just like any other RA Evaluation rule, is loaded during the Server startup. It is implemented as a .dll or .so file.

2. Depending on the type of Callout (**Evaluation** or **Scoring**), the framework collects all the required data from Transaction Server and prepares the HTTP or HTTPS data.

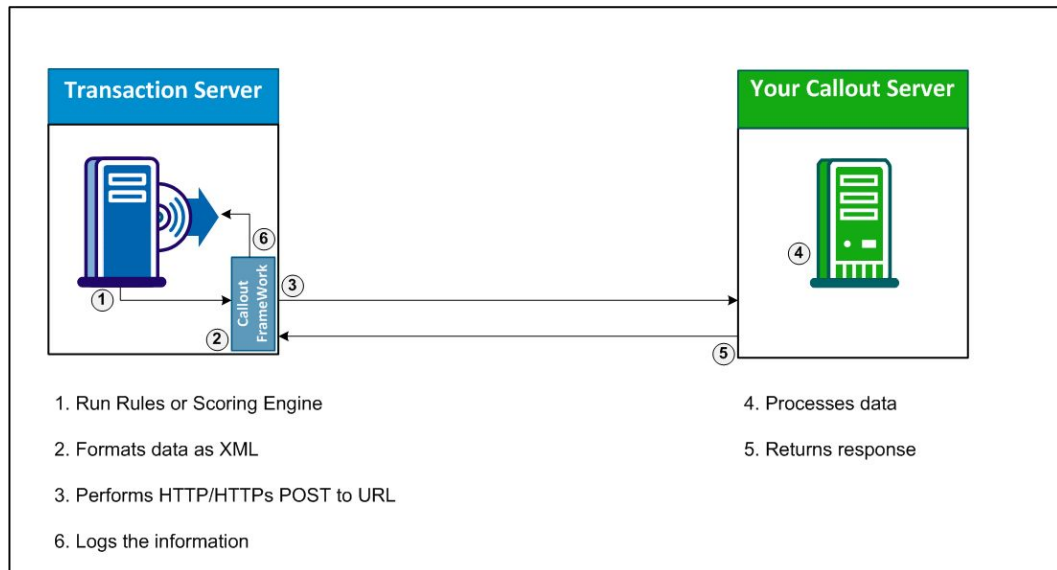
Note: RA supports both one-way and two-way SSL-based connections between Transaction Server and your Callout in case of HTTPS data.

3. This data is then posted (HTTP or HTTPS) to the (configured) URL of your Callout. The Callout framework now waits for a response from the Callout. If the response from your Evaluation Callout is received within a specified time-out period, then the framework parses the response and sends the result to Transaction Server. If the response is not received within the specified time-out period, then the framework returns FAILURE as the rule result and empty strings ("") for the modifier and annotation.

Note: The time-out period can be configured by using Administration Console.

4. Your Callout processes the data by using custom logic.
5. Your Callout then returns an appropriate response to the Callout framework, which forwards the same to Transaction Server.
6. Transaction Server logs all the information returned by the framework for reporting and auditing purposes.

The following figure illustrates the interaction between Transaction Server, Callout Framework, and your Callout.



callout_impl

What are Rulesets

A *ruleset* is a collection of one or more configured RA rules, along with their execution order and scoring priority. Each ruleset can be different from the other in terms of:

- Set of configured rules
- Score and priority for each rule in the set
- Enabling or disabling of rules in the set
- Configured parameters and data for each rule

In simple terms, a ruleset is a parent container that constitutes one or more rules. Even if you have configured a rule in RA, it will not be executed unless it belongs to a ruleset. In other words, every rule - out-of-the-box or custom - must belong to a ruleset.

As a GA, you can configure multiple global rulesets that are available to all the organizations. These rulesets can then be used by other GAs or OAs of these organizations to create new rulesets simply by "copying from" an existing ruleset. In addition, the "copied" rules within a ruleset can also be edited. This not only significantly saves the time and effort required for individually configuring each rule again for organizations, but also reduces the number of errors.

Note: RA is shipped with an out-of-the-box global ruleset called **DEFAULT**.

What Are Channels

An end user can perform a transaction in many ways. Some of these include:

- Online (Transactions that originate when the user uses a credit card or a debit card online, but the transaction is not governed by 3D Secure protocol.)
- 3D Secure (Transactions that originate when the user uses a credit card or a debit card online.)
- Online banking (Transactions that originate when the user logs into their banking site, without using a credit card.)

- Online wire transfers (Transactions that originate when the user transfers money.)
- App (Transactions that originate when the user uses a smartphone app.)
- SMS (Transactions that originate using SMS messaging.)
- ATM (Transactions that originate at an ATM machine.)
- POS (Transactions that originate at a store's or shop's point of sale.)

These different origins of transactions are referred to as *channels* in RA terminology.

RA can be configured to evaluate risk for transactions coming from any of these channels. It can also be configured to evaluate transactions from each channel differently to generate a risk score. In addition, an RA rule can be evaluated across different channels to arrive at a score. This is known as *cross-channel* configuration.

RA supports the channels listed in the following table.

Channel	Description
DEFAULT	Transactions that are initiated using a Web browser. This may be either a computer, smart phone, tablet, or set-top box. The default channel is the Web channel.
3D Secure	Online transactions initiated using credit card or debit card.
ATM	<p>Transactions initiated through ATM.</p> <p>ATMs are terminals primarily used as an alternate channel for availing banking services, such as account balance inquiry or cash withdrawal.</p>
POS	<p>Transactions initiated at physical Point of Sale (POS).</p> <p>POS terminals are primarily used as channels for recording a financial payment made by the card holder to a merchant for goods or services purchased by the card holder from the merchant</p>
IMPS	<p>Transactions initiated using Immediate Payment Service (IMPS), a channel-agnostic payment service.</p> <p>Using IMPS, bank customers can transfer money instantly within any of the IMPS-enabled member banks across India. IMPS is accessible through mobile banking, net banking, and ATM channel.</p> <p>IMPS can be used for funds transfer and merchant payments. It supports the following services:</p> <ul style="list-style-type: none"> ▪ P2P: Person to Person

Channel	Description
	<ul style="list-style-type: none"> ▪ P2A: Person to Account ▪ P2M (Push): Person to Merchant initiated by Customer ▪ P2M (Pull): Person to Merchant initiated by Merchant
ECOM	Ecommerce transactions received as ISO 8583 messages.

What Is Predictive Model

Predictive Model is RA's advanced fraud modeling capability. A pre-defined Model is not shipped with RA, but you need to build it using the historical data and then deploy it. In this way, a Model deployment is like deploying a Custom Rule, which is an additional rule and needs to be similarly created and deployed.

By using the available transaction data and system data, the Model generates a score that describes the extent to which the model suspects a transaction's genuineness. This score typically ranges from 0 through 100, where the higher the number, the greater the possibility of fraud. RA can be configured to send different responses to your calling application based on this model score.

The model score is available as a part of the system parameters (as **ModelScore**) while configuring rules on the Rules and Scoring Management page in Administration Console. This score can be used in conjunction with other data elements to arrive at a risk advice.

RA publishes an interface specification called **Predictive Model Integration Interface**, and can support any Model platform that conforms to the same. Currently, the following Model platforms are supported:

- Global Decisioning Platform (GDP) v2.7.4
- Data Science Platform (DSP) v1.0

Model Deployment Options

- RA can connect simultaneously to one or more types of Model platforms or to one or more instances of the Model platform.
- Each organization can either have their own Model setup or share the same model setup, as long as one organization has exactly one model setup.

What Is Rules Engine

After RA collects the data (discussed in section, [Understanding the Data RA Uses](#)) for risk evaluation, it is forwarded to *Rules Engine* (a module of Transaction Server). Rules Engine executes the configured rules in the order of their priority.

The Rules Engine generates an individual risk score and advice for each rule it executes and then passes it to the [Scoring Engine](#).

What Is Scoring Engine

Scoring Engine is a module of Transaction Server that works with [Rules Engine](#). It accepts the input from the Rules Engine, evaluates the score of each rule in the order of priority set (by the administrator).

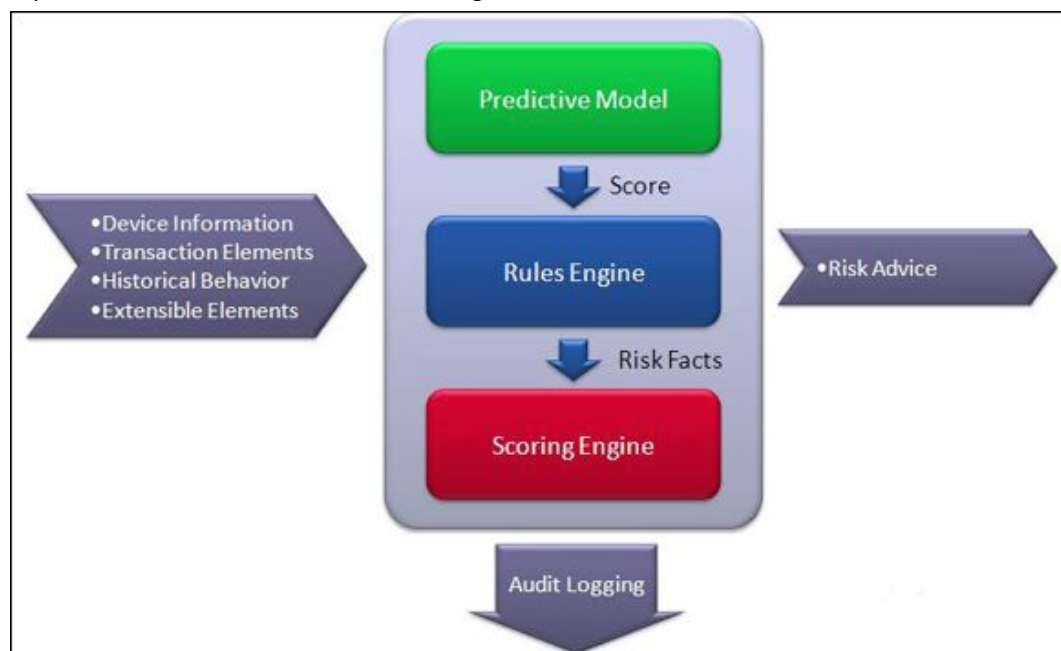
The *risk score* generated by the Scoring Engine is an integer from 0 through 100. Scoring Engine then uses this risk score to generate the corresponding *advice* and returns this advice to your application.

What Is Rule Priority

RA evaluates and scores each configured and active rule in the specific order of its priority.

For example, if the priority of a rule is set as 3, then it will be evaluated only after rules with priority 1 and 2 have been run.

By default, RA assigns a priority for each out-of-the-box rule, but based on your business requirements, you can change this priority of rule scoring. The following figure is a schematic representation of RA rules and their scoring order.



rule_priority

How Does Risk Score Work

Based on the result of the execution of each rule that Rules Engine provides, the Scoring Engine evaluates the score of each rule in the order of priority set (by the administrator) and returns the score corresponding to the first rule that matched.

Scoring Example

Consider that you have configured these rules in the following order:

1. Negative IP (say, with a score of 85)

2. User Velocity (say, with a score of 70)
3. High Amount Check (say with a score of 80)
4. Device Velocity (say, with a score of 65)

Note: High scores are typically assigned to rules that are more critical.

If RA determines that a transaction is coming from a risky IP address, then it returns a score of 85 (Deny), based on the first configured rule that matched. If another transaction exceeds the configured Device Velocity, then RA returns a score of 65.

The *risk score* generated by the Scoring Engine is an integer from 0 through 100. RA then uses this risk score to generate the corresponding *advice* and returns this advice to your application.

Scoring Matrix

The following table shows the default out-of-the-box risk score and corresponding advice matrix. You can configure these ranges according to your organization policies and requirements.

Score Value (From)	Score Value (To)	Advice	Default Recommended Action
0	30	ALLOW	Allow the transaction to proceed.
31	50	ALERT	Take an appropriate action. For example, if the user name is currently unknown, then on getting an alert you can either redirect it to a Customer Support Representative (CSR) or you can create a user in RA.
51	70	INCREASEAUTH	Perform additional authentication before proceeding any further.
71	100	DENY	Deny the transaction.

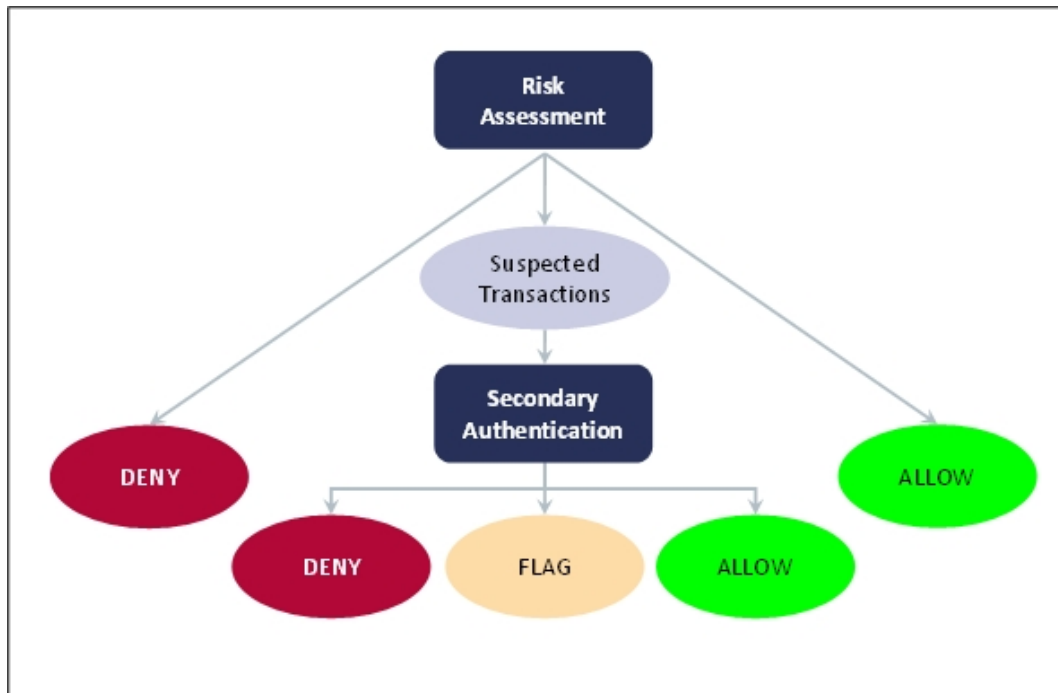
What Does Risk Advice Mean

Based on the Risk Score generated by RA, *risk advice* can be one of the following:

- **ALLOW:** RA returns ALLOW, if the risk score associated with the transaction is low.
- **ALERT:** If a user who is not registered with RA tries to log in, then ALERT is returned.

- **INCREASE AUTHENTICATION:** When RA detects a suspicious transaction, it flags the transaction with INCREASE AUTHENTICATION and advises the application to force the user for additional authentication.
For example, when a user registered with RA attempts a transaction from a device that is not yet recognized by RA, then the user must undergo secondary authentication (such as OTP or QnA) with your application.
- **DENY:** RA returns the DENY advice when a high risk score is associated with the transaction.

The following figure illustrates the advices returned by RA:



what_risk_Advice_mean

How Does Rule Engine Work

The working of Rules Engine is explained with the help of the following topics:

- [How are Rules Triggered](#)
- [How Rule Engine Uses Model to Calculate Model Score](#)
- [How Rules Engine Uses Rules to Calculate a Risk Score and Advice](#)

How Are Rules Triggered

If the incoming information from a login attempt or a transaction satisfies a condition configured for a rule, then the rule fires. In RA terminology, a rule that is triggered is also referred to a "matched rule".

RA executes all configured and enabled rules in the parent ruleset. However, it scores the first matched rule and returns the risk score and advice of the rule that matched as final.

See section, "[How Rules Engine Uses Rules to Calculate a Risk Score and Advice](#)" to understand the process RA uses to arrive at the final risk score and advice.

How Rule Engine Uses Model to Calculate Model Score

RA allows for an organization-level (or tenant-level) usage of the Predictive Model through the **Model Callout** feature. The Model Callout is executed, if the Model is configured for the specified organization. It is executed *after* all the system rules are executed and *before* the execution of any custom rules you might have deployed. The output of the Model is made available as **Predictive_Score** for the Rule Engine. This value can be used to create other rules, if required.

RA expects a numerical value between 0 and 1 as the Model Score from the Model, representing the probability of the transaction being a fraudulent. Because this score is multiplied by a factor prior to making the same available to the Rule Engine for risk evaluation, the Model Score received from the Model is referred to as **Raw Model Score**. The multiplication factor is called **Score Multiplication Factor**.

Valid Raw Model Score: All score output values between 0 and 1 (both inclusive)

Invalid Raw Model Score: Any score output values less than 0 or greater than 1

DSP Model Score Multiplication Factor

DSP's Raw Model Score (**PREDICTIVE_SCORE**) is multiplied by a factor (generally, **1000**) prior to making the same available to the Rule Engine for risk evaluation.

GDP Model Score Multiplication Factor

GDP's Raw Model Score (**MODEL_SCORE**) is multiplied by a factor (generally, **100**) prior to making the same available to the Rule Engine for risk evaluation.

How it Works

When a valid Raw Model Score is received, the RA system multiplies the same by the configured Score Multiplication Factor, rounds it up to the nearest integer, and finally, presents the same as **PREDICTIVE_SCORE** or **MODEL_SCORE** to the Rule Engine for risk evaluation. The multiplied value is also persisted as **PREDICTIVE_SCORE** as part of the transaction audit logs.

When an invalid Raw Model Score is received, then the RA system persists a corresponding negative value. The actual received invalid value is stored in the debug log files.

If any error message or error code is received along with the Raw Model Score, then the same is logged in the Transaction Server's debug logs. This information is not available in the database.

If for some reason, no Raw Model Score is received, then the Risk Analytics system persists a negative value.

Model Deployment Options

- RA can connect simultaneously to one or more types of Model platforms or to one or more instances of the Model platform.
- Each organization can either have their own Model setup or share the same model setup, as long as one organization has exactly one model setup.

How Rules Engine Uses Rules to Calculate a Risk Score and Advice

RA scores rules in the order of their precedence (or Scoring Priority, or Priority, in short). The evaluation result is then forwarded to another module of Transaction Server called the Scoring Engine. Between Rules Engine and Scoring Engine, the rules are run in the following two phases:

1. Execution Phase

Transaction Server does a first parse of all the rules in the active ruleset. In this phase, the Server:

- a. Executes all the rules, including the configured Model, in the list in the order of execution priority.

Note: This execution priority is internal, and is defined by the Server.

- b. Generates an individual risk score and advice for each rule it executes.

2. Scoring Phase

Transaction Server now does the second parse of the rules. In this phase, the Server:

- a. Uses the result for each rule in the first parse, and parses the rules in the ruleset based on the scoring priority.

Note: The scoring priority is configured by the Global Administrator (GA) by using the Administration Console.

- b. Stops the scoring at first matched rule.
The term "matched rule" implies that the risk score generated for the rule in the Execution Phase was in the (default) risky range of 51-100.

- c. Returns the score and advice of the rule that matched as final.

Note: Depending on when the first rule matched, the second parse may not be run completely.

State Diagrams

This section quickly discusses the states a rule and a ruleset can undergo. It covers:

- [States of Rules](#)
- [States of Rulesets](#)

States of Rules

A rule, in its lifetime, can undergo the following states:

- **Proposed**

You might configure a rule over a period of time by using several console sessions. These changes are reflected in the **Proposed** column in the Rules and Scoring Management page. While a rule stays in proposed state, it is not used for risk evaluation.

- **Active**

When you configure the rule to meet your requirements, you enable it for a ruleset, migrate it to production, and refresh the server cache. When you do this, the proposed rule configuration is moved to the **Active** column of the Rules and Scoring Management page. Only when you do this, the rule is active and used in any future risk evaluations.

- **Deprecated**

This is not a formal state, but when you disable a rule from its parent ruleset, the rule is deprecated. Although the rule continues to exist in the system, it is not used in future risk evaluations.

The deprecated rule can be made active any time by assigning it to a ruleset, migrating it to production, and refreshing the server cache.

States of Rulesets

A ruleset, in its lifetime, can undergo one of these states:

- **Assigned**

In this state, a ruleset is assigned to be the primary (or active) ruleset for an organization. You can use the Assign the Ruleset page in the Administration Console for this purpose.

- **Unassigned**

This is not a formal state, but when you unassign a ruleset from its organization, the ruleset is unassigned. Although the ruleset continues to exist in the system, it is not used in future risk evaluations.

The deprecated ruleset can be made active any time by assigning it to an organization, migrating it to production, and refreshing the server cache.

Understanding the Data RA Uses

Risk Analytics bases the result of a risk analysis by comparing the following incoming information, if available, with the historical data for the user:

- **Location Data**

- [How Is Geolocation Information Derived from IP Address Used](#)
- [How Is Geolocation Data Derived from Address Used](#)
- [How Is Geolocation Data Derived from Anonymizers Used](#)
- [How Is Zone Hopping Information Used](#)
- [How Is Negative IP Address List Used](#)

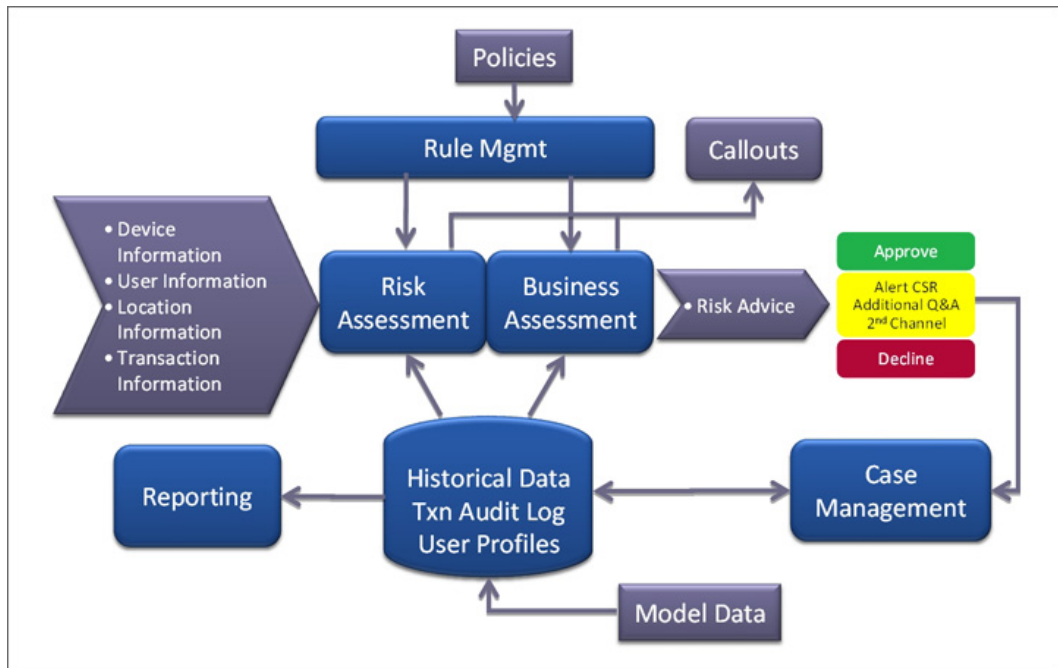
- **Device Data**

- [How Is Device Identification Data Used](#)
- [How Is Device User Association Data Used](#)

- **User Data**

- [How Is User Information Used](#)
- **Transaction Data**
 - [How Is Transaction Information Used](#)
- **Case Management Data**
 - [How Is Case Management Information Used](#)
- **Model Data**
 - [How Is Model Information Used](#)
- **Currency Data**
 - [How Is Currency Conversion Used](#)

The following figure illustrates how Risk Analytics uses this data. The following subsections provide a quick overview of each of the data categories.



understanding_ra_data

How Is Geolocation Information Derived from IP Address Used

RA uses the IP address of the end user's device to derive geo-location information, such as locale, ISP, time zone, and related geographical information.

Note: To obtain this information, RA works with Neustar®, who specialize in providing detailed geographic information for each IP address by mapping it to a region.

This information is especially useful in pre-login risk assessments, where RA does not have any other transaction data yet. For example, if RA decides that the IP address is from a designated negative country (such as Nigeria), then it generates DENY. In this case, your application can choose to not even display the login page.

Note: See [Understanding Data Elements](#) for detailed information on all Geolocation Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this location information in the following rules:

- Exception User Check
- Trusted IP/Aggregator Check
- Untrusted IP Types List
- Negative IP Address List
- Negative Country List
- Zone Hopping
- Other custom rules that you create using IP address, city, state, country, ISP, or time zone as rule variables

How Is Geolocation Data Derived from Address Used

For non-Internet-based, card-present channels, such as ATM and POS, RA derives the geolocation (latitude/longitude) information in two ways:

- If the **ZIPCODE** (or **PINCODE**) of the Card Acceptor (ATM Terminal or Merchant) is available, then the same is used to derive the geolocation mapping data.
- If the **ZIPCODE** (or **PINCODE**) data is *not* available, then the CITY or STATE or COUNTRY information available for the Card Acceptor (ATM Terminal or Merchant) is used to derive the geolocation mapping data.

Card Acceptor's ZIPCODE (or PINCODE) to determine the following geolocation mapping data:

- City
- State
- Country
- Latitude
- Longitude

Note: See [Understanding Data Elements](#) for detailed information on all Geolocation Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this geolocation information in the following rules:

- Zone Hopping

- Negative Country
- Other custom rules that you create using city, state, or country as rule variables

How Is Geolocation Data Derived from Anonymizers Used

IP addresses can also be classified with an anonymizer status. You can control the types of anonymizer IPs that you include in the rule. The different categories of negative IP types are:

- Negative
- Active
- Suspect
- Private
- Inactive
- Unknown

You must either set the rule to the defaults listed or you must clear Suspect IPs. While the use of an anonymizer does not necessarily indicate intent to commit a crime, it is highly suspicious because the user is masking their location. For example, users may be participating in marginal activities such as accessing gaming from a country where it is not allowed or accessing video or music content from a region that is not licensed. The hit rate for this rule is highly variable by customer because it is influenced by the portfolio of end users. However, the approximate review rate based on Anonymizers is 0.1% (one in 1000 transactions). False positive rates tend to vary greatly from as low as 20:1 for US and European users to as high as 100:1 for less developed regions.

Note: See [Understanding Data Elements](#) for detailed information on all Geolocation Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this geolocation information in the following rules:

- Zone Hopping
- Negative Country
- Other custom rules that you create using city, state, or country as rule variables

How Is Zone Hopping Information Used

The location latitude and longitude are the most important information used in the **Zone Hopping Check** rule. This rule verifies the time and speed required for physically travelling between the points of origin of two successive transactions using the IP addresses that were used.

If two successive transactions are originating at a speed beyond what is reasonably possible within a short time span, then you must conclude that either two different people were accessing the same account from different locations or the user did something, either intentionally or inadvertently, to mask their true location. As a result, you can use this as a Deny rule.

It is highly recommended that you start by setting the values of the Zone Hopping Check rule to the default values provided. Based on the performance of this rule over time, you can tune the settings of this rule to make them more precise.

In its default settings, you should expect the rule to fire about 0.02% of the time. The false-positive rate for this rule is good at under 10:1.

Note: See [Understanding Data Elements](#) for detailed information on all Geolocation Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this geolocation information in the following rules:

- Zone Hopping
- Other custom rules that you create using city, state, or country as rule variables

How Is Negative IP Address List Used

The Negative IP Check Rule performs two functions within a single rule:

- The rule checks the IP addresses of end users against the list of known anonymizer proxies.
- The rule consults the Negative IP address list that you define to verify whether the IP is in one of the ranges defined in your table.

You can use the Manage List Data and Category Mappings page in Administration Console to add IP Addresses to the Negative IP address list. The rule performance for blacklisted IP addresses depends on how you manage your list. Typically, you add IPs to the list when you see fraudulent or risky access that you want to stop and you remove IPs from the list when a legitimate user requests for the same.

Note: See [Understanding Data Elements](#) for detailed information on all Geolocation Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this geolocation information in the following rules:

- Negative Country
- Other custom rules that you create using city, state, or country as rule variables

How Is Device Identification Data Used

The following subsections briefly walk you through the device identification and analytics technique used by Risk Analytics:

- Device ID
- Machine FingerPrint (MFP)

- DeviceDNA

RA matches this incoming device data against the stored information to fine tune the score and advice.

Note: See [Understanding Data Elements](#) for detailed information on all Device Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this device-related information in the following rules:

- DeviceID Known
- Device MFP Match
- Device Velocity Check
- Other custom rules that you create using Device Elements

Device ID

The *Device ID* is a server-generated identifier that RA generates and sets on the end user's system to identify and track the device when the end user logs in to your online application and performs transactions. The information is stored in the RA database in an encrypted format.

The Device ID is stored as a Browser cookie, which is an HTTP identifier's extension and storage location depends on the browser used by the end user.

Note: Device ID is not available to Risk Analytics when it evaluates a device for the first time. This data is used in subsequent evaluations.

When a user is evaluated by RA for the first time, it generates this cookie and sets it on the user's system. Every subsequent time the user is assessed, RA verifies if the Device ID on the user's system matches the Device ID stored in the RA database. If the two Device IDs match, the incoming information is considered "safe".

Machine FingerPrint (MFP)

Machine FingerPrint (also referred to as Device fingerprinting or PC fingerprinting in industry terms) represents the browser information and device identification attributes (such as operating system, installed software applications, screen display settings, multimedia components, and other attributes) that are gathered from the end user's system and are analyzed to generate a risk profile of a device in real time. Some of the attributes that are collected from the end user's device include:

- Browser information (such as name, UserAgent, major version, minor version, JavaScript version, HTTP headers)
- Operating system name and version
- Screen settings (such as height, width, color depth)
- System information (such as time zone, language, system locale)

For every transaction performed by the end user, Risk Analytics matches the corresponding MFP stored in its database with the incoming information. If this match percentage (%) is equal to or more than the value specified for the Device-MFP Match rule, then it is considered "safe".

DeviceDNA

DeviceDNA is a device identification and analytics technique that uses both Machine FingerPrint (MFP) and Device ID for more accurate information analyses. For accuracy, more information is collected than in case of MFP. For example:

- Additional system information (such as platform, CPU, MEP, system fonts, camera, and speaker information)
- Additional browser information (such as vendor, VendorSubID, BuildID)
- Additional screen settings (such as buffer depth, pixel depth, DeviceXDPI, DeviceYDPI)
- Plug-in information (such as QuickTime, Flash, Microsoft Windows Media Player, ShockWave, Internet Explorer plug-ins)
- Network information (such as connection type)

How Is Device User Association Data Used

RA uniquely identifies a user as a valid user by automatically associating (or binding) a user to the device that they use to access your application. This is referred to as a *user-device association* (or *device binding*) in RA terminology. Users who are not bound are more likely to receive the Increase Authentication advice.

RA also allows users to be bound to more than one device. For example, a user can use a work and a home computer to access your application. Similarly, you can bind a single device to more than one user. For example, members of a family can use one computer to access your application.

Note: See [Understanding Data Elements](#) for detailed information on all Device Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this device-related information in the following rules:

- User Associated with DeviceID
- Other custom rules that you create using Device Elements

How Is User Information Used

Typically, a user's login ID (USERNAME) identifies a user uniquely in the system. RA uses this information as one of the attributes to identify the risk associated with an incoming transaction. If a user exists in the Risk Analytics database, the user is considered "known", and therefore, less risky. Also, RA can match the incoming user against the stored information to further fine tune the score and advice.

Where Can This Data Be Used

You can use this user-related information in the following rules:

- Exception User Check
- User Known
- User Associated with DeviceID
- User Velocity Check

How Is Transaction Information Used

Using a custom rule, RA can also accept contextual or transaction information for analyzing the risk associated with a transaction. This information includes:

- Transaction amount
- Transaction type
- Transaction date

Note: See [Understanding Data Elements](#) for detailed information on all Transaction Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this transaction-related information in the following rules:

- Custom rules that you create using transaction data elements

How Is Case Management Information Used

The *Case Management* feature of RA provides administrators and fraud analysts a single unified view of the data related to suspect transactions (or cases). This helps in the efficient analysis of collected data and take faster, better-informed decisions towards determining fraud patterns.

This feature also allows you to constantly track the status and progress of cases and maintain complete case histories with instant access to all related information. As a result, Case Management is an efficient tool to analyze data and identify new patterns of fraud from historical data. These patterns, in turn, can be used to configure new rules to reduce fraud.

Where Can this Data be Used

Case Management data serves very useful in:

- Locating suspicious transactions and patterns.
- Testing effectiveness of deployed rules (with the help of **Rule Effectiveness Report**).
- Determining false positives (with the help of **False Positives Report**). If the false positives ratio is high, then also rules need further fine-tuning.

How Is Model Information Used

When you create and deploy an RA Model, it generates a score, typically in a range from 0 through 100. This score is available as a part of the system parameter called **PREDICTIVE_SCORE** (for DSP) and **MODEL_SCORE** (for GDP).

When you configure this parameter alone or in conjunction with other data elements as a part of a custom rule and enable the rule, RA can further fine tune a risk advice.

Note: See [Understanding Data Elements](#) for detailed information on all Model Elements that you can use to create custom rules.

Where Can this Data be Used

You can use this Model-related information in the following rules:

- Custom rules that you create using Model data element

How Is Currency Conversion Used

When the transaction currency and the base currency of the organization to which the user belongs are different, then RA automatically converts the transaction amount to the base currency of the organization.

Some rule operators in specific channels allow you to specify the threshold amount in multiple currencies, in addition to specifying it in the base currency of the organization. When such a rule is executed, the transaction currency is compared with the currencies in which the threshold amount has been specified:

- If a match is found, then the transaction amount is directly compared with the threshold amount in that currency. In this case, no currency conversion is required.
- However, if a match is not found, then the transaction amount is first converted to the base currency and then compared with the threshold set in the base currency.

Important! Setting one of the threshold amounts in base currency is mandatory.

The following examples illustrate how this feature works:

Example 1

You have configured a rule with threshold amounts in USD, JPY, and AUD, while the organization base currency is USD. The following scenarios explain how currency conversion takes place during various types of transactions:

- **Scenario 1:** A transaction is being conducted in USD. Because the transaction currency is the same as the organization's base currency, the specified threshold is used without any need for currency conversion.
- **Scenario 2:** A transaction is being conducted in JPY. Because JPY is one of the currencies in which the threshold amount has been specified, the transaction amount is directly compared with the threshold amount in JPY. No currency conversion is required in this scenario.

- **Scenario 3:** A transaction is being conducted in EUR. Because EUR is *not* one of the currencies in which the threshold amount has been specified, the transaction currency is first converted from EUR to USD. The threshold value specified in USD is used for the comparison.

Example 2

You have configured a rule with threshold amounts in GBP, JPY, and AUD, while the organization base currency is GBP. The following scenarios explain how currency conversion takes place during various types of transactions:

- **Scenario 1:** A transaction is being conducted in GBP. Because the transaction currency is the same as the organization's base currency, the specified threshold is used without any need for currency conversion.
- **Scenario 2:** A transaction is being conducted in JPY. Because JPY is one of the currencies in which the threshold amount has been specified, the transaction amount is directly compared with the threshold amount in JPY. No currency conversion is required in this scenario.
- **Scenario 3:** A transaction is being conducted in EUR. Because EUR is *not* one of the currencies in which the threshold amount has been specified, the transaction currency is first converted from EUR to USD and then from USD to GBP. The threshold value specified in GBP is used for the comparison.

Understanding RA Predictive Model

Risk Analytics offers an advanced fraud modeling capability. Based on the historical data, this modeling capability can be built and created in RA. By using the available transaction data and system data, the model generates a score that describes the extent to which the model suspects a transaction's genuineness. This score typically ranges from 0 through 100, where the higher the number, the greater the possibility of fraud. RA can be configured to send different responses to your calling application based on this model score.

The model score is available as a part of the system parameters (as **ModelScore**) while configuring rules on the Rules and Scoring Management page in Administration Console. This score can be used in conjunction with other data elements to arrive at a risk advice.

RA publishes an interface specification called **Predictive Model Integration Interface**, and can support any Model platform that conforms to the same. Currently, the following Model platforms are supported:

- Global Decisioning Platform (GDP) v2.7.4
- Data Science Platform (DSP) v1.0

This topic briefly explains about how RA uses the Predictive Model and lists the error codes that you will need to be familiar with while building rules. It covers following sub-topics:

- How the Rule Engine Uses Model
- Error Codes When RA is Configured to Use DSP Model

How the Rule Engine Uses the Predictive Model

See topic, [How Rule Engine Uses Model to Calculate Model Score](#).

Error Codes When RA Is Configured to Use DSP Model

The following table lists the error codes logged by Risk Analytics during its interaction with DSP Model. In case of errors, these are the values that you will see in the **Model Score** column instead of the actual score (which is expected to be between 0 and 1000).

As a person building rules, you need to know these values when using Model Score in your new rules.

ERROR	ERROR_CODE
UNKNOWN_FAILURE	-1
READ_TIMEOUT	-2
READ_GDPRESPONSE_FAILURE	-3
WRITE_GDPREQUEST_FAILURE	-4
XML_PARSE_FAILURE	-5
MODEL_SCORE_NOT_RECEIVED	-6
MODEL_SCORE_NEGATIVE	-7
MODEL_SCORE_INVALID	-8
TRANSACTIONID_INVALID	-9
ARCOT_EXCEPTION	-10
TRANSPORT_EXCEPTION	-11
TRANSPORT_READ_EXCEPTION	-12
TRANSPORT_WRITE_EXCEPTION	-13
UNKNOWN_EXCEPTION	-14
UN_TRANSPORT_WRITE_EXCEPTION	-15
UN_TRANSPORT_READ_EXCEPTION	-16
UN_GDPREQ_EXCEPTION	-17
UN_GDPREQ_POSEVAL_EXCEPTION	-18
UN_CONN_SNDRCV_EXCEPTION	-19
UN_CONN_SNDRCV_FAILURE	-20
UN_CONN_EXCEPTION	-21
LOGGING_EXCEPTION	-22
HTML_REPONSE_ERROR	-23
MODEL_NOT_CALLED	-999

Important! If DSP Model returns any specific error code and/or error details, the same will be logged to the Transaction Server debug logs. However, this information will not be available in the database.

Working with Rulesets

A ruleset is a collection of one or more RA rules that you have configured, along with their execution order and scoring priority. Each ruleset can be different from the other in terms of:

- Set of configured rules
- Score and priority for each rule in the set
- Enabling or disabling of rules in the set
- Configured parameters and data for each rule

As a GA, you can configure multiple global rulesets that are available to all the organizations. These rulesets can then be used by other GAs or OAs of these organizations to create new rulesets simply by "copying from" an existing ruleset. In addition, the "copied" rules within a ruleset can also be edited. This not only significantly saves the time and effort required for individually configuring each rule again for organizations, but also reduces the number of errors.

Important! RA is shipped with an out-of-the-box global ruleset called **DEFAULTORG-DEFAULT**. When you create a new organization, a default ruleset called `<ORGANIZATION_NAME>-DEFAULT` is automatically created.

This article covers the following topics:

- [How Do Rulesets Work](#)
- [How to Create a New Ruleset](#)
- [How to Clone a Ruleset](#)
- [How to Assign a Ruleset to an Organization](#)
- [How to Edit a Ruleset](#)
- [How to Migrate a Ruleset to Production](#)

How Do Rulesets Work

A ruleset is just a container and does not work on its own. You need to create rules within its context. Also, just creating it is not sufficient. You must assign it to an organization. Here is how to make rulesets work:

- **Step 1:** Create a ruleset either at a global level or at the level of an organization. You can also clone an existing ruleset for the purpose.
See [How to Create a Ruleset](#) and [How to Clone a Ruleset](#).
- **Step 2:** Configure and enable rules (out-of-the-box or custom) with the ruleset.
See [Working with Out-of-the-Box Rules](#) and [Creating Custom Rules by Using Rule Builder](#).
- **Step 3:** Assign the ruleset to an organization.
See [How to Assign a Ruleset to an Organization](#).

How to Create a Ruleset

Important! After you create a global ruleset as a GA, the OAs of the individual organizations must assign these rulesets to their respective organizations. See [How to Assign a Ruleset to an Organization](#) for more information about how to do this.

When you create a new rule simply by specifying a name, you create a rule based on default ruleset. This implies, your new ruleset inherits the default configurations for all out-of-the-box rules that make up the out-of-the-box ruleset. Like other RA configurations, you can create a ruleset at two levels::

- [How to Create a Ruleset at the Global Level](#)
- [How to Create a Ruleset at the Organization Level](#)

How to Create a Ruleset at the Global Level

Important! After you create a global ruleset as a GA, the OAs of the individual organizations must assign these rulesets to their respective organizations. See [How to Assign a Ruleset to an Organization](#) for more information about how to do this.

To create a new ruleset with all default settings at a global level, so that it is available to all organizations in the scope of the administrator who creates it:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Ruleset Management** section on the side-bar menu, click the **Create Ruleset** link.
The Create Ruleset page is displayed.
5. Specify the name of the ruleset in the **Name** field.
6. Click **Create** to create and save the new ruleset.
The ruleset is not yet active, and not available to your end users.
7. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

How to Create a Ruleset at the Organization Level

Important! After you create a global ruleset as a GA, the OAs of the individual organizations must assign these rulesets to their respective organizations. See "[How to Assign a Ruleset to an Organization](#)" for more information about how to do this.

To create a new ruleset with all default settings at the level of an organization, so that it is only available to the current organization:

1. Ensure that you are logged in as an OA.
2. Activate the **Organizations** tab.

3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
6. Activate the **Risk Engine** tab.
7. Under the **Ruleset Management** section on the side-bar menu, click the **Create Ruleset** link.
The Create Ruleset page is displayed.
8. Specify the name of the ruleset in the **Name** field.
9. Click **Create** to create and save the new ruleset.
The ruleset is not yet active, and not available to your end users.
10. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

How to Clone a Ruleset

Important! Before you clone a ruleset, you must ensure that the source ruleset has been assigned to an organization. See [How to Assign a Ruleset to an Organization](#) for detailed instructions, if you have already not done so.

As a GA or an OA, you can configure multiple rulesets that are available to all the organizations in your scope. These rulesets can then be used by other GAs or OAs of these organizations to create new rulesets simply by "copying from" an existing ruleset. This not only significantly saves the time and effort required for individually configuring each rule again for every required organization, but also reduces the number of potential errors. You can either clone from a system ruleset or some ruleset you created earlier. This topic covers:

- [How to Clone from SYSTEM Ruleset](#)
- [How to Clone an Existing Ruleset](#)

How to Clone from SYSTEM Ruleset

RA is shipped with an out-of-the-box ruleset called **DEFAULTORG-DEFAULT**. When you create a new organization, a default ruleset called <ORGANIZATION_NAME>-DEFAULT is automatically created. This ruleset offers the default settings for all the out-of-the-box rules that constitute this ruleset.

Initially, it is highly recommended that you create new rulesets by cloning this SYSTEM ruleset.

Cloning SYSTEM Ruleset at Global Level

To clone from the SYSTEM ruleset at a global level:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Ruleset Management** section on the side-bar menu, click the **Create Ruleset** link.
The Create Ruleset page is displayed.
5. Specify the name of the ruleset in the **Name** field.
6. In the **Advanced Option** section:
 - a. Select the **Copy from an Existing Ruleset** option to clone an existing ruleset.
 - b. Select **SYSTEM - DEFAULT** from the corresponding list.
7. Click **Create** to create and save the new ruleset.
The ruleset is not yet active, and not available to your end users.
8. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

Cloning SYSTEM Ruleset at Organization Level

To clone from the SYSTEM ruleset at the level of an organization:

1. Ensure that you are logged in as an OA.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
6. Activate the **Risk Engine** tab.
7. Under the **Ruleset Management** section on the side-bar menu, click the **Create Ruleset** link.
The Create Ruleset page is displayed.
8. Specify the name of the ruleset in the **Name** field.
9. In the **Advanced Option** section:
 - a. Select the **Copy from an Existing Ruleset** option to clone an existing ruleset.
 - b. Select **SYSTEM - DEFAULT** from the corresponding list.

10. Click **Create** to create and save the new ruleset.
The ruleset is not yet active, and not available to your end users.
11. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

How to Clone an Existing Ruleset

This section walks you through the steps for cloning an existing ruleset.

Cloning an Existing Ruleset at Global Level

To clone from an existing ruleset at a global level:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Ruleset Management** section on the side-bar menu, click the **Create Ruleset** link.
The Create Ruleset page is displayed.
5. Specify the name of the ruleset in the **Name** field.
6. In the **Advanced Option** section:
 - a. Select the **Copy from an Existing Ruleset** option to clone an existing ruleset.
 - b. Select the name of the ruleset whose configuration you want to copy from the corresponding list.
7. Click **Create** to create and save the new ruleset.
The ruleset is not yet active, and not available to your end users.
8. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

Cloning an Existing Ruleset at Organization Level

To clone from an existing ruleset at the level of an organization:

1. Ensure that you are logged in as an OA.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.

5. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
6. Activate the **Risk Engine** tab.
7. Under the **Ruleset Management** section on the side-bar menu, click the **Create Ruleset** link.
The Create Ruleset page is displayed.
8. Specify the name of the ruleset in the **Name** field.
9. In the **Advanced Option** section:
 - a. Select the **Copy from an Existing Ruleset** option to clone an existing ruleset.
 - b. Select the name of the ruleset whose configuration you want to copy from the corresponding list.
10. Click **Create** to create and save the new ruleset.
The ruleset is not yet active, and not available to your end users.
11. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

How to Assign a Ruleset to an Organization

After a GA or an OA creates a ruleset for their organization and migrates it to production, you must activate this ruleset for an organization within your scope for it to take effect. This is achieved by assigning the ruleset to an organization.

To assign an existing ruleset to an organization:

1. Ensure that you are logged in with the required privileges and scope to assign rulesets.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
6. Activate the **Risk Engine** tab.
7. Under the **Ruleset** section, click the **Assign Ruleset** link.
The Assign Ruleset page appears.

8. Select the ruleset that you want to activate from the **Select Ruleset to assign** list.
9. Click **Save** to make the specified ruleset active for the current organization.
10. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

How to Edit a Ruleset

Important! Before you modify the definition of a ruleset, you must assign the ruleset. See [How to Assign a Ruleset to an Organization](#) for detailed instructions, if you have already not done so.

To edit the definition of an existing ruleset:

1. Ensure that you are logged in with the required privileges and scope to assign rulesets.
2. Ensure that the rule has been assigned.
3. Activate the **Organizations** tab.
4. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
5. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
6. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
7. Activate the **Risk Engine** tab.
8. Under the **Rules Management** section, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
9. Select the ruleset that you want to edit from the **Select Ruleset to assign** list.
10. For each rule that you want to change in the ruleset, in the **PROPOSED** column of the displayed table:
 - a. Select (to enable the rule) or clear (to disable the rule) the **Enable** option.
 - b. Specify the required **Risk Score**.
 - c. Select a priority for the rule from the **Priority** list.
11. In the **PROPOSED** column for **Default Score** (the second table on the page), specify the required Risk Score.

Note: RA uses this value to generate the final Risk Score and Advice if none of the rules in the preceding table match.
12. Click **Save** to save the changes you made on this screen.
The changes are not yet active and are not available to your end users.

13. To make the changes active, you must migrate them to production.
Refer to [How to Migrate a Ruleset to Production](#) for instructions to do so.

How to Migrate a Ruleset to Production

When you configure an out-of-the-box rule, custom rule, or callout, the change is yet not permanent, and the changed configuration data is referred to as *Proposed data*. This data can be created over a period of time by using several administrative sessions. While you configure this data, it is stored in the **Proposed Configuration** area and is reflected in the **Proposed** column on respective configuration page. As a result, any changes that you make to the **Proposed** column affect this data.

When all data is configured according to your requirements, then the Proposed data can be converted to *Active data* (the **Active** column on respective configuration page) by migrating it to production and refreshing the Transaction Server cache.

Note: At any point in time, RA Servers work with Active data configurations *only*. This means, RA only uses Active data for real-time risk evaluations and for generating Risk Score and the corresponding Risk Advice.

After the Proposed data has been migrated to Active data, if you configure the data again, a copy of the Active data is created in the Proposed configuration area. Further additions or deletions can be done to the Proposed data until configurations are ready to be migrated to production. All modifications are reflected only in the Proposed data. However, Reports can be viewed as Active or Proposed configurations. Active data is versioned to keep track of the changes made to the RA configuration data. Every time the Proposed data is migrated to production, unique data versions are created for the new set of Active configuration data. Like other RA configurations, you can migrate a ruleset to production at two levels:

- Global level ([How to Migrate a Ruleset to Production at the Global Level](#))
- Organization level ([How to Migrate a Ruleset to Production at the Organization Level](#))

How to Migrate a Ruleset to Production at the Global Level

To migrate a ruleset at system (or global) level:

1. Ensure that you are logged in as a GA or as an OA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **Risk Analytics** tab.
4. Under the **Migrate to Production** section on the side-bar menu, click the **Migrate to Production** link.
The Migrate to Production page appears.
5. On the page, either:
 - Select the **Select All Rulesets** option, if you want to migrate all the changes that you made to all the configured rulesets.
or
 - Select a specific ruleset from the **Select Ruleset(s)** list to migrate the changes that you made to this ruleset.

6. Click **Migrate**.
The page to confirm the action is displayed.

7. On the confirmation page, click **Confirm** to start the migration process.

Note: Based on the volume of data that you are migrating to production, the migration process might take a few minutes.

After the migration is completed, the "The proposed data has been successfully migrated to Production." message is displayed.

How to Migrate a Ruleset to Production at the Organization Level

To migrate a ruleset to production so that the changes are available:

1. Ensure that you are logged in as an OA.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the `<ORGANIZATION_NAME>` link for the required organization.
The Organization Information page appears.
6. Activate the **Risk Analytics** tab.
7. Under the **Migrate to Production** section on the side-bar menu, click the **Migrate to Production** link.
The Migrate to Production page appears.
8. On the page, either:
 - Select the **Select All Rulesets** option, if you want to migrate all the changes that you made to all the configured rulesets.
or
 - Select a specific ruleset from the **Select Ruleset(s)** list to migrate the changes that you made to this ruleset.
9. Click **Migrate**.
The page to confirm the action is displayed.
10. On the confirmation page, click **Confirm** to start the *migration process*.

Note: Based on the volume of data that you are migrating to production, the migration process might take a few minutes.

After the migration is completed, the "The proposed data has been successfully migrated to Production." message is displayed.

Working with Out-of-the-Box Rules

Managing rule configurations is a key part of RA management and optimization, and a key responsibility of GAs and OAs. This article explains rules and the related concepts. It then guides you through the steps for configuring the out-of-the-box rules that are automatically available when you install and bootstrap RA. It covers the following topics:

- [What are Out-of-the-Box Rules](#)
- [How to Create and Deploy Out-of-the-Box Rules](#)
- [How to Create a Device-Based Rule](#)
- [I Have Configured My Rule, Now What](#)
- [How to Upload Rule List Data](#)
- [How to Create a List](#)
- [How to Edit a List](#)
- [How to Activate a Rule \(Migrate Rules to Production\)](#)
- [How to Refresh Server Cache](#)
- [How to Edit Rule Definitions](#)
- [How to Delete a Rule](#)

What are Out-of-the-Box Rules

After the required data is collected, it is forwarded to Rules Engine (a module of Transaction Server). The Rules Engine is a set of configured rules that evaluate this information based on incoming information and historical data, if available.

A rule, in turn, is a condition or a set of conditions that must be true for a rule to be invoked. By default, each rule is assigned a priority and is evaluated in the specific order of its priority level. However based on your business requirements, you can change this priority of rule scoring.

See [Out-of-the-Box Rules](#) for a quick overview of the out-of-the-box rules.

How to Create and Deploy Out-of-the-Box Rules

You will need to use the Rule Configuration page in the Administration Console for:

- Enabling or disabling the out-of-the-box rules
- Configuring the risk score and priority of the out-of-the-box rules

The generic steps to configure an out-of-the-box rule are:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. For each rule, in the **PROPOSED** column of the displayed table:
 - a. Select (to enable the rule) or clear (to disable the rule) the **Enable** option.
 - b. Specify the required **Risk Score**.
 - c. Select a priority for the rule from the **Priority** list.
9. In the **PROPOSED** column for **Default Score** (the second table on the page), specify the required Risk Score.

Note: RA uses this value to generate the final Risk Score and Advice if none of the rules in the preceding table match.
10. Click **Save** to save the changes you made on this screen.
The changes are not yet active and are not available to your end users.
11. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
12. Refresh all deployed Transaction Server instances.
Refer to [How to Refresh Server Cache](#) for instructions to do so.

How to Create a Device-Based Rule

RA allows you to create the following rules based on Device-User associations:

- [Device User Velocity](#)
- [Device User Maturity](#)

The following subsections briefly explain what these rules are and walk you through the steps for creating these rules.

How to Configure the Out-of-Box Device User Velocity Rule

The **Device Velocity Check** rule checks if there are frequent transactions by one or more users from a particular device, exceeding a defined velocity. This can result in inaccurate results in cases where a single device is shared by many users. The *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.

It is based on the following parameters:

- **Number of Distinct Users Allowed Per Device**
Denotes the number of distinct users performing transactions using a specified device, irrespective of whether the risk evaluation resulted in success or failure.
The default value for this parameter is **5**.
- **Time Interval**
Denotes the time period in which the number of transactions are tracked.
The default value for this parameter is **60**.
- **Unit for Time Interval**
Denotes the unit in which the time period is measured.
The default value for this parameter is **Minutes**.

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.

Configuring Device User Velocity Rule

To configure the Device User Velocity rule:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. Click **Add a New Rule**.
The Risk Analytics Rule Builder page appears.
9. Enter the **Name**, **Mnemonic**, and **Description** of the rule that you want to create.
10. Select the **Channels** and **Actions** for which this rule is applicable.

11. Build the rule fragment, as follows:
 - a. From the **Device Elements** list, select **DEVICEID**.
 - b. Select **VELOCITY_DISTINCT_USER** from the **Select Operator** list.
 - c. Specify the number of distinct users performing transactions from the device in the **Greater Than or Equal To** field.
 - d. Specify the time interval.
This value denotes the maximum number of transactions (within the specified time interval) that is considered safe for a device for $n-1$ distinct users. If the actual number of transactions within the specified time is equal to or greater than this number, then RA tracks the transaction as a risk, which results in the matching of the Device User Velocity rule.
 - e. Select the unit for the time interval from the drop-down list.
 - f. Click **Add** to build the rule fragment.
12. Click **Create** at the bottom of the Rule Builder page to create the rule.
The changes are not yet active and are not available to your end users.
13. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
14. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

How to Configure Organizations for Device Velocity Rules with Scope as Org Family

To create Device Velocity rules for organizations with Scope as Org Family, you must enable constraints by running the following database scripts:

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWINUI, DISPLAYORDERID) VALUES
(ARRFCONFIGSEQUENCE.NEXTVAL, '<ORGNAME>', -1, 'GLOBAL', 'LOGDEVICEPINGS', 'Y', 'Log Device TimeStamps', 'Log Device TimeStamps', 0, 0, 0);
```

Example

```
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWINUI, DISPLAYORDERID) VALUES(ARRFCONFIGSEQUENCE.NEXTVAL,
'FAMILYORG1', -1, 'GLOBAL', 'LOGDEVICEPINGS', 'Y', 'Log Device TimeStamps', 'Log Device TimeStamps', 0, 0, 0);
INSERT INTO ARRFCONFIGURATION
(SEQUENCEID, ORGNAME, CHANNELID, CATEGORY, NAME, VALUE, DESCRIPTION, DISPLAYNAME, TYPE, SHOWINUI, DISPLAYORDERID) VALUES(ARRFCONFIGSEQUENCE.NEXTVAL,
'FAMILYORG2', -1, 'GLOBAL', 'LOGDEVICEPINGS', 'Y', 'Log Device TimeStamps', 'Log Device TimeStamps', 0, 0, 0);
COMMIT;
```

After adding these database entries, organizations can create Device Velocity rules with Scope as Org Family.

How to Configure the Out-of-Box Device User Maturity Rule

The *User Associated with DeviceID* rule evaluates transactions by checking the association between the user and the device, irrespective of the time the association was created. If the user-device association exists, then the transactions receive a low risk score. There might be cases where fraudsters can reset a user's password and associate themselves with the device. In such cases, evaluating the transaction based only on the User-Device association might not be sufficient to rule out fraudulent activity.

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.

It is based on the following parameters:

- **Number of Successful Transactions per User-Device Association**
Denotes the number of successful transactions identified by RA for a specified User-Device association.
- **First Successful Transaction**
Denotes the time (in days) before which the first successful transaction was identified.

These parameters determine the strength of the User-Device association. The Device User Maturity rule returns True if the user has used the device for at least the specified number of days and the number of successful transactions is greater than or equal to the configured value.

Configuring Device User Maturity Rule

To configure the Device User Maturity rule:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. Click **Add a New Rule**.
The Risk Analytics Rule Builder page appears.

9. Enter the **Name**, **Mnemonic**, and **Description** of the rule that you want to create.
10. Select the **Channels** and **Actions** for which this rule is applicable.
11. Build the rule fragment, as follows:
 - a. From the **Transaction Elements** list, select **USERNAME**.
 - b. Hold the **CTRL** key, and select **DEVICEID** from the **Device Elements** list.
 - c. Select **MATURITY** from the **Select Operator** list.
 - d. Specify the number of successful transactions.
 - e. Specify the number of days before which the first successful transaction took place.
 - f. Click **Add** to build the rule fragment.
12. Click **Create** at the bottom of the Rule Builder page to create the rule.
The changes are not yet active and are not available to your end users.
13. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
14. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

I Have Configured My Rule, Now What

After you configure an out-of-the-box rule, you need to do the following tasks so that the rule is used during risk evaluation:

1. Upload any data, if the rule uses a list.
2. Enable the rule.
3. Assign the ruleset (to which the rule belongs) to an organization.
4. Migrate it to production.
5. Refresh the server cache.

The following topics quickly explain these tasks.

Step 1: Upload Rule List Data, If Any

If your rule uses a list of values against which it assesses a condition, then you need to upload that data as a list.

To upload the data for a list, see, [How to Upload Rule List Data](#) for detailed instructions.

Step 2: Enable the Rule

The rule that you just configured must be enabled so that it can be a part of the parent ruleset. To enable the rule:

1. In the Administration Console, access the Rules and Scoring Management page.
2. From the **Select a Ruleset** list, select the ruleset for which this configuration is applicable. The configuration for the specified ruleset appears.
3. Select the **Enable** option against the rule you just created.
4. Click **Save** at the bottom of the rules table.

Step 3: Assign the Ruleset to Which the Rule Belongs

After you activated the new rule by enabling it (as discussed in the preceding section), then the next thing you will need to do is activate the parent ruleset to which your rule belongs. This process of activating a ruleset is known as assigning a ruleset.

To assign a ruleset, see, [How to Assign a Ruleset to an Organization](#) for detailed instructions.

Step 4: Migrate the Rule to Production

When the rule is configured, it is still in the Proposed Configuration area and is only still available in the **Proposed** column of rule configuration. When the rule is ready and all its data is configured according to your requirements, then you must convert it from its current the Proposed state to Active state (the **Active** column on respective configuration page). This can only be done by migrating it to production.

To make the changes active, see [How to Activate a Rule \(Migrate Rules to Production\)](#) for detailed instructions.

Step 5: Refresh the Server Cache

Migrating a major change (such as a new rule) to production does not affect the cache of the active server instances. Each instance's cache needs to be refreshed before the server can start serving it for risk evaluations. That is why, you now need to refresh the server cache.

To refresh the cache of all deployed Transaction Server instances, see [How to Refresh Server Cache](#) for detailed instructions.

How to Upload Rule List Data

Important! All the configurations and tasks discussed in this section should primarily be performed by Organization Administrators. If required, these steps can also be performed by Global Administrators. However, they must be performed at the organization level (through the **Organizations** tab).

If any rule that you deployed requires additional data in the form of a list, then you must perform the tasks in this section. You can add, modify, or delete list data by using the Manage List Data and Category Mappings page in Administration Console. This topic describes how to manage data for the following lists:

- Negative Country Lists

- Untrusted IP Lists
- Trusted IP Lists
- Trusted Aggregator Lists
- Data Lists
- Category Mapping Lists

For Negative Country List

Negative Country list comprises all countries from which fraudulent or malicious transactions are known to have originated in the past. Enterprises may also maintain this list in line with the regulations of their country.

RA derives the country information based on the input IP address. It, then, uses this data to score the potential for fraud for online transactions originating from such countries. For this purpose, RA also integrates with Neustar IP Intelligence (formerly, Quova), which enhances the analysis by providing detailed geographic information for each IP address by mapping it to a region.

To know more about Neustar IP Intelligence and their services, go to:

<http://www.neustar.biz>

RA evaluates the incoming transactions and checks if these transactions originated from an IP address that belongs to a country marked as negative. Such transactions are typically denied.

Use the Manage List Data and Category Mappings page to add a country to the Negative Country list or remove a country from the list.

Configuring Negative Country List

To configure the Negative Country list:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **Risk Engine** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.
The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.
9. Select the **Manage List Data** option.

10. From the **Select List Type** list, select **Negative Country Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. **Select Negative Countries** that you want to add to the list.
13. Click the > or < button to move selected countries to the desired list.
You can also click the >> or << buttons to move all countries to the desired lists.
14. Click **Save** to save the changes.
The changes are not yet active and are not available to your end users.
15. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
16. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

For Untrusted IP Addresses

The **Untrusted IP Address List** is a collection of IP addresses that have been the origin of known anonymizer proxies or fraudulent and malicious transactions in the past. This list is the source of the Negative category discussed in the "Configuring Untrusted IP Types" section.

Use the Manage List Data and Category Mappings page to configure the untrusted IP address ranges for your organization.

Configuring Untrusted IP Addresses

To configure the untrusted IP address ranges:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **Risk Engine** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.
The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.
The ruleset configuration information is displayed.
9. Select the **Manage List Data** option.

10. From the **Select List Type** list, select **Untrusted IP Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. In the **Upload Untrusted IP Ranges** section, select the appropriate mode for writing data:
 - **Append**: This option appends the data that you are uploading to a list or dataset.
Note: You must select this option if the list does not exist.
 - **Replace**: This option overwrites the existing data in the specified list or dataset.
13. Click **Browse** to navigate to the data file that contains the list of entries.
14. Click **Upload** to complete the task.
15. In the **Add/Delete Untrusted IP Range** section:
 - a. Enter the starting IP address in the **IP Address** field.
 - b. Select one of the following options:
 - **Subnet Mask**: If you want to specify a range of IP addresses based on the subnet mask to be added to the Untrusted IP Address List.
 - **End IP Address**: If you want to specify a simple range of IP addresses to be added to the Untrusted IP Address List.
 - c. Specify the **Information Source** (or vendor) of the untrusted IP address range.
16. Click one of the following buttons, as required:
 - **Add Range**: To add the specified IP address or range to the database.
 - **Delete Range**: To delete the specified IP address or range from the database.

The appropriate message is displayed.
The changes are not yet active and are not available to your end users.
17. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
18. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

For Trusted IP Addresses

In RA, transactions that either originate from or are routed through IP addresses and ranges that belong to the **Trusted IP Address List** are considered low risk. As a result, RA bypasses these transactions from risk evaluations and assigns them a low Score and the ALLOW Advice.

Use the Manage List Data and Category Mappings page to perform the following tasks related to trusted IP addresses and ranges:

- Adding a Trusted IP Address Range

- Updating a Trusted IP Address Range
- Deleting a Trusted IP Address Range

Adding a Trusted IP Address Range

To add a Trusted IP Address Range:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **Risk Engine** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.
The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.
The ruleset configuration information is displayed.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Trusted IP Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. Specify the required **IP Address** that will be added to the Trusted IP List.
13. Specify one of the following:
 - **Subnet Mask:** If you want to specify a range of IP addresses based on the subnet mask to be added to the Trusted IP List.
 - **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Trusted IP List.
14. Click **Add Range** to add the IP addresses or ranges to the Trusted IP List.
The Trusted IP List table with the range that you just added appears at the end of the page.
15. Click **Update** to save the changes.
The changes are not yet active and are not available to your end users.
16. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.

17. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Updating a Trusted IP Address Range

To update a Trusted IP Address Range:

1. Perform the tasks listed from Step 1 through Step 11 in "Adding a Trusted IP Address Range" to display the **Trusted IP List** table.
2. Make the required changes in the **Trusted IP List** table.
3. Select all the affected IP address range(s) in the **Trusted IP List** table.
4. Click **Update** to update the changes that you made.
The changes are not yet active and are not available to your end users.
5. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
6. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Deleting a Trusted IP Address Range

To delete a Trusted IP Address Range:

1. Perform the tasks listed from Step 1 through Step 11 in "Adding a Trusted IP Address Range" to display the **Trusted IP List** table.
2. In the **Trusted IP List** table, select the required IP address range(s) that you want to delete.
3. Click **Delete** to delete the ranges that you selected.
4. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
5. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

For Trusted Aggregators

Aggregators are third-party vendors who provide account aggregation services by collating login information of users across multiple enterprises. The originating IP addresses when users log in from a protected portal versus when they come in through such aggregators are different. Many enterprises use the services of these account and data aggregation service providers to expand their online reach.

Transactions originating from (or routed through) aggregators "trusted" to the organization are considered low-risk. For this purpose, RA provides the ability to configure a list of these aggregators so that all transactions originating from the aggregators' IP addresses are assigned a low Score, and the ALLOW Advice.

RA uniquely identifies an aggregator by combining their IP address range and a unique Aggregator ID. This Aggregator ID must also be sent to RA along with the transaction.

RA also enables you to specify up to *three* unique IDs for each aggregator at any time. This allows for the periodical rotation of the ID for the purpose of enhanced security. During this rotation, RA continues to recognize the previous ID in addition to the new ID to allow updates to the aggregator at a later time.

Use the Manage List Data and Category Mappings page to perform the following tasks related to trusted aggregators:

- Adding a Trusted Aggregator
- Updating a Trusted Aggregator
- Deleting a Trusted Aggregator

Adding a Trusted Aggregator

To add a Trusted Aggregator:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **Risk Engine** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.
The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.
The ruleset configuration information is displayed.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Trusted Aggregator Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. Specify the name of the new aggregator in the **Add New Aggregator** field and click **Create**.
The updated Trusted Aggregator Configuration page.
13. Select the **Aggregator** that you want to configure from the drop-down list.
14. Enter the starting IP Address in the **IP Address** field.
15. Select one of the following options:

- **Subnet Mask:** If you want to specify a range of IP addresses based on the subnet mask to be added to the Trusted Aggregator List.
 - **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Trusted Aggregator List.
16. Click **Add Range** to add this IP address or range to the database.
The Trusted IP List table with the range that you just added for the aggregator appears at the end of the page.
The changes are not yet active and are not available to your end users.
 17. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
 18. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Updating a Trusted Aggregator

RA enables you to update the Aggregator IDs. The periodic update of these IDs is referred to as *rotation of Aggregator IDs*.

Important! You must periodically rotate or change the Aggregator IDs for security purposes. You can decide this rotation duration according to your business rules.

After an ID is updated, you must ensure that the latest Aggregator ID is conveyed to the aggregator. There might be a delay in propagating the Aggregator IDs. In this duration, RA recognizes the old, as well as the new Aggregator ID associated with the IP address.

Note: The transactions originating from the aggregator-end must contain this aggregator ID in the form specified by RA APIs.

To update a Trusted Aggregator information:

1. Complete Step 1 through Step 11 in "Adding a Trusted Aggregator" to display the Trusted Aggregator Configuration information.
2. Select an existing aggregator from the **Aggregator** list.
The Trusted Aggregator Configuration information with the Aggregator ID(s) for the selected aggregator appears.
3. Click **Update Aggregator ID** to generate a new Aggregator ID.
The updated Aggregator ID(s) for the aggregator appears, and the next empty Aggregator ID is displayed.
4. In the **Trusted IP List** table, select the aggregator IP addresses or ranges you want to update.
5. Make the required changes and click **Update**.
The changes are not yet active and are not available to your end users.
6. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
7. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Deleting a Trusted Aggregator

To delete a Trusted Aggregator:

1. Complete Step 1 through Step 11 in "Adding a Trusted Aggregator" to display the Trusted Aggregator Configuration information.
2. Select an existing aggregator from the **Aggregator** list.
The Trusted Aggregator Configuration information appears.
3. In the **Trusted IP List** table, select the aggregator IP addresses or ranges you want to delete.
4. Click **Delete** to delete the selected information.
The changes are not yet active and are not available to your end users.
5. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
6. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

For Simple Lists

Note: If your list contains 10 or fewer items, you can use the **Show List** link in the Rule Builder to add the list items in the Rule Builder itself.

To upload the data for a rule that uses the IN_LIST operator:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under the **Select Organizations to Modify** section, click the link with the organization's name to which you want to apply the rule.
6. Click the **Risk Engine** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.
The Manage List Data and Category Mappings page appears.
8. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Other Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
The updated page appears.

12. In the **Upload File Or Enter Data** section, select the appropriate mode for writing data:

- **Append:** This option appends the data that you are uploading to a list or dataset.

Note: You must select this option if the list does not exist.

- **Replace:** This option overwrites the existing data in the specified list or dataset.

13. Do *one* of the following:

- Click **Browse** to navigate to the data file that contains the list of entries (separated by a newline character.)
- Type in the entries in the **Enter Data** field, if a data file does not exist.

Important! Ensure that the entries are separated by a newline character (ENTER).

14. Click **Upload** to complete the task.

For Category Mapping Lists

To upload the data for a rule that uses the IN_CATEGORY operator:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under the **Select Organizations to Modify** section, click the link with the organization's name to which you want to apply the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.
The Manage List Data and Category Mappings page appears.
7. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. Select the **Manage Category Mappings** option.
9. From the **Select Category Mapping** list, select the mapping set identifier that you specified while creating the corresponding list.
The updated page appears.
10. In the **Upload File Or Enter Classification Data** section, select the appropriate mode for writing data:
 - **Append:** This option appends the data that you are uploading to a list or dataset.

Note: You must select this option if the list does not exist.

 - **Replace:** This option overwrites the existing data in the specified list or dataset.

11. Perform *one* of the following:

- Click **Browse** to navigate to the data file that contains the list of entries (separated by a newline character.)
- Type in the entries in the **Enter Data** field, if a data file does not exist.

Important! Ensure that the entries are separated by a newline character (ENTER).

12. Click **Upload** to complete the task.

How to Create a List

If any rule that you deployed requires additional data in the form of a list, then you can create a list by using the Create List page in the Administration Console.

To create a list for an organization:

1. Log in to the Administration Console with the required privileges and scope.
2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **Ruleset Management** section, click the **Create List** link.
The Create List page appears.
7. Specify the **List Name**.
8. Specify who can access the list using **Scope**:
 - **ORG**: Whether the list is only accessible to the current organization for which you are configuring the list.
 - **Ruleset**: Whether the list is accessible to all organizations that share a ruleset.
9. Specify the data element that the list is based on in the **Element Name** field.
These are data elements for the IN_LIST-based rules. For example, you will choose the BROWSER element if a browser or a specific version of the browser has been found vulnerable to recent attacks. Similarly, you can select the CITY element if you find that a specific city has been a hotbed for fraudulent online transactions.
10. Specify the **List Usage** as follows:
 - **General Purpose**: To use for any data that is neither blacklisted nor whitelisted.
 - **Blacklist**: To ensure any matched data is instantly marked as fraud.

- **Whitelist:** To ensure any matched data is instantly marked as safe.

11. Specify whether you want to **HotList** the list you are creating.

Note: Currently the HotList option is only enabled for Blacklists.

If you specify **Yes**, then this list is reflected in the **Manage Inbound Calls** and **Work On Cases** pages of Case Management.

12. Specify if this is a **Preferred List**.

Note: This option is only available if you selected **Blacklist** in the **List Usage** option. Also, Preferred Lists can only be set for an organization.

This option is useful if you want to set a hotlist as preferred and to be used by Customer Service Representatives (CSRs) for easy blacklisting from the Case Management screens.

13. Specify what other organizations this list can be shared with and using what privileges (Read Only or Read-Write) from the **Sharing & Privileges** option.

Note: This release only supports the Read Only option.

Create List

Use this screen to create a data list. A list is created by specifying its specific properties and can optionally be shared with its peer organizations. This list may then be used in Rule creation.

List Type	List Data		
List Name	MYDEVICEIDLIST		
Scope	<input checked="" type="radio"/> ORG <input type="radio"/> Ruleset	SAFESOUTHWESTBANK - DEFAULT	
Element Name	DEVICEID		
List Usage	Blacklist		
Elements with Hotlist option	DEVICEID		
HotList	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Preferred List	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Sharing & Privileges	<div> <div>SAFENORTHWESTBANK</div> <div>SAFENORTHWESTBANK</div> <div>SAFEBANKS (ORG Family)</div> </div>	Read Only	Add

List is not shared

create_list

14. Click **Create** to make the specified list active for the current organization.

15. To make the changes active, you must migrate them to production.
Refer to [How to Migrate to Production](#) for instructions to do so.

16. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions to do so.

How to Edit a List

To edit a list:

1. Log in to the Administration Console with the required privileges and scope.

2. Activate the **Organizations** tab.
3. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
4. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization.
The Organization Information page appears.
5. Activate the **Risk Engine** tab.
6. Under the **Ruleset Management** section, click the **Edit List** link.
The Edit List page appears.
7. Select the list that you want to edit.
8. Select if you want to make this list a preferred list or not.
If you choose to make this list a Preferred List, then it can be used by Customer Service Representatives (CSRs) for easy blacklisting from the Case Management screens.
9. Click **Save**.

How to Activate a Rule (Migrate Rules to Production)

When a rule, ruleset, or data is configured in RA, it is still in the Proposed Configuration area and is only still available in the **Proposed** column of rule configuration. When the rule is ready and all its data is configured according to your requirements, then you must convert it from its current the Proposed state to Active state (the **Active** column on respective configuration page). This can only be done by migrating it to production.

Notes on Migrating to Production

- At any point in time, Transaction Servers work with Active data configurations *only*.
- Active data is versioned to keep track of the changes made to the RA configuration data. Every time the Proposed data is migrated to production, unique data versions are created for the new set of Active configuration data.

Migrating a Rule to Production

To migrate a rule to production

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.

6. Under the **Migrate to Production** section on the side-bar menu, click the **Migrate to Production** link.

The Migrate to Production page appears.

7. On the page, either:

- Select the **Select All Rulesets** option, if you want to migrate all the changes that you made to all the configured rulesets.
- Select a specific ruleset from the **Select Ruleset(s)** list to migrate the changes that you made to this ruleset.

8. Click **Migrate**.

The page to confirm the action is displayed.

9. On the confirmation page, click **Confirm** to start the *migration process*.

Note: Based on the volume of data that you are migrating to production, the migration process might take a few minutes.

After the migration is completed, the "The proposed data has been successfully migrated to Production." message is displayed.

10. Refresh the Transaction Server cache.

Refer to [How to Refresh Server Cache](#) for instructions to do so.

How to Refresh Server Cache

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

The RA Servers cache can be refreshed in two ways:

- At the system (or global level), for all organizations in the administrator's scope. See [How to Refresh Server Cache at System Level](#) for instructions.
- At the level of a specific organization (organization level) **to which the administrator is currently logged in**. See [How to Refresh Server Cache at Organization Level](#) for instructions.

Privileges Required

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

How to Refresh Server Cache at System Level

To refresh cache for all RA servers:

1. Ensure that you are logged in as a GA or as an OA.
2. Activate the **Services and Server Configurations** tab.

3. Activate the **Administration Console** sub-tab.
4. Under the **System Configuration** section on the side-bar menu, click the **Refresh Cache** link.
The Refresh Cache page is displayed.
5. Select one or both of the following options:
 - Select the **Refresh System Configuration** option to refresh the cache configuration of Administration Console, User Data Service, and all Transaction Server and Case Management Server instances.
 - Select the **Refresh Organization Configuration** option to refresh the cache configuration of all organizations in your purview.
6. Click **OK**.
A confirmation dialog box appears.
7. Click **OK** again.

How to Refresh Server Cache at Organization Level

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

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

To refresh the organization cache:

1. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
5. Select the organizations whose cache you want to refresh.
6. Click **Refresh Cache**.
7. Click **OK** in the dialog box to confirm your cache refresh request.
A message with a Request ID for the current cache refresh request is displayed. You can check the status of your cache refresh request by clicking the **Check Cache Refresh Status** link and selecting this **Request ID**.

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

How to Edit Rule Definitions

The out-of-the-box rules in RA are generic and are configured for evaluating risk based on the rules that are applicable to all. If you need custom or industry-specific rules that are significantly different from those that RA provides out-of-the-box, then you need to deploy your own rules by using the *Rule Builder*, which is available through the Administration Console.

This topic describes how you can use the Rule Builder to make changes to the following rule definitions:

- Untrusted IP Check
- User Velocity Check
- Device Velocity Check
- Zone Hopping Check
- Device MFP Match

Editing Untrusted IP Types

RA uses the IP address of the user's computer as one of the input parameters to assess the risk of each transaction. RA evaluates the incoming transaction and checks if it originated from an IP address marked as *untrusted*. Such transactions are typically denied. The different categories of untrusted IP types are:

- **Negative**
IP addresses with this designation have been sources of fraudulent transactions in the past.

Important! Use this option, if you manually configured an IP addresses as negative, as discussed in "[Configuring Untrusted IP Addresses](#)".
- **Active**
IP addresses with this designation allegedly are anonymizing proxies that have been sources of fraudulent transactions and have been active in the last six months.
- **Suspect**
IP addresses with this designation allegedly are anonymizing proxies that have been active over the last two years, but not for the last six months.
- **Private**
IP addresses with this designation allegedly are anonymizing proxies that are not publicly accessible. These addresses typically belong to commercial ventures that sell anonymity services to the public.
- **Inactive**
IP addresses with this designation allegedly have been sources of fraudulent transactions, but have been found inactive in the last two years.
- **Unknown**
IP addresses with this designation allegedly are anonymizing proxies for which no positive results are currently available.

Note: The Active, Suspect, Private, Inactive, and Unknown negative type categories are derived from the Neustar IP Intelligence (formerly Quova) data.

To edit Untrusted IP Types:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. In the **RULENAME** column, click the **Untrusted IP Check** link.
The Risk Analytics Rule Builder page appears.
9. In the **Negative IP Types Configuration** section, select the applicable types of negative IP address categories, and click **Update**.
10. Click **Update** at the bottom of the Rule Builder page to save the changes.
The changes are not yet active and are not available to your end users.
11. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
12. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Editing User Velocity

The **User Velocity Check** rule keeps a check on the number of transactions from a user within a specified period of time. It is based on the following parameters:

- **Number of Risk Evaluations per User**
Denotes the number of transactions (**N**) performed by RA for a specified user, irrespective of the Advice or Risk Score.
The default value for this parameter is **5**.
- **Time Interval**
Denotes the time period (**T**) in which the number of transactions are tracked.
The default value for this parameter is **60**.
- **Unit for Time Interval**
Denotes the unit in which the time period (**T**) is measured.
The default value for this parameter is **Minutes**.

Note: The User Velocity Check rule uses the RA system time rather than the transaction time received as part of the incoming message when comparing the transaction history to determine whether the rule should be triggered or not. This allows for cross-channel rule configuration

To configure the User Velocity rule:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. In the **RULENAME** column, click the **User Velocity Check** link.
The Risk Analytics Rule Builder page appears.
9. Specify a value for the number of risk evaluations per user in the **Greater than** field.
10. Specify the time interval.
This value denotes the maximum number of transactions (within the specified time interval) that is considered safe for a user. If the actual number of transactions within the specified time exceeds this number, then RA will track it as a risk, which will result in the matching of the User Velocity rule.
11. Select the unit for the time interval from the drop-down list.
12. Click **Update** to build the rule fragment.
13. Click **Update** at the bottom of the Rule Builder page to save the changes.
The changes are not yet active and are not available to your end users.
14. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
15. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Editing Device Velocity

The **Device Velocity Check** rule keeps a check on the number of transactions from a device within a specified period of time. It is based on the following parameters:

- **Number of Risk Evaluations per Device**

Denotes the number of transaction (**M**) performed by RA for a specified device, irrespective of whether the risk evaluation resulted in success or failure.

The default value for this parameter is **10**.

- **Time Interval**

Denotes the time period (**T**) in which the number of transactions are tracked.

The default value for this parameter is **60**.

- **Unit for Time Interval**

Denotes the unit in which the time period (**T**) is measured.

The default value for this parameter is **Minutes**.

Editing Device Velocity Rule

To edit the configuration of the Device Velocity rule:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. In the **RULENAME** column, click the **Device Velocity Check** link.
The Risk Analytics Rule Builder page appears.
9. Specify the number of risk evaluations per device in the **Greater than** field.
10. Specify the time interval.
This value denotes the maximum number of transactions (within the specified time interval) that is considered safe for a device. If the actual number of transactions within the specified time exceeds this number, then RA tracks the transaction as a risk, which results in the matching of the Device Velocity rule.
11. Select the unit for the time interval from the drop-down list.
12. Click **Update** to build the rule fragment.
13. Click **Update** at the bottom of the Rule Builder page to save the changes.
The changes are not yet active and are not available to your end users.
14. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.

15. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Editing Zone Hopping

Zone hopping tracks successive transactions from the same user that occur at distant locations (separated by large distances) at a speed beyond what is reasonably possible within a short time span. For example, if Bob logs in from New York at 9 AM (GMT) and again from London at 10 AM (GMT), then the Zone Hopping Check rule will track the latter transaction as risky.

Parameters Used by the Rule

The Zone Hopping Check rule is based on the following parameters:

- **Maximum Speed at which a User can Travel**
Denotes the maximum speed (**S**, in miles per hour) at which a user can physically travel using conventional transport, such as airplanes, cars, and trains.
If the speed at which a user appears to have moved (in the time frame between two successive transactions) exceeds this pre-configured threshold speed (**S**), then RA considers it as a case of zone hopping.
By default this value is 500 miles, but you can configure it by setting the value of the **Maximum Speed at which a User can Travel** field in the RA Rule Builder page.
- **Maximum Number of Users Sharing the Same User ID**
Sometimes, multiple users (for example, husband and wife) can use the same user name because they might be located in different zones. In such cases, RA must not consider this as a case of Zone hopping. For example, if husband logs in from New York at 10 AM (GMT) and wife from London at 11 AM (GMT), then RA will not mark these transactions as risky.
By default this value is 1, but you can configure it to 2 by editing the **Maximum Number of Users Sharing the Same Username** field in the RA Rule Builder page.
- **Maximum Distance Tolerance for IP Address Locations**
Because of variation in location of the IP address provided by ISPs, a user's physical location (geographic latitude and longitude) cannot be determined to a high level of precision by using their public IP address. To address this, RA uses an uncertainty offset (**U**, in miles) to accommodate the variation in the physical location of the IP address from which the transaction originated.
By default this variation is about 50 miles, but you can configure it by setting the value of **Maximum Distance Tolerance for IP Address Location** field in the Risk Analytics Rule Builder page.

Note: The Zone Hopping Check rule uses the RA system time rather than the transaction time received as part of the incoming message when comparing the transaction history to determine whether the rule should be triggered or not. This allows for cross-channel rule configuration.

To edit the definition of the Zone Hopping rule in a ruleset:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.

5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. In the **RULENAME** column, click the **Zone Hopping Check** link.
The Risk Analytics Rule Builder page appears.
9. Specify a value for the **Maximum Speed at Which the User Can Travel** parameter.
10. Specify a value for the **Maximum Number of Users Sharing the Same User ID** parameter.
11. Specify a value for the **Maximum Distance Tolerance for IP Address Location** parameter.
12. Click **Update**.
13. Click **Update** at the bottom of the Rule Builder page to save the changes.
The changes are not yet active and are not available to your end users.
14. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
15. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

Editing Machine FingerPrint (MFP) Match Percentage

The **Device MFP Match** rule checks if the match percentage between the input device signature and the corresponding stored device signature is greater than or equal to a specified Signature Pass Threshold.

To configure the MFP Match Percentage rule:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.

8. In the **RULENAME** column, click the **Device MFP Match** link.
The Risk Analytics Rule Builder page appears.
9. Enter a value for the **Signature Match Threshold** and **Reverse Lookup Threshold**, and click **Update**.
10. Click **Update** at the bottom of the Rule Builder page to save the changes.
The changes are not yet active and are not available to your end users.
11. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
12. Refresh *all* deployed Transaction Server instances.
See [How to Refresh Server Cache](#) for instructions on how to do this.

How to Delete a Rule

Important! You can delete only the new rules that you have created and deployed. You cannot delete the out-of-the-box rules shipped with RA. Also, it is strongly recommended that you do not delete a rule that is still being used by another organization. That is why this task must be done at organization level.

To delete a rule:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.
The Rules and Scoring Management page appears.
8. Expand the rule that you want to delete by clicking the [+] sign.
9. Click **Delete this Rule**.
You get a message.
10. Click **OK** to complete the task.
You get the confirmation message.
11. Click **OK**.
The changes are not yet active and are not available to your end users.

12. To make the changes active, you must migrate them to production.
Refer to [How to Activate a Rule \(Migrate Rules to Production\)](#) for instructions to do so.
13. Refresh all deployed Transaction Server instances.
Refer to [How to Refresh Server Cache](#) for instructions to do so.

Creating Custom Rules by Using Rule Builder

The out-of-the-box rules in RA are generic and are configured for evaluating risk based on the rules that are applicable to all. If you need custom or industry-specific rules that are significantly different from those that RA provides out-of-the-box, then you need to deploy your own rules. RA provides a powerful feature called **Rule Builder** for this purpose. This feature is available through the Administration Console and is a GUI-based console that enables you to build rules on-the-fly by providing information in various fields and controls.

The information that you need to supply to this Rule Builder includes:

- Data Elements (See [What Are Data Elements](#))
 - Rule Tags (See [What Are Rule Tags](#))
- Operators (See [Understanding the Types of Operators Used by the Rule Builder](#))
- Multi-Byte characters and encrypted parameters (See [What Are Multi-Byte Characters and Encrypted Parameters](#))

[Examples of Using New Rules](#) illustrates with examples how these rule building blocks can be used.

[How to Create a Custom Rule](#) and [After Creating a Custom Rule, What Next](#) walk you through the process of creating a new rule and ensuring that it is used in future risk evaluations by RA. Finally, [What Else Can I Do with My Custom Rule](#) discusses how to manage the your custom rule..

What are Data Elements

You can select from the following types of data elements to build a new rule using Rule Builder:

- **Transaction Elements**
Enable you to create a rule to identify suspicious transaction patterns on all channels.
- **Device Elements**
Enable you to create a rule to identify risk associated with a particular device.
- **Geolocation Elements**
Enable you to create a rule to analyze the user's geolocation data from where the transaction was performed.
- **Model Elements**
Enable you to create a rule to analyze a transaction based on the Model score.

- **Custom Elements**

Enable you to create your own data element, which is not available in the list of pre-configured data elements.

Note: For detailed information on Data Elements that can be used in each channel and the operators that are allowed with them, see [Understanding Data Elements](#).

What are Rule Tags

Rules take data elements, called *tags*, as input. In other words, data elements are also known as Tags in RA terminology. Two most common tags used by RA are the end user's country and the transaction amount. These tags are then referenced in rules either through an explicit reference called a *TagName*, or by using an implicit reference by the context of the rule.

You can use the data listed in the following table to include in your rules. This data is classified into the following broad categories:

- **User Information:** Provides information about the user and the account.
- **Device Information:** Provides information about the device used to originate the transaction.
- **Transaction Information:** Provides information about elements of every transaction, such as the channel and action.
- **Currency Information:** Provides information such as currency conversion rate and base currency.
- **Location Information:** These elements are derived from a maintained database of IP geolocation, which provides location data and connection attributes of the IP address.
- **Internal Parameters:** Support the construction of custom rule types.

Note: Some of this data is collected by the **evaluateRisk()** API call with the help of extensible data structures called *contexts*. On the other hand, the other data is derived through lookups, such as the geolocation of the end user's or cardholder's IP address.

Tag Name	Channel	Description
User Information		
IDENTITY.USERID	All	The user identifier. If encryption was enabled, then this tag represents the encrypted version of the user identifier.
RULESET.GROUPNAME	All	The organization name.
Device Information		
DEVICEID.http	Default, 3D Secure	The alpha-numeric ID assigned by RA for this device.
DEVICEID.flash	Default, 3D Secure	The Flash device ID string specific to the transaction.
DEVICESIG	Default, 3D Secure	The device signature gathered from the end user's system to generate a risk profile of a device in real time.

Tag Name	Channel	Description
SHORTDEVICESIG	Default, 3D Secure	The compact form of the device signature.
AGGREGATORINFO	Default, 3D Secure	Aggregator ID string specific to the transaction.
RULE.SIGPASSTHRESHOLD	Default, 3D Secure	Pass threshold used by the Device MFP Match rule.
General Transaction Information		
RULESET.CHANNELNAME	All	The channel using which the user accesses the system.
TRANSACTION.TXNID	All	The numeric identifier for this transaction generated by RA.
TRANSACTION.EXT	Default, 3D Secure	Name-value Extensible element string sent by the client.
Currency Information		
BASE_CURR_CODE	3D Secure, ATM, POS	Numeric designation corresponding to the 3-letter designation of the base currency of the organization.
BASE_CURR_AMOUNT	3D Secure, ATM, POS	Transaction amount converted to the Base Currency.
BASE_CONVERSION_RATE	3D Secure, ATM, POS	Conversion rate from transaction currency to the base currency of the organization.
Location Information		
RULESET.COUNTRYISO	Default, 3D Secure	Contains the two letter ISO 3166 alpha country code of the country, for example AU.
RULESET.STARTIP	Default, 3D Secure	Starting IP for the user IP block.
RULESET.ENDIP	Default, 3D Secure	Ending IP for the user IP block.
RULESET.GEOLAT	Default, 3D Secure	Latitude is expressed as a floating point number with positive numbers representing North and negative numbers representing South.
RULESET.GEOLONG	Default, 3D Secure	Longitude is expressed as a floating point number with positive numbers representing East and negative numbers representing West.
RULESET.GEOCF	Default, 3D Secure	Confidence Factor (CF) in the geolocation. Confidence Factors are calculated based on the precision, completeness, and consistency of the data available to assign a specific geographic location to an IP

Tag Name	Channel	Description
		address range. Confidence Factors are provided for Country, State, and City. Their value ranges from 1 to 99. A higher value indicates that the likelihood of a correct location assignment is higher; a lower value indicates the opposite. These values are not percentages. Their intended use is as a relative measure of "confidence" on the correctness of the corresponding location assignment.
Internal Parameters		
RULE.USERCONTEXT	Default, 3D Secure	User context information used internally by the rules engine to store state information.
RULE.DEVICECONTEXT	Default, 3D Secure	Device context information used internally by the rules engine to store state information.
ADDONRULE.DESCRRESULT	All	The concatenated string of results from the add-on rules called till this point.
ADDONRULE.ANNOTATION	All	The concatenated strings of annotations set by all add-on rules called till this point.
RULE.RULEMNEMONIC	All	Rule mnemonic configured for the rule.

The following table provides an interpretation of RESULT_DEVICEIDCHECK.

RESULT_DEVICEID CHECK	DEVICEIDCHECKR ULE	USERDEVICEASSO CIATEDRULE	ISDEVICEKNOWN	ISUSERASSOCIATE D
YY	Enabled	Enabled	Y	Y
NN	Enabled	Enabled	N	N
YN	Enabled	Enabled	Y	N
<blank>	Enabled	Disabled	Y	None
NN	Enabled	Disabled	N	None
<blank>	Disabled	Disabled	None	None

What are Operators

See [Understanding the Types of Operators Used by the Rule Builder](#) for details on operators that you can use with data elements to create complex equations.

What are Multi-Byte Character and Encrypted Parameters

RA supports the UTF-8 standard, which is a variable-width 8-bit encoding format of the universal Unicode encoding scheme. This variable-width encoding enables you to use varying number of bytes to encode a character set.

RA also enables you to use hardware- or software-based encryption of your sensitive data. You can choose to encrypt sensitive parameters and also decide whether you want to display clear text data or encrypted data in Reports. The following table lists the parameters that can be selected for encryption and multi-byte character encoding. It also lists the keys used for the parameter and the level at which the key is applicable.

Parameter	IsEncrypted	HSM Support	KeyLevel	Key Type	IsMultiByte
UserName	Optional	Yes	Organization	OrgKey	Yes
User attributes	Optional	Yes	Organization	OrgKey	Yes
Configurations					
Action	No	No	None	None	No
OrgName	No	No	None	None	No
DeviceID	No	No	Global	Fixed - Internal	Yes
Device Signature	No	No	None	None	Yes
CALLERID	No	No	None	None	Yes
CONFIGNAME	No	No	None	None	No
CHANNELNAME	No	No	None	None	No
CLIENTIPADDRESS	No	No	None	None	No
AGGREGATORNAME	No	No	None	None	No
ASSOCIATIONNAME	No	No	None	None	No
ACCOUNTTYPE	No	No	None	None	No
MATCHEDRULE	No	No	None	None	No
LINESPEED	No	No	None	None	No
CONNECTIONTYPE	No	No	None	None	No
ANONYMIZATIONTYPE	No	No	None	None	No
IP_ROUTINGTYPE	No	No	None	None	No
Rule Mnemonic	No	No	None	None	No
Rule Name	No	No	None	None	Yes
Rule Description	No	No	None	None	Yes
ACCOUNTID	No	No	None	None	Yes
PARENTUSERID	No	No	None	None	Yes

Parameter	IsEncrypted	HSM Support	KeyLevel	Key Type	IsMultiByte
ERROR MESSAGE	No	No	None	None	Yes
QUEUE NAME	No	No	None	None	No
QUEUE DESCRIPTION	No	No	None	None	Yes
CASENOTE	No	No	None	None	Yes
3D Secure Elements					
ACQ_BIN	No	None	None	None	No
MERCHANT_NAME	No	No	None	None	Yes
MERCHANT_ID	No	No	None	None	No
MERCH_COUNT	No	No	None	None	No
MERCHANT_URL	No	No	None	None	No
XID	No	No	None	None	No
PURCHASE_DESCRIPTION	No	No	None	None	Yes
PAN	No	No	None	None	No
EXPIRY	No	No	None	None	No
MERCH_CAT	No	No	None	None	No
TERM_URL	No	No	None	None	No
PREVTXNDATA	No	No	None	None	No

The following table describes whether the parameter is case-insensitive and whether it is displayed in reports.

Parameter	Case Insensitive	Displayed in Reports
UserName	Yes	Yes
User attributes	Yes	Yes
Configurations		
Action	No	Yes
OrgName	No	Yes
DeviceID	No	Yes
Device Signature	No	No
CALLERID	No	No
CONFIGNAME	No	Yes
CHANNELNAME	No	Yes
CLIENTIPADDRESS	No	Yes
AGGREGATORNAME	No	Yes
ASSOCIATIONNAME	No	
ACCOUNTTYPE	No	Yes

Parameter	Case Insensitive	Displayed in Reports
MATCHEDRULE	No	Yes
LINESPEED	No	
CONNECTIONTYPE	No	
ANONYMIZERTYPE	No	Yes
IP_ROUTINGTYPE	No	
Rule Mnemonic	No	Yes
Rule Name	No	Yes
Rule Description	No	Yes
ACCOUNTID	No	Yes
ERROR MESSAGE	No	No
QUEUE NAME	No	Yes
QUEUE DESCRIPTION	No	Yes
CASENOTE	No	Yes
3D Secure elements		
ACQ_BIN	No	Yes
MERCHANT_NAME	No	Yes
MERCHANT_ID	No	Yes
MERCH_COUN	No	Yes
MERCHANT_URL	No	Yes
XID	No	No
PURCHASE_DESCRIPTION	No	No
PAN	No	No
EXPIRY	No	No
MERCH_CAT	No	No
TERM_URL	No	No
PREVTXNDATA	No	No

Examples of Using New Rules

The following examples illustrate how you can combine out-of-the-box RA rules and your rules to define custom combination rules by using multiple factors and conditions:

- High Amount Check
- High User Velocity from Unexpected Locations
- High Device Velocity from Unexpected Locations
- Wire Transfers from Unexpected Locations

Note: The rule (for example, SAFE_COUNTRIES) that you see in these examples represent a simple list rule that uses a list of countries considered to be the origin of safe transfers.

- Daily Maximum Amount Check
- Transactions Exceeding Thresholds
- Transactions Exceeding Thresholds for a Specified Action

High Amount Check

Consider the following details for an AMOUNT_CHECK rule that must check for transaction amounts more than \$500:

Rule Mnemonic: HIGHAMTCHK

Rule Display Name: High Amount Check

Description: This rule checks for high transaction amounts that exceed \$500.

Amount: 500

This example rule performs the following:

1. Parses the AdditionalInput string (say Amount=750) that is passed in the evaluateRisk() API call by the tag named Amount, and extract the value of this tag in a variable, say ActualAmount.
- Note:** Refer to the Javadocs for details on parsing the AdditionalInput elements.
2. Extracts the parameter value (500) for the rule, and store it in a variable, say ParameterAmount.
 3. Returns Matched because ActualAmount(750), in this case, is greater than ParameterAmount (500).

High User Velocity from Unexpected Locations

Consider that the SAFE_COUNTRIES refers to a simple list rule (where some of the elements are US,CA, UK, DE), then you can define a new rule to determine transactions with high User Velocity from unusual locations as:

USERVELOCITY AND NOT SAFE_COUNTRIES

High Device Velocity from Unexpected Locations

Similar to "High User Velocity from Unexpected Locations", you can define a new rule to determine transactions with high Device Velocity from unusual locations as:

DEVICEVELOCITY AND NOT SAFE_COUNTRIES

Wire Transfers from Unexpected Locations

Consider that you have created a rule called HIGHAMTCHK (as discussed in "High Amount Check".) Also, if the SAFE_COUNTRIES rule uses a list of countries considered to be origin of safe transfers, then you can define a rule to track low-value or high-amount wire transfers from unusual locations as:

(HIGHAMTCHK OR Amount < 20) AND NOT SAFE_COUNTRIES

Daily Maximum Amount Check

If the card holder has withdrawn cash exceeding the set threshold for three consecutive days (including the day of the current transaction), then you can restrict the current transaction.

Channel: ATM
Action: WITHDRAW
Element: Amount
Operator: GROUPED_CUMULATIVE_AMOUNT
Operator Parameters:
Threshold Cumulative Amount = <Desired Threshold Amount>
Grouping Period Count = 3
Minimum Threshold Breach Count = 3
Duration to look back(in Minutes)= 4320
Maximum Transactions to look back = 100
Time Frame Start Time = 0000
Time Frame End Time = 2359
Transactions to Consider = ALL

Three period groups (1 Group = 1 calendar day) are created, including the group (day) for the current transaction. The rule is triggered if the Threshold Cumulative Amount is exceeded for all the three groups (days).

Transactions Exceeding Thresholds

If the card holder has used the card for an amount exceeding the set threshold in the last one day or performed more than the specified number of transactions in the last one day for specified types of transactions, such as specific merchant categories or specific countries, then you can restrict the current transaction.

Channel: POS
Action: PURCHASE
Element: Amount
Operator: CUMULATIVE_AMOUNT
Operator Parameters:
Threshold Cumulative Amount = <Desired Threshold Amount>
Threshold Transaction Count=10
Duration to look back(in Minutes)= 1440
Maximum Transactions to look back = 100
Transactions to Consider = ALL
AND
Element: MERCH_CAT
Operator: IN_LIST

If the cumulative amount in the specified time frame (one day) exceeds the Threshold Cumulative Amount or the number of transactions exceeds the Threshold Transaction Count, then the rule is triggered.

Transactions Exceeding Thresholds for a Specified Action

If the card holder has changed their PIN in the last one day and has used the card for an amount exceeding the set threshold in the last one day or performed more than the specified number of transactions in the last one day for specified types of transactions, such as specific merchant categories or specific countries, then you can restrict the current transaction.

Channel:ATM
Action:WITHDRAWAL
Element:Amount
Operator:ACTION_CUMULATIVE_AMOUNT
Operator Parameters:
Threshold Cumulative Amount = <Desired Threshold Amount>
Threshold Transaction Count=10
Duration to look back(in Minutes)= 1440
Maximum Transactions to look back = 100
Threshold Action = PINCHANGE
Transactions to consider = All
AND
Element:MERCH_CAT
Operator:IN_LIST

If there was a PINCHANGE in the specified time frame (one day) and if the cumulative amount in the specified time frame (one day) exceeds the Threshold Cumulative Amount or the number of transactions exceeds the Threshold Transaction Count, then the rule is triggered.

How to Create a Custom Rule

To build a new rule to meet your business requirements:

1. Ensure that you are logged in as a GA or an OA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **Risk Engine** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.
The Rules and Scoring Management page appears.
7. From the **Select a Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. Click **Add a New Rule**.
The Risk Analytics Rule Builder page is displayed.
9. Enter the basic information for the rule, as described:
 - Name: The display name for the rule that you want to create.
 - Mnemonic: A short name for the rule that is used for logging purposes and in APIs. The maximum length of the mnemonic is 15 characters and no spaces are allowed.
 - Description: A short description of the rule being created.
10. Select the **Channels** and **Actions** for which this rule is applicable.

11. If you want to select all the channels and all the actions, select the **All Channels** and **All Actions** check boxes.
Each rule must be associated with one or more Channels and Actions. By default, a rule is associated with **All Channels** and **All Actions**.
12. Build the rule fragment, as follows:
 - a. From the **Select Data Element(s)** list, select from the following elements:
 - Transaction
 - Device
 - Geolocation
 - Model
 - Custom
 - b. Select the operator from the **Select Operator** list to edit the rule that you are creating.
 - c. Click **Add** to add the rule fragment to the **Rule being developed** area.
13. Build your complete rule by using the available logical operators, your rule fragment, and the rules in the **Saved Rules** list.
14. Click **Create** to create your rule.

After Creating a Custom Rule, What Next

After you create a new rule, you need to do the following tasks so that the rule is used during risk evaluation:

1. Upload any data, if the rule uses a list.
2. Enable the rule.
3. Assign the ruleset (to which the rule belongs) to an organization.
4. Migrate it to production.
5. Refresh the server cache.

The following steps quickly explain these tasks.

Step 1: Upload Rule List Data, If Any

If your rule uses a list of values against which it assesses a condition, then you need to upload that data as a list.

To upload the data for a list, see, [How to Upload Rule List Data](#) for detailed instructions.

Step 2: Enable the Rule

The rule that you just created ([How to Create a Custom Rule](#)) must be enabled so that it can be a part of the parent ruleset. To enable the rule:

1. In the Administration Console, access the Rules and Scoring Management page.
2. From the **Select a Ruleset** list, select the ruleset for which this configuration is applicable. The configuration for the specified ruleset appears.
3. Select the **Enable** option against the rule you just created.
4. Click **Save** at the bottom of the rules table.

Step 3: Assign the Ruleset to Which the Rule Belongs

After you activated the new rule by enabling it (as discussed in the preceding section), then the next thing you will need to do is activate the parent ruleset to which your rule belongs. This process of activating a ruleset is known as assigning a ruleset.

To assign a ruleset, see, [How to Assign a Ruleset to an Organization](#) for detailed instructions.

Step 4: Migrate the Rule to Production

When the rule is configured, it is still in the Proposed Configuration area and is only still available in the **Proposed** column of rule configuration. When the rule is ready and all its data is configured according to your requirements, then you must convert it from its current the Proposed state to Active state (the **Active** column on respective configuration page). This can only be done by migrating it to production.

To make the changes active, see [How to Activate a Rule \(Migrate Rules to Production\)](#) for detailed instructions.

Step 5: Refresh the Server Cache

Migrating a major change (such as a new rule) to production does not affect the cache of the active server instances. Each instance's cache needs to be refreshed before the server can start serving it for risk evaluations. That is why, you now need to refresh the server cache.

To refresh the cache of all deployed Transaction Server instances, see [How to Refresh Server Cache](#) for detailed instructions.

What Else Can I Do with My Custom Rule

After you have successfully created and activated a rule for risk evaluation, you can manage the rule as follows:

- At a later stage, you can **edit the rule definition** to fine-tune its performance. See section [How to Edit Rule Definitions](#) for more information.
- If the rule becomes obsolete, then you can **delete the rule**. See section [How to Delete a Rule](#) for more information.

Understanding Data Elements

This article describes the data elements and rule tags that you can use to build and deploy rules in the Rule Builder. It covers the following topics:

- [Quick Overview of Data Elements](#)
- [Transaction Elements](#)
- [Device Elements](#)
- [Geolocation Elements](#)
- [Predictive Model Elements](#)
- [Custom Elements](#)
- [History Rule Elements for ATM and POS](#)

Quick Overview of Data Elements

The out-of-the-box rules in Risk Analytics are generic and are configured for evaluating risk based on the rules that are applicable to all. If you need custom or your industry-specific rules that are significantly different from those that RA provides out-of-the-box, then you need to build and deploy your own rules by using the **Rule Builder** capability in RA.

When using the Rule Builder, you need to supply the following types of information:

- Data Elements
- Operators
- Rule Tags

What Are Data Elements

A *Data Element* is a unit of data that can be uniquely identified, defined, and assigned a value. By defining key data elements, RA ensures that you (as a rule builder) have access to a data dictionary that offers a clear understanding of the data element as well as its value.

When you use Risk Analytics Rule Builder to create new rules, you need *Data Elements* and *Operators* to do so.

What Are Rule Tags

Data elements are referenced in RA rules either using an explicit reference called a *TagName*, or implicit reference by the context of the rule. You can use the data listed in the following table to include in your rules. Some of this data is provided in the RA **evaluateRisk()** call and other data is derived through lookup, such as the geolocation of the end user's or cardholder's IP address.

What Are the Different Types of Data Elements Available

Depending on the rule that you want to create, the key types of data elements that are identified and defined in the risk profile that you can select from are:

- **Transaction Elements:** Enable you to create a rule to identify suspicious transaction patterns on all channels.
- **Device Elements:** Enable you to create a rule to identify risk associated with a particular device.
- **Geolocation Elements:** Enable you to create a rule to analyze the user's geolocation data from where the transaction was performed.
- **Model Elements:** Enable you to create a rule to analyze a transaction based on the Model score.
- **Custom Elements:** Enable you to create your own data element, which is not available in the list of pre-configured data elements. For a list of element names that you can use for custom elements, see **Risk Analytics Rule Tags**.

What Are the Different Operators That I Can Use

An *Operator* is a boolean, arithmetic, logical, or assignment functions that enable you to manipulate the supported data elements to build desired custom rules.

Operators that you use to create rules can be grouped into the following categories:

- **Expression:** These operators are used to combine rule fragments to build a rule. Possible operators include AND, OR, NOT, (, and) operators.
- **Match Type:** These operators are used by the IN_CATEGORY and IN_LIST operators. Possible operators include the following:
 - **EXACT:** If the list value matches the input value exactly, then the rule is triggered.
 - **PARTIAL:** If any of the values in the list is a partial substring of the input value, then the rule is triggered.

For example, a list with values 40001, 50001, and 60001 would trigger the rule for PARTIAL match with an input value of 40001000100010001. Similarly, a list with values alice, cathy, and karim would trigger the rule for PARTIAL match with an input value of "Karima" and for EXACT match with an input value of "Karim".

Note: Both EXACT and PARTIAL matches are case-insensitive.

- **LookUp Type:** Possible operators include IN_LIST, IN_TRUSTED_LIST, and IN_NEGATIVE_LIST.
- **Operator:** These operators are used for numeric comparison of data elements. Possible operators include RANGE, EQUAL_TO (=), NOT_EQUAL_TO (!=), GREATER_OR_EQUAL (>=), LESS_OR_EQUAL (<=), GREATER_THAN (>), and LESS_THAN (<).

Operators specific to ATM and POS channels include the following:

- EQUAL_TO_CB, NOT_EQUAL_TO_CB, GREATER_OR_EQUAL_CB, LESS_OR_EQUAL_CB, GREATER_THAN_CB, and LESS_THAN_CB, where CB indicates the Card BIN.

- **History-Based Operators:** Transaction History is defined as the list of transactions for the same account (Card Number or PAN) over ATM and POS channels in reverse chronological sequence. The transaction history available is restricted to the maximum history duration (Duration to Look Back) set at the global level. Operators that leverage the Transaction History are referred to as "History-Based Operators". For more information, see **History-Based Operators**.

Transaction Elements

Incoming transaction data during an online transaction constitutes one of the most important category of information that RA uses to identify suspicious user behavior and build behavior patterns. Key transaction elements include user name, transaction time and date, action performed. In addition to these generic elements, RA also collects and uses channel-specific transaction elements to build the channel-specific profile. For example, RA collects details related to acquirer BIN and merchant details during a 3D Secure transaction. On the other hand, during an ATM or POS transaction, RA collects information pertaining to the card and to the ATM or POS device.

This topic walks you through the transaction elements that can be used for building your custom rule and covers the following sub-topics:

- [Transaction Elements for the Default Channel](#)
- [Transaction Elements for 3D Secure Channel](#)
- [Transaction Elements for ATM and POS Channels](#)
- [Transaction Elements for IMPS Channel](#)
- [Transaction Elements for ECOM Channel](#)

Transaction Elements for the Default Channel

The following table describes the transaction elements and the corresponding operators for the **Default channel**.

Data Element	When to Use	Operator Description
ACTION	If your rule needs to track whether one or more pre-defined actions is available in a list or performed during a particular duration.	<ul style="list-style-type: none"> ▪ IN_LIST:Checks whether the action performed is available in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ VELOCITY:Checks whether the frequency of transactions of the specified

Data Element	When to Use	Operator Description
		<p>set of actions have met or exceeded a pre-defined threshold and returns True if this condition is met. This rule is useful to detect situations where a prior password change makes the current transaction risky. For example, to check for a money transfer preceded by a password reset in the last 24 hours, you must set this rule Greater Than or Equal To 1 In last 24 Hours for the FORGOT_PWD action in the For Set of Actions list.</p> <ul style="list-style-type: none"> IN_CATEGORY: Checks for the action performed in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
USERNAME	If your rule needs to check whether the transaction was performed by a particular user.	<ul style="list-style-type: none"> IN_LIST: Checks whether the user is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. VELOCITY: Checks whether the number of transactions for a particular user exceeds the limits set by the specified duration and frequency. ZONE_HOP: Checks for transactions that originate from the same user from large distances within a short interval.
CURRENTTIME	If your rule needs to identify suspicious transaction patterns based on the time the transaction was performed.	<ul style="list-style-type: none"> Compares the CURRENTTIME when the transaction was performed with the specified Time by using the following operators: <ul style="list-style-type: none"> EQUAL_TO

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> ▪ NOT_EQUAL_TO ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL ▪ IN_LIST: Checks whether CURRENTTIME is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for CURRENTTIME in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: The format of CURRENTTIME is HHMM.</p>
DATE	If your rule needs to identify suspicious transaction patterns based on the date the transaction was performed.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether DATE is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ Compares the transaction DATE with the specified Date by using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> IN_CATEGORY: Checks for DATE in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: The format of DATE is YYYYMMDD.</p>
DAYOFMONTH	If your rule needs to identify suspicious transaction patterns based on the day of the month when the transaction was performed.	<ul style="list-style-type: none"> IN_LIST: Checks whether DAYOFMONTH is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the DAYOFMONTH when the transaction was performed with the selected Day of Month by using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for DAYOFMONTH in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: DAYOFMONTH is a 2-digit number where 01=January, 02=February, and so on.</p>
DAYOFWEEK	If your rule needs to identify suspicious transaction patterns based on the day of the week when the transaction was performed.	<ul style="list-style-type: none"> IN_LIST: Checks whether DAYOFWEEK is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to

Data Element	When to Use	Operator Description
		<p>enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> IN_CATEGORY: Checks for DAYOFWEEK in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: Permitted values for DAYOFWEEK are SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, and SATURDAY.</p>
HOUROFDAY	If your rule needs to identify suspicious transaction patterns based on the hour of the day when the transaction was performed.	<ul style="list-style-type: none"> IN_LIST: Checks whether HOUROFDAY is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the HOUROFDAY when the transaction was performed with the selected Hour of Day by using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for HOUROFDAY in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
<p>Note: HOUROFDAY is a 2-digit number representing hours of the day from 00 to 23.</p>		
MONTH	If your rule needs to identify suspicious transaction patterns based on the month the transaction was performed.	<ul style="list-style-type: none"> IN_LIST: Checks whether the transaction MONTH is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the transaction MONTH with the specified Month using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for MONTH in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: The format of MONTH is MM.</p>
PERSPECTIVE	If your rule needs to identify suspicious transaction patterns based on the perspective from which you want to monitor the transaction, whether Acquirer, Issuer, or Beneficiary.	MATCHES: Compares the perspective name with the String to compare . Only exact matches are allowed.
YEAR	If your rule needs to identify suspicious transaction patterns based on the year the transaction was performed.	<ul style="list-style-type: none"> IN_LIST: Checks whether the transaction YEAR is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than

Data Element	When to Use	Operator Description
		<p>10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <ul style="list-style-type: none"> ▪ Compares the transaction YEAR with the specified Year using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL ▪ IN_CATEGORY: Checks for YEAR in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: The format of YEAR is YYYY.</p>

Transaction Elements for 3D Secure Channel

The following table describes the transaction elements that are specific to the **3D Secure channel**. This channel pertains to all transactions that are based on 3D Secure protocol used for Visa and MasterCard payments, for protection from the unauthorized use of their credit cards.

Data Element	When to Use	Operator Description
ACQ_BIN	If your rule needs to check the Acquirer BIN of the merchant where the transaction was made.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Acquirer BIN is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for Acquirer BIN in a table in the mapping data set, and then compares the

Data Element	When to Use	Operator Description
		<p>associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <ul style="list-style-type: none"> ▪ MATCHES: Compares the Acquirer BIN with the String to compare. Only exact matches are allowed.
ACTION	If your rule needs to track whether one or more pre-defined actions is available in a list or performed during a particular duration.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the action performed is available in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ VELOCITY: Checks whether the frequency of transactions of the specified set of actions have met or exceeded a pre-defined threshold and returns True if this condition is met. This rule is useful to detect situations where a prior password change makes the current transaction risky. For example, to check for a money transfer preceded by a password reset in the last 24 hours, you must set this rule Greater Than or Equal To 1 In last 24 Hours for the FORGOT_PWD action in the For Set of Actions list. ▪ IN_CATEGORY: Checks for the action performed in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
AMOUNT	If your rule needs to track transactions against a threshold amount in the specified currency.	<ul style="list-style-type: none"> ▪ Compares the transaction AMOUNT with the specified amount using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO

Data Element	When to Use	Operator Description
	<p>You can configure your rule to support automatic currency conversion. If this is enabled, then you need to only specify the threshold amount in your base currency. You may specify thresholds in additional currencies where you want to override the automatic conversion.</p> <p>For more information about the currency conversion table, see Currency Conversion.</p>	<ul style="list-style-type: none"> ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL ▪ IN_LIST: Checks whether the AMOUNT is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the AMOUNT in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
CURR_CODE	If your rule needs to check the 3-digit numeric currency code used for the transaction.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the currency code is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the currency code in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the currency code with the String to compare. Only exact matches are allowed.
MERCHANT_ID		<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether merchant ID is in a simple look-up list. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
	If your rule needs to identify suspicious transaction patterns based on the unique identifier of the merchant involved in the transaction.	<p>If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> ▪ IN_CATEGORY: Checks for the merchant ID in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the merchant ID with the String to compare. Only exact matches are allowed.
MERCHANT_NAME	If your rule needs to identify suspicious transaction patterns based on the name of the merchant involved in the transaction.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether merchant name is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the merchant name in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the merchant name with the String to compare. Only exact matches are allowed.
MERCHANT_URL	If your rule needs to identify suspicious transaction patterns based on the URL of the merchant involved in the transaction.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the merchant URL is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than

Data Element	When to Use	Operator Description
		<p>10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> IN_CATEGORY: Checks for the merchant URL in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. MATCHES: Compares the merchant URL with the String to compare. Only exact matches are allowed.
MERCH_CAT	If your rule needs to identify suspicious transaction patterns based on the category of the merchant involved in the transaction.	<ul style="list-style-type: none"> IN_LIST: Checks whether merchant category is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. IN_CATEGORY: Checks for the merchant category in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. MATCHES: Compares the merchant category with the String to compare. Only exact matches are allowed.
MERCH_COUN	If your rule needs to identify suspicious transaction patterns based on the country code of the merchant where the purchase is being made. MERCH_COUN is 3-digit ISO country code.	<ul style="list-style-type: none"> IN_LIST: Checks whether the merchant country is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> ▪ IN_CATEGORY: Checks for the merchant country in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the merchant country with the String to compare. Only exact mctches are allowed.
PREVTXNDATA	<p>If your rule wants to check whether the previous transaction matches any of the selected actions in the specified number of hours.</p> <p>The rule returns True if a previous transaction type was the same as the selected type for this user in the specified time frame.</p>	<ul style="list-style-type: none"> ▪ CHECK: Checks whether the type of the previous transaction performed in the specified duration for the given user matches one or more of the selected actions. The transaction types are: <ul style="list-style-type: none"> ▪ REGULAR: Regular purchase transaction. ▪ ATTEMPTS: Attempts transaction (user is not enrolled and the bank is permitted to notify the merchant that the bank attempted to authenticate the user). ▪ AE_WITH_PWD: Auto enrollment where all card holders have a valid password. ▪ AE_WITHOUT_PWD: Auto enrollment where some of the card holders may have empty passwords. ▪ FORGOT_PWD: Forgot password transaction. ▪ SEC_CH: Secondary Cardholder Addition (An additional card holder (username/password) was added to an existing card number). ▪ FORGOT_PWD_MULTI_CH: Forgot password transaction in a multiple cardholder scenario.

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> ▪ FORGOT_PWD_SINGLE_CH: Forgot password transaction in a single cardholder scenario (This is the same as FORGOT_PWD). ▪ ABRIDGED_ADS: Activation during shopping with a temporary password. ▪ SEC_CH_ABRIDGED: Secondary cardholder through abridged registration. ▪ UNKNOWN: Unknown transaction type (this is an exceptional situation).

Note: For the description of other 3D Secure elements, such as USERNAME, CURRENTTIME, DATE, DAYOFMONTH, DAYOFWEEK, HOUROFDAY, MONTH, PERSPECTIVE, and YEAR, see the table in [Transaction Elements for the Default Channel](#).

Transaction Elements for ATM and POS Channels

The following table describes the transaction elements that are specific to and common between the **ATM** and **Point of Sale (POS) channels**. This channel pertains to any card-based transactions that you perform on an Automated Teller Machine (ATM) or at a Point of Sale (POS).

Data Element	When to Use	Operator Description
ACCEPTOR_ID	If your rule needs to identify suspicious transaction patterns based on the ID of the card acceptor (merchant) operating the POS.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Acceptor ID is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ MATCHES: Compares the Acceptor ID with the String to compare. Only exact matches are allowed.
ACCEPTOR_TERMID	If your rule needs to identify suspicious transaction patterns based on the ID of the card acceptor (merchant) terminal or a POS.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Acceptor Terminal ID is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use

Data Element	When to Use	Operator Description
		<p>the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> ▪ MATCHES: Compares the Acceptor Terminal ID with the String to compare. Only exact matches are allowed.
ACQ_BIN	<p>If your rule needs to check the Acquirer BIN of the merchant where the transaction was made.</p> <p>The Acquirer BIN is a unique code allotted by ISO to identify the financial institution that acts as an acquirer.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Acquirer BIN is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the Acquirer BIN in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the Acquirer BIN with the String to compare. Only exact matches are allowed.
ACQ_COUNTRY	<p>If your rule needs to identify suspicious transaction patterns based on the code of the country where the acquiring institution for the POS is located.</p> <p>ACQ_COUNTRY is the country code defined according to the ISO 3166 standard.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Acquirer country code is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the Acquirer country code in a table in the mapping data set, and then compares the

Data Element	When to Use	Operator Description
		<p>associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <ul style="list-style-type: none"> ▪ MATCHES: Compares the Acquirer country code with the String to compare. Only exact matches are allowed.
ACTION	<p>If your rule needs to track whether one or more pre-defined actions is available in a list or performed during a particular duration.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the action performed is available in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ VELOCITY: Checks whether the frequency of transactions of the specified set of actions have met or exceeded a pre-defined threshold and returns TRUE if this condition is met. ▪ IN_CATEGORY: Checks for the action performed in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
AMOUNT	<p>If your rule needs to track transactions against a threshold amount in the specified currency.</p> <p>You can configure your rule to support automatic currency conversion.</p> <p>If this is enabled, then you need to only specify the threshold amount in your base currency. You may specify thresholds in additional currencies where you want to override the automatic conversion.</p>	<ul style="list-style-type: none"> ▪ Compares the transaction amount with the specified amount using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL ▪ If the configured Card BIN prefix matches the incoming Card BIN prefix, then this element can be used to compare the transaction amount with the Threshold

Data Element	When to Use	Operator Description
	For more information about currency conversion, see Currency Conversion .	<p>Amount based on Card BIN by using the following operators:</p> <ul style="list-style-type: none"> ▪ EQUAL_TO_CB ▪ NOT_EQUAL_TO_CB ▪ GREATER_THAN_CB ▪ LESS_THAN_CB ▪ GREATER_OR_EQUAL_CB ▪ LESS_OR_EQUAL_CB <p>▪ CUMULATIVE_AMOUNT: See table on the CUMULATIVE_AMOUNT operator in History-Based Operators.</p> <p>▪ GROUPED_CUMULATIVE_AMOUNT: See table on the GROUPED_CUMULATIVE_AMOUNT operator.</p> <p>▪ ACTION_CUMULATIVE_AMOUNT: See table on the ACTION_CUMULATIVE_AMOUNT operator.</p> <p>Note: For the ATM channel, the AMOUNT element appears only if you have selected the WITHDRAWAL action.</p>
CARDBIN_NAME	<p>If your rule needs to track transactions based on the Card BIN name.</p> <p>The card BIN is identified by the system based on Card Issuer to Organization mapping for the card involved in the transaction.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the card BIN name is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ MATCHES: Compares the card BIN name with the String to compare. Only exact matches are allowed.
CARDBIN_PREFIX	<p>If your rule needs to track transactions based on the Issuer BIN prefix.</p> <p>The card BIN is identified by the system based on Card Issuer to Organization mapping for the card involved in the transaction.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the card BIN prefix is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in

Data Element	When to Use	Operator Description
		<p>the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> ▪ MATCHES: Compares the card BIN prefix with the String to compare. Only exact matches are allowed.
CARD_HOLDER_AUTH_METHOD	<p>If your rule needs to track the transaction based on the method used to authenticate the card holder.</p> <p>This is a 1-digit value that represents how the card holder was authenticated at the POS terminal. Possible values are:</p> <ul style="list-style-type: none"> ▪ 0: Unknown ▪ 1: Not authenticated ▪ 2: PIN ▪ 3: Signature ▪ 4: Biometric ▪ 5: OTP ▪ 6: E-comm Type1 Pin ▪ 7: E-comm Type1 OTP ▪ 8: E-com Type 2 ▪ 9: IVR Type 2 	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the card holder authentication method is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the card holder authentication method in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the card holder authentication method with the String to compare. Only exact matches are allowed.
CURRCODE	<p>If your rule needs to check the currency code used for the transaction. CURRCODE represents the transaction currency code defined according to the ISO 4217 standard.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the currency code is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the currency code in a table in the mapping data set, and then compares the associated derived value of

Data Element	When to Use	Operator Description
		<p>the input in a list data set. Exact and partial matches are allowed.</p> <ul style="list-style-type: none"> ▪ MATCHES: Compares the currency code with the String to compare. Only exact matches are allowed.
LOCAL_DATE	<p>If your rule needs to identify suspicious transaction patterns based on the local date the transaction was performed.</p> <p>This is the date recorded in the POS device when the transaction began at the card acceptor location (in the local timezone of the merchant).</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the local date is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ Compares the local date with the specified date using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL <p>Note: The format of LOCALDATE is YYYYMMDD.</p>
LOCAL_TIME	<p>If your rule needs to identify suspicious transaction patterns based on the local time the transaction was performed.</p> <p>This is the time recorded in the POS device when the transaction began at the card acceptor location (in the local timezone of the merchant).</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the local time is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ Compares the local time with the specified time using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO ▪ GREATER_THAN

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL <p>Note: The format of LOCALTIME is HHMM.</p>
MERCH_CAT	<p>If your rule needs to identify suspicious transaction patterns based on the category code of the merchant involved in the transaction.</p> <p>MERCH_CAT is a 4-digit number that classifies suppliers into market segments.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether merchant category code is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. MATCHES: Compares the merchant category with the String to compare. Only exact matches are allowed.
POS_CONDITION_CODE	<p>If your rule needs to identify suspicious transaction patterns based on the 2-digit code that determines the transaction conditions at the POS.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> 00: Normal 01: Customer not present 02: Unattended terminal 03: Merchant suspicious 05: Customer present, Card not present 06: Preauthorization completion always contains 06 07: Telephone Request (IVR) 08: MO/TO Request 51: Request for Account and CVD verification without authorization 59: E-Commerce Request 71: Card present - Magnetic stripe cannot be read 	<ul style="list-style-type: none"> IN_LIST: Checks whether the POS condition code is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. IN_CATEGORY: Checks for the POS condition code in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. MATCHES: Compares the POS condition code with the String to compare. Only exact matches are allowed.
POS_ENTRY_MODE	<p>If your rule needs to identify suspicious transaction patterns based on the</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether POS_ENTRY_MODE is in a simple look-up list. Exact

Data Element	When to Use	Operator Description
	<p>POS_ENTRY_MODE, which is a 3-digit code that indicates the method used to enter the account number.</p> <p>The first two digits of the POS_ENTRY_MODE represent the PAN Entry Mode that can be one of the following:</p> <ul style="list-style-type: none"> 00: PAN entry mode unknown 01: Manual 02: Magnetic Stripe Read 03: Barcode reader 04: Optical card reader 05: ICC 06: IVR 07: Contactless payment using chip card 80: Fallback transactions 81: E-commerce 90: Full and unaltered magnetic stripe read (enables CVD validation) 91: Contactless using CVD, iCVD checking possible 95: Chip card with unreliable CVD 	<p>and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> IN_CATEGORY: Checks for POS_ENTRY_MODE in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. MATCHES: Compares the POS_ENTRY_MODE with the String to compare. Only exact matches are allowed.
	<p>The last digit represents PIN Entry Capability, and can take the following values:</p> <ul style="list-style-type: none"> 0: Unspecified 1: PIN Entry Capability 2: No PIN Entry Capability 3: PIN Pad Inoperative 	
TERMINALID	<p>If your rule needs to identify suspicious transaction patterns based on the Terminal ID. The Terminal ID is a combination of ACQ_BIN, ACCEPTOR_ID, ACCEPTOR_TERMID, and has the following format "ACQ_BIN-ACCEPTOR_ID-ACCEPTOR_TERMID".</p>	<ul style="list-style-type: none"> CUMULATIVE_AMOUNT: See table on the CUMULATIVE_AMOUNT operator in History-Based Operators. HISTORY_USER_VELOCITY: Checks whether the number of transactions (All, Approved, or Denied) from a particular Terminal ID exceeds the limits set by the specified duration and frequency. You can also choose to Exclude Current Transaction. An optional

Data Element	When to Use	Operator Description
		<p>custom history filter allows for additional filtering of the history data with the specified filter. The filter options available are: Reversed Transactions (REVERSAL_STATUS EQ 1), Issuer Approved Transactions (TXN_ACTION_CODE EQ 00), and Issuer Declined Transactions (TXN_ACTION_CODE NEQ 00). This additional history filter is not applicable to the current transaction and is applied to the history data fetched based on the normal history criteria prior to the actual data tabulation for rule triggering. The Distinct Attribute field allows you to specify the total number of distinct attributes in the user transaction history, for example if the user has used three different ATMs in the last 30 minutes.</p> <ul style="list-style-type: none"> IN_LIST: Checks whether the Terminal ID is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.
TIME	<p>If your rule needs to identify suspicious transaction patterns based on the transmission time.</p> <p>This is the time extracted from the date/time when the ISO 8583 message was constructed and is represented in GMT/UTC.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether the transmission time is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> Compares the transmission time with the specified time using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL <p>Note: The format of TIME is HHMM.</p>
TXN_ACTION_CODE	If your rule needs to identify suspicious transaction patterns based on the Issuer response, which is available if the incoming transaction message contains the same.	<ul style="list-style-type: none"> IN_LIST: Checks whether the transaction action code is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. MATCHES: Compares the transaction action code with the String to compare. Only exact matches are allowed.
TXN_TYPE	<p>If your rule needs to identify suspicious transaction patterns based on the transaction type.</p> <p>The transaction type is a 2-character code extracted from the processing code and can be one of the following:</p> <ul style="list-style-type: none"> 00: Purchase 01: Cash withdrawal/Cash at POS/Cash advance 02: Debit Adjustment 09: Purchase with Cashback 10: Withdrawal 20: Credit/Refund 21: Deposit 22: Credit Adjustment 30: Available Funds Enquiry 31: Balance Enquiry 40: Funds Transfer 	<ul style="list-style-type: none"> IN_LIST: Checks whether the transaction type is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. IN_CATEGORY: Checks for the transaction type in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> ▪ MATCHES: Compares the transaction type with the String to compare. Only exact matches are allowed.
USERNAME	If your rule needs to identify suspicious transaction patterns based on the card number of the card used in the financial transaction.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the card number is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ VELOCITY: Checks whether the number of transactions for a particular card number exceeds the limits set by the specified duration and frequency. For more information, see Configuring User Velocity. ▪ HISTORY_ZONE_HOPPING: Checks for transactions (All, Approved, or Denied) that originate from the same card number from large distances within a short interval. For more information, see Configuring Zone Hopping.
		<ul style="list-style-type: none"> ▪ HISTORY_USER_VELOCITY: Checks whether the number of transactions (All, Approved, or Denied) for a particular card number exceeds the limits set by the specified duration and frequency. You can also choose to Exclude Current Transaction. An optional custom history filter allows for additional filtering of the history data with the specified filter. The filter options available are: Reversed Transactions (REVERSAL_STATUS EQ 1), Issuer Approved Transactions (TXN_ACTION_CODE EQ 00),

Data Element	When to Use	Operator Description
		<p>and Issuer Declined Transactions (TXN_ACTION_CODE NEQ 00). This additional history filter is not applicable to the current transaction and is applied to the history data fetched based on the normal history criteria prior to the actual data tabulation for rule triggering. The Distinct Attribute field allows you to specify the total number of distinct attributes in the user transaction history, for example if the user has used three different ATMs in the last 30 minutes.</p>
CURRENTTIME	If your rule needs to identify suspicious transaction patterns based on the time the transaction was performed.	<ul style="list-style-type: none"> ▪ Compares the CURRENTTIME when the transaction was performed with the specified Time by using the following operators: <ul style="list-style-type: none"> ▪ EQUAL_TO ▪ NOT_EQUAL_TO ▪ GREATER_THAN ▪ LESS_THAN ▪ GREATER_OR_EQUAL ▪ LESS_OR_EQUAL ▪ IN_LIST: Checks whether CURRENTTIME is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for CURRENTTIME in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
DATE		

Data Element	When to Use	Operator Description
	<p>If your rule needs to identify suspicious transaction patterns based on the date the transaction was performed.</p> <p>The date is extracted from the date/time when the ISO 8583 message was constructed and is represented in GMT/UTC.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether DATE is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the transaction DATE with the specified Date by using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for DATE in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: The format of DATE is YYYYMMDD.</p>
DAYOFMONTH	<p>If your rule needs to identify suspicious transaction patterns based on the day of the month when the transaction was performed.</p> <p>The DAYOFMONTH is extracted from the date/time when the ISO 8583 message was constructed and is represented in GMT/UTC.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether DAYOFMONTH is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the DAYOFMONTH when the transaction was performed with the selected Day of Month by using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for DAYOFMONTH in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: DAYOFMONTH is a 2-digit number where 01=January, 02=February, and so on.</p>
DAYOFWEEK	<p>If your rule needs to identify suspicious transaction patterns based on the day of the week when the transaction was performed.</p> <p>The DAYOFWEEK is extracted from the date/time when the ISO 8583 message was constructed and is represented in GMT/UTC.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether DAYOFWEEK is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. IN_CATEGORY: Checks for DAYOFWEEK in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: Permitted values for DAYOFWEEK are SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, and SATURDAY.</p>
HOUROFDAY	If your rule needs to identify suspicious transaction patterns based on the hour of the day when the transaction was performed.	<ul style="list-style-type: none"> IN_LIST: Checks whether HOUROFDAY is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists

Data Element	When to Use	Operator Description
		<p>containing more than 10 items, use the Manage List Data and Category Mappings page.</p> <ul style="list-style-type: none"> Compares the HOUROFDAY when the transaction was performed with the selected Hour of Day by using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for HOUROFDAY in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: HOUROFDAY is a 2-digit number representing hours of the day from 00 to 23.</p>
MONTH	<p>If your rule needs to identify suspicious transaction patterns based on the month the transaction was performed.</p> <p>The MONTH is extracted from the date/time when the ISO 8583 message was constructed and is represented in GMT/UTC.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether the transaction MONTH is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the transaction MONTH with the specified Month using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for MONTH in a table in the mapping data set, and then

Data Element	When to Use	Operator Description
		<p>compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>Note: The format of the MONTH is MM.</p>
PERSPECTIVE	If your rule needs to identify suspicious transaction patterns based on the perspective from which you want to monitor the transaction, whether Acquirer, Issuer, or Beneficiary.	MATCHES: Compares the perspective name with the String to compare . Only exact matches are allowed.
YEAR	<p>If your rule needs to identify suspicious transaction patterns based on the year the transaction was performed.</p> <p>The YEAR is extracted from the date/time when the ISO 8583 message was constructed and is represented in GMT/UTC.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether the transaction YEAR is in a simple look-up list. Only exact match is allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. Compares the transaction YEAR with the specified Year using the following operators: <ul style="list-style-type: none"> EQUAL_TO NOT_EQUAL_TO GREATER_THAN LESS_THAN GREATER_OR_EQUAL LESS_OR_EQUAL IN_CATEGORY: Checks for YEAR in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. <p>Note: The format of the YEAR is YYYY.</p>

Transaction Elements for IMPS Channel

The following table describes the transaction elements that are specific to the **Interbank Payment Service (IMPS) channel**, an Indian inter-bank money transfer service using mobile phones.

IMPS is a channel-agnostic payment service introduced by National Payments Corporation of India (NPCI). Using IMPS, bank customers can transfer money instantly within any of the IMPS-enabled member banks across India. IMPS is accessible through mobile banking, net banking, and ATM channel. IMPS can be used for funds transfer and merchant payments. It supports the following services:

- P2P: Person to Person
- P2A: Person to Account
- P2M (Push): Person to Merchant initiated by Customer
- P2M (Pull): Person to Merchant initiated by Merchant

The following actions are supported for the IMPS channel:

- Purchase
- Funds Transfer

Data Element	When to Use	Operator Description
BENEFICIARY_ACCOUNTNO	If your rule needs to track the transaction based on the Beneficiary account number.	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Beneficiary account number is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data. ▪ IN_CATEGORY: Checks for the Beneficiary account number in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
BENEFICIARY_IMPSID	<p>If your rule needs to track the transaction based on the Beneficiary IMPSID.</p> <p>In the case of Person to Account (P2A) service, IMPSID is constructed as {A + IFSC CODE + Account Number}.</p>	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the Beneficiary IMPSID is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the

Data Element	When to Use	Operator Description
	For other services, IMPSID is constructed as {M + Beneficiary MMID + Beneficiary mobile number}.	<p>Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <ul style="list-style-type: none"> ▪ IN_CATEGORY: Checks for the Beneficiary IMPSID in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ CUMULATIVE_AMOUNT: See table on the CUMULATIVE_AMOUNT operator in History-Based Operators. ▪ HISTORY_USER_VELOCITY: Checks whether the number of transactions (All, Approved, or Denied) for a particular beneficiary exceeds the limits set by the specified duration and frequency. You can also choose to Exclude Current Transaction. An optional custom history filter allows for additional filtering of the history data with the specified filter. The filter options available are: Reversed Transactions (REVERSAL_STATUS EQ 1), Issuer Approved Transactions (TXN_ACTION_CODE EQ 00), and Issuer Declined Transactions (TXN_ACTION_CODE NEQ 00). This additional history filter is not applicable to the current transaction and is applied to the history data fetched based on the normal history criteria prior to the actual data tabulation for rule triggering. The Distinct Attribute field allows you to specify the total number of distinct attributes in the user transaction history, for

Data Element	When to Use	Operator Description
		example if the user has used three different ATMs in the last 30 minutes.
BENEFICIARY_MOBILE	<p>If your rule needs to track the transaction based on the mobile number of the Beneficiary.</p> <p>This is applicable for transactions other than P2A type.</p>	<ul style="list-style-type: none"> IN_LIST: Checks whether the Beneficiary mobile number is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data. IN_CATEGORY: Checks for the Beneficiary mobile number in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
CARD_HOLDER_AUTH_METHOD	<p>If your rule needs to track the transaction based on the method used to authenticate the card holder.</p> <p>This is a 1-digit value that represents how the card holder was authenticated at the POS terminal. Possible values are:</p> <ul style="list-style-type: none"> 0: Unknown 1: Not authenticated 2: PIN 3: Signature 4: Biometric 5: OTP 6: E-comm Type1 Pin 7: E-comm Type1 OTP 8: E-com Type 2 9: IVR Type 2 	<ul style="list-style-type: none"> IN_LIST: Checks whether the card holder authentication method is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data. IN_CATEGORY: Checks for the card holder authentication method in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
		<ul style="list-style-type: none"> ▪ MATCHES: Compares the card holder authentication method with the String to compare. Only exact matches are allowed.
IMPS_MODE	<p>If your rule needs to track the transaction based on the IMPS mode.</p> <p>IMPS_MODE is a 2-digit value depicting the IMPS transaction type. Possible values are:</p> <ul style="list-style-type: none"> ▪ 45: Person to Person (P2P) ▪ 46: Merchant to Person (M2P) ▪ 47: Person to Merchant (P2M) ▪ 48: Person to Account (P2A) 	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the IMPS mode is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the IMPS mode in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the IMPS mode with the String to compare. Only exact matches are allowed.
ORIGINATING_CHANNEL	<p>If your rule needs to track the channel from which the transaction originated.</p> <p>This is a 3-character value depicting the channel from where the transaction originated. Possible values are:</p> <ul style="list-style-type: none"> ▪ SMS ▪ IVR ▪ POS 	<ul style="list-style-type: none"> ▪ IN_LIST: Checks whether the originating channel is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. ▪ IN_CATEGORY: Checks for the originating channel in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ▪ MATCHES: Compares the originating channel with the String to compare. Only exact matches are allowed.

REMITTER_MOBILE

If your rule needs to track the transaction based on the mobile number of the Remitter.

- **IN_LIST:** Checks whether the Remitter mobile number is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the **Show List** link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.
 - **IN_CATEGORY:** Checks for the Remitter mobile number in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
 - **MATCHES:** Compares the Remitter mobile number with the **String to compare**. Only exact matches are allowed.
-

Transaction Elements for ECOM Channel

The following table describes the transaction element specific to the **Ecommerce (ECOM) channel**. This channel pertains to all financial (eCommerce) transactions that use the ISO 8583 standard.

Data Element	When to Use	Operator Description
ECI_INDICATOR	<p>If your rule needs to track the transaction based on the ECI indicator.</p> <p>ECI indicator is a 2-digit value representing how the eCommerce transaction was authenticated. Possible values are:</p> <ul style="list-style-type: none">▪ 05: Secure eCommerce with 3D▪ 06: Not authenticated. Merchant attempted to authenticate using 3D secure▪ 07: Non-secure transactions with data encrypted.▪ 08: Non-secure transaction	<ul style="list-style-type: none">▪ IN_LIST: Checks whether the ECI indicator is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page.▪ IN_CATEGORY: Checks for the ECI indicator in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
	<ul style="list-style-type: none"> 15: Secure eCommerce transaction registration required with OTP 	<ul style="list-style-type: none"> MATCHES: Compares the ECI indicator with the String to compare. Only exact matches are allowed.
	<ul style="list-style-type: none"> 16: Secure eCommerce transaction registration required with Internet banking 17: Secure eCommerce transaction registration required with other method 21: Secure eCommerce transaction with valid Image select 22: Non-secure eCommerce transaction with invalid Image select and one day lock 23: Non-secure eCommerce transaction with invalid Image select and permanent lock 24: Non-secure eCommerce transaction with browser close and one day lock 25: Non-secure eCommerce transaction with browser close and permanent lock 	

Device Elements

During an online transaction, the incoming data also includes elements to identify the device (desktop, laptop, smartphone, or tablet) used by the end user. Everytime a user performs a transaction, RA uses this device information to identify if the incoming request is genuine or fraud. This article walks you through the device elements that can be used for building your custom rule.

Device Elements (Applicable to All Channels)

The following table describes the Device elements and the corresponding operators.

Data Element	When to Use	Operator Description
BROWSER	If your rule needs to check the browser from which the transaction originated.	IN_LIST: Checks whether the browser name is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more

Data Element	When to Use	Operator Description
		<p>than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>IN_CATEGORY: Checks for the browser name in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the browser name with the String to compare. Only exact matches are allowed.</p> <p>Note: Supported browsers are Mobile Safari, Android Webkit, Microsoft Internet Explorer, Firefox, Epiphany, K-Meleon, Konqueror, Minimo, Mozilla, SeaMonkey, Netscape, NetPositive, Novarra, OmniWeb, Opera, Safari, Camino, Shiira, Lynx, w3m, Chrome, CrMo, CriOS, Avant Browser, PSP, ELinks, Links, and OffByOne.</p>
DEVICEID	If your rule needs to identify suspicious transaction patterns based on the ID of the device involved in the transaction.	<p>VELOCITY: Checks whether the number of transactions performed by one or more users from a specific device exceeds the limits set by the duration and frequency.</p> <p>IN_LIST: Checks whether the Device ID is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>IN_CATEGORY: Checks for the Device ID in a table in the mapping data set, and then compares the associated</p>

Data Element	When to Use	Operator Description
		<p>derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the Device ID with the String to compare. Only exact matches are allowed.</p> <p>VELOCITY_DISTINCT_USER: Counts the number of <i>n</i> distinct users who have done a transaction in the configured duration from the specific device. For more information, see "Creating the Device User Velocity Rule".</p>
DEVICETYPE	If your rule needs to check for the type of device involved in the transaction.	<p>IN_LIST: Checks whether the device type is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>IN_CATEGORY: Checks for the device type in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the device type with the String to compare. Only exact matches are allowed.</p> <p>Note: Supported device types are PC, Mac, iPad, iPhone, Kindle, Android, Linux, BlackBerry, Nokia, iPod, PlayBook, Web OS, HP Tablet, Sony, PlayStation, and Nintendo Wii.</p>
MFPMATCHPERCENT	If your rule needs to check for the Machine FingerPrint match.	Checks if the match percentage between the input device signature and the

Data Element	When to Use	Operator Description
		<p>corresponding stored device signature is GREATER_OR_EQUAL to the following thresholds:</p> <p>Signature Match Threshold: Threshold against which match percentage is checked in cases where the transaction has a valid Device ID and the input signature is matched against the signature of the previous transaction.</p> <p>Reverse Lookup Threshold: Threshold against which match percentage is checked in cases where the Device ID is obtained by matching the input device signature against the device signatures that were successfully associated with the user.</p>
OS	If your rule needs to check for the operating system used by the device involved in the transaction.	<p>IN_LIST: Checks whether the operating system is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>IN_CATEGORY: Checks for the operating system value in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the operating system with the String to compare. Only exact matches are allowed.</p> <p>Note: Supported OSs are Windows 98, Windows 95, Windows NT 4.0, Windows NT 3.51, Windows NT, Windows CE, Windows, PPC Mac OS X Mach-O, PPC Mac OS X, Intel</p>

Data Element	When to Use	Operator Description
		Mac OS X, PPC Mac OS, Intel Mac OS, Mac OS, Macintosh, Linux, FreeBSD, NetBSD, OpenBSD, Debian, Gentoo, Red Hat Linux, SUSE, CentOS, Fedora, Mandriva, PCLinuxOS, Ubuntu, OS/2, SunOS, PalmOS, Symbian, Darwin, J2ME/MIDP, PSP, iOS, and Android.

Geolocation Elements

During an online transaction, the incoming data also includes elements to identify the location of the device used by the end user. RA uses this location information to preliminarily identify if the incoming request might be genuine or fraud and also uses this information to build strong user behavior profile.

This article walks you through the geolocation elements that can be used for building your custom rule:

- [Geolocation Elements \(Applicable to All Channels\)](#)
- [Geolocation Elements for PINCode-Based Zone Hopping for POS Channels](#)

Geolocation Elements (Applicable to All Channels)

The following table describes the Geolocation elements and the corresponding operators.

Data Element	When to Use	Operator Description
CITY	If your rule needs to check for the city from which the transaction originated.	<p>IN_LIST: Checks whether the city of origin is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the city of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the city of origin with the String to compare. Only exact matches are allowed.</p>

Data Element	When to Use	Operator Description
		<p>You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p>
CLIENTIPADDRESS	If your rule needs to check for the client IP address used to perform the transaction.	<p>IN_TRUSTED_LIST: Checks whether the IP address of the client is in a pre-defined list of trusted IP addresses.</p> <p>IN_LIST: Checks whether the IP address is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>VELOCITY: Checks whether the number of transactions from this IP address exceeds the limits set by the duration and frequency.</p> <p>IN_NEGATIVE_LIST: Checks for anonymizing proxies.</p> <p>IN_CATEGORY: Checks for the IP address in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p>
CONNECTIONTYPE	If your rule needs to check the type of connection used to perform the transaction. CONNECTIONTYPE indicates the type of connection to the Internet provider.	<p>IN_LIST: Checks whether the CONNECTIONTYPE is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p>

Data Element	When to Use	Operator Description
		<p>IN_CATEGORY: Checks for CONNECTIONTYPE in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the CONNECTIONTYPE with the String to compare. Only exact matches are allowed.</p> <p>For a list of possible values, see "Connection Type".</p>
CONTINENT	If your rule needs to check for the continent from which the transaction originated.	<p>IN_LIST: Checks whether the continent from which the transaction originated is in a simple look-up list. Exact and partial matches are allowed. RA derives the country information based on the input IP address. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the continent from which the transaction originated in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the continent with the String to compare. Only exact matches are allowed.</p> <p>You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data. For a list of continents, see "Continent".</p>
COUNTRY	If your rule needs to check for the country from which the transaction originated.	IN_NEGATIVE_LIST: Checks whether the country of origin is in a pre-defined list of "negative" countries.

Data Element	When to Use	Operator Description
		<p>IN_LIST: Checks whether the country of origin is in a simple look-up list. Exact and partial matches are allowed. RA derives the country information based on the input IP address. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the country of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the country of origin with the String to compare. Only exact matches are allowed.</p> <p>You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p>
IP_ROUTINGTYPE	<p>If your rule needs to check for the IP routing type of the connection used to perform the transaction.</p> <p>IP_ROUTINGTYPE is an attribute of the IP address that helps assess the accuracy of the location.</p>	<p>IN_LIST: Checks whether the IP_ROUTINGTYPE is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>IN_CATEGORY: Checks for IP_ROUTINGTYPE in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p>

Data Element	When to Use	Operator Description
		<p>MATCHES: Compares the IPROUTINGTYPE with the String to compare. Only exact matches are allowed.</p> <p>For a list of possible values, see "IP Routing Type".</p>
LINESPEED	If your rule needs to check for the speed of the user's internet connection used to perform the transaction.	<p>IN_LIST: Checks whether the LINESPEED is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>IN_CATEGORY: Checks for LINESPEED in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the LINESPEED with the String to compare. Only exact matches are allowed.</p> <p>For a list of possible values, see "Line Speed".</p>
REGION	If your rule needs to check for the region from which the transaction originated.	<p>IN_LIST: Checks whether the region of origin is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the region of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p>

Data Element	When to Use	Operator Description
		<p>MATCHES: Compares the region of origin with the String to compare. Only exact matches are allowed.</p> <p>You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p> <p>For a list of possible values, see "Region".</p>
STATE	If your rule needs to check for the state from which the transaction originated.	<p>IN_LIST: Checks whether the state of origin is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the state of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the state of origin with the String to compare. Only exact matches are allowed.</p> <p>You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p>

Geolocation Elements for PINCode-Based Zone Hopping for POS Channels

The following table describes the Geolocation elements and the corresponding operators.

Data Element	When to Use	Operator Description
CITY	If your rule needs to check for the city from which the transaction originated.	IN_LIST: Checks whether the city of origin is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can

Data Element	When to Use	Operator Description
		<p>use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the city of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the city of origin with the String to compare. Only exact matches are allowed.</p> <p>You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data.</p>
COUNTRY	If your rule needs to check for the country from which the transaction originated.	<p>IN_NEGATIVE_LIST: Checks whether the country of origin is in a pre-defined list of "negative" countries.</p> <p>IN_LIST: Checks whether the country of origin is in a simple look-up list. Exact and partial matches are allowed. RA derives the country information based on the input IP address. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.</p> <p>IN_CATEGORY: Checks for the country of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.</p> <p>MATCHES: Compares the country of origin with the String to compare. Only exact matches are allowed.</p> <p>You can upload data to the data list and manage category mappings in the Manage List</p>

Data Element	When to Use	Operator Description
STATE	If your rule needs to check for the state from which the transaction originated.	Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data .
		IN_LIST: Checks whether the state of origin is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself.
		IN_CATEGORY: Checks for the state of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
		MATCHES: Compares the state of origin with the String to compare . Only exact matches are allowed.
LONGITUDE	If your rule needs to check for the east-west position on earth's surface from which the transaction originated.	You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data .
		IN_TRUSTED_LIST: Checks whether the IP address of the client is in a pre-defined list of trusted IP addresses.
		IN_LIST: Checks whether the IP address is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data .
LATITUDE	If your rule needs to check for the north-south position on earth's surface from which the transaction originated.	VELOCITY: Checks whether the number of transactions from this IP address exceeds the limits set by the duration and frequency.

Data Element	When to Use	Operator Description
		IN_NEGATIVE_LIST: Checks for anonymizing proxies.
		IN_CATEGORY: Checks for the IP address in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

You can use the geolocation information in the following rules:

- Zone Hopping
- Negative Country
- Other rules that you create using city, state, or country as rule variables

Predictive Model Elements

RA offers an advanced fraud modeling capability called Predictive Model, which can be built using the historical data collected by RA. When deployed, the model generates a score that describes the extent to which the model suspects a transaction's genuineness. This score typically ranges from 0 through 100, where the higher the number, the greater the possibility of fraud. RA can be configured to send different responses to your calling application based on this model score.

If you have a Model deployed, you can use the Model element for building your custom rule that analyzes a transaction based on the Model score. This article walks you through the Model element that can be used for the purpose.

Model Elements (Applicable to All Channels)

The following table describes the Model element and the corresponding operators.

Data Element	When to Use	Operator Description
MODEL_SCORE or PREDICTIVE_SCORE	If your rule needs to check for the resulting score from the Predictive model evaluation	Compares the model score with the specified value using the following operators: - EQUAL_TO - NOT_EQUAL_TO - GREATER_THAN - LESS_THAN - GREATER_OR_EQUAL - LESS_OR_EQUAL

Data Element	When to Use	Operator Description
		- RANGE
		IN_LIST: Checks whether the model score is in a simple look-up list. Exact and partial matches are allowed. If your list has 10 or fewer items, you can use the Show List link to enter list items in the Rule Builder itself. For lists containing more than 10 items, use the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data .
		IN_CATEGORY: Checks for the model score in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Custom Elements

Custom element (**CUSTOM**) enables you to create your own data elements that are not available in the list of the data elements shipped out of the box.

The following table lists the rule tags that you can use for the CUSTOM element. The data in the table is classified into the following categories:

- **User:** Provides information about the user and the account.
- **Device:** Provides information about the device used to originate the transaction.
- **General Transaction:** Provides information about elements of every transaction, such as the channel and action.
- **Currency:** Provides information such as currency conversion rate and base currency.
- **Location:** These elements are derived from a maintained database of IP geolocation, which provides location data and connection attributes of the IP address.
- **Internal Parameters:** Support the construction of custom rule types.

Tag Name	Channel	Description
User Information		
IDENTITY.USERID	All	The user identifier. If encryption was enabled, then this tag represents the encrypted version of the user identifier.

Tag Name	Channel	Description
RULESET.GROUPNAME	All	The organization name.
Device Information		
DEVICEID.http	Default, 3D Secure	The alpha-numeric ID assigned by RA for this device.
DEVICEID.flash	Default, 3D Secure	The Flash device ID string specific to the transaction.
DEVICESIG	Default, 3D Secure	The device signature gathered from the end user's system to generate a risk profile of a device in real time.
SHORTDEVICESIG	Default, 3D Secure	The compact form of the device signature.
AGGREGATORINFO	Default, 3D Secure	Aggregator ID string specific to the transaction.
RULE.SIGPASSTHRESHOLD	Default, 3D Secure	Pass threshold used by the Device MFP Match rule.
General Transaction Information		
RULESET.CHANNELNAME	All	The channel using which the user accesses the system.
TRANSACTION.TXNID	All	The numeric identifier for this transaction generated by RA.
TRANSACTION.EXT	Default, 3D Secure	Name-value Extensible element string sent by the client.
Currency Information		
BASE_CURR_CODE	3D Secure, ATM, POS	Numeric designation corresponding to the 3-letter designation of the base currency of the organization.
BASE_CURR_AMOUNT	3D Secure, ATM, POS	Transaction amount converted to the Base Currency.
BASE_CONVERSION_RATE	3D Secure, ATM, POS	Conversion rate from transaction currency to the base currency of the organization.
Location Information		
RULESET.COUNTRYISO	Default, 3D Secure	Contains the two letter ISO 3166 alpha country code of the country, for example AU.
RULESET.STARTIP	Default, 3D Secure	Starting IP for the user IP block.
RULESET.ENDIP	Default, 3D Secure	Ending IP for the user IP block.
RULESET.GEOLAT	Default, 3D Secure	Latitude is expressed as a floating point number with positive numbers representing North and negative numbers representing South.
RULESET.GEOLONG	Default, 3D Secure	

Tag Name	Channel	Description
		Longitude is expressed as a floating point number with positive numbers representing East and negative numbers representing West.
RULESET.GEOCF	Default, 3D Secure	Confidence Factor (CF) in the geolocation. Confidence Factors are calculated based on the precision, completeness, and consistency of the data available to assign a specific geographic location to an IP address range. Confidence Factors are provided for Country, State, and City. Their value ranges from 1 to 99. A higher value indicates that the likelihood of a correct location assignment is higher; a lower value indicates the opposite. These values are not percentages. Their intended use is as a relative measure of "confidence" on the correctness of the corresponding location assignment.
Internal Parameters		
RULE.USERCONTEXT	Default, 3D Secure	User context information used internally by the rules engine to store state information.
RULE.DEVICECONTEXT	Default, 3D Secure	Device context information used internally by the rules engine to store state information.
ADDONRULE.DESCRRESULT	All	The concatenated string of results from the add-on rules called till this point.
ADDONRULE.ANNOTATION	All	The concatenated strings of annotations set by all add-on rules called till this point.
RULE.RULEMNEMONIC	All	Rule mnemonic configured for the rule.

History Rule Elements for ATM and POS

In RA, *Transaction History* is defined as the list of transactions for the same account (Card Number or PAN) over ATM and POS channels in reverse chronological sequence. The transaction history available is restricted to the maximum history duration (Duration to Look Back) set at the global level. Operators that leverage the Transaction History are referred to as *history-based operators*.

Note the following restrictions when you use these history-based operators:

- History-based rule fragments can be combined with other rule fragments using AND and OR operators, along with the NOT operator. However, the use of parenthesis is not permitted.
- History-based rule fragments cannot be combined with Saved Rules.
- Multiple history-based rule fragments cannot be combined into a single rule.
- History-based rule fragments cannot be combined with operators that maintain their own private history, such as ZONE_HOP, VELOCITY (USERNAME), and VELOCITY (ACTION).
- History-based rules can be used as Saved Rules to create other rules.

The following subsections list the history elements that you can use, criteria to identify different types of transactions using these elements, and a list of available transaction types and their corresponding actions.

History Rule Elements

The following default rule elements are available for use within the history rules for ATM and POS channels:

- ACCEPTOR_COUNTRY
- ACCEPTOR_ID
- ACCEPTOR_TERMID
- ACQ_BIN
- ACTION
- ACTION_CODE
- ADVICEID
- ALERT_STATUS
- AMOUNT
- BASE_CURR_AMOUNT
- BASE_CURR_CODE
- CHANNELNAME
- CITY
- CLIENTLAT
- CLIENTLONG
- COUNTRY
- CURR_CODE

- CURRENCY_CODE
- CURRENCY_CODE_TXN
- DATETIME_LOCAL_TXN
- DATETIME_LOCAL_TXN
- DATETIME_TRANSMISSION
- DATETIME_TRANSMISSION
- INSTANCEID
- LOCAL_DATE
- LOCAL_TIME
- MATCHEDRULE
- MERCH_CAT
- PROCESSING_CODE
- REVERSAL_STATUS
- SCORE
- STAN
- TXID
- TXN_ACTION_CODE
- TXNSTATUS
- TXNTYPE

Criteria to Identify Transactions

The following code samples describe the criteria used to identify repeat, reversal, and advice transactions.

Repeat Transactions

The criteria to identify Repeat transactions is as follows:

```
Repeat.STAN = Original.STAN AND Repeat.DATETIME_TRANSMISSION =
Original.DATETIME_TRANSMISSION
```

Reversal Transactions

The criteria to identify the original transaction for Reversals is as follows:

```
DE90::ORG_STAN = STAN AND DE90::ORG_DATETIME_TRANSMISSION = DATETIME_TRANSMISSION
```

Advice Transactions

The criteria to identify the original transaction for Advice transactions is as follows:

PostEval.STAN = Original.STAN AND PostEval.DATETIME_TRANSMISSION = Original.DATETIME_TRANSMISSION

Transaction Types and Actions for ATM and POS Channels

The following table describes the mapping between a Transaction Type and Action for ATM and POS channels.

DE3:Processing Code	Action
00	PURCHASE
01	WITHDRAWAL
31	FINANCIALINQUIRY
34	FINANCIALINQUIRY
70	PINCHANGE

Understanding the Types of Operators Used by the Rule Builder

To build a new rule by using the RA Rule Bulder, you need **Data Elements** (see [Quick Overview of Data Elements](#)) and different types of **Operators**. This article quickly lists the different types of Operators that you can use to build your custom rules. It also briefly touches on the different types of Data Elements with which these operators are used.

Note: For detailed information on Data Elements that can be used in each channel and the the operators that are allowed with them, see [Understanding Data Elements](#).

Based on their usage, operators in RA can be divided in the following categories:

- [Generic Operators](#)
- [Operators Specific to ATM and POS Channels](#)
- [History-Based Operators](#)

Generic Operators

Operators that you will use to manipulate these Data Elements to create rules can be grouped into the following major categories:

- **Expression Operators**
These operators are used to combine rule fragments to build a rule. Possible operators include:
 - AND
 - OR

- NOT
- **Match Type Operators**
These operators specify what type of match will be performed for the **IN_CATEGORY** and **IN_LIST** operators. Possible operators include:
 - EXACT
If the list value matches the input value exactly, then the rule is triggered. This match is case-sensitive.
 - PARTIAL
If any of the values in the list is a partial substring of the input value, then the rule is triggered. This match is case-sensitive.

For example, a list with values 40001, 50001, and 60001 triggers the rule for PARTIAL match with an input value of 40001000100010001. Similarly, a list with values Alice, Cathy, and Karen trigger the rule for PARTIAL match with an input value of "Karenina" and for EXACT match with an input value of "Karen".

- **LookUp Type Operators**
These operators match specified values in a list. Possible operators include:
 - IN_LIST
 - IN_TRUSTED_LIST
 - IN_NEGATIVE_LIST
- **Relational Operators**
These operators are used for numeric comparison of data elements. Possible operators include:
 - RANGE,
 - EQUAL_TO (=)
 - NOT_EQUAL_TO (!=)
 - GREATER_OR_EQUAL (>=)
 - LESS_OR_EQUAL (<=)
 - GREATER_THAN (>)
 - LESS_THAN (<)

Operators Specific to ATM and POS Channels

These operators include:

- EQUAL_TO_CB
- NOT_EQUAL_TO_CB
- GREATER_OR_EQUAL_CB

- LESS_OR_EQUAL_CB
- GREATER_THAN_CB
- LESS_THAN_CB

In the preceding list, **CB** indicates **Card BIN**.

History-Based Operators

Transaction History is defined as the list of transactions for the same account (**Card Number** or **PAN**) over ATM and POS channels in reverse chronological sequence. Operators that leverage this Transaction History are referred to as **History-Based Operators**.

The available transaction history is restricted to the maximum history duration (**Duration to Look Back**), set at the global level.

Restrictions While Using History-Based Operators

Note the following restrictions when you use history-based operators:

- History-based rule fragments can be combined with other rule fragments using AND and OR operators, along with the NOT operator. However, the use of parenthesis is *not* permitted.
- History-based rules can be used as Saved Rules to create other rules.
- History-based rule fragments *cannot* be combined with Saved Rules.
- Multiple history-based rule fragments *cannot* be combined into a single rule.
- History-based rule fragments *cannot* be combined with operators that maintain their own private history. These operators include ZONE_HOP, VELOCITY (USERNAME), and VELOCITY (ACTION).

The following table describes the history-based operators supported by the current release of RA.

Operator	Description
CUMULATIVE_AMOUNT	<p>Fetches the transaction history and provides a cumulative total of the amount (in the organization's base currency) for transactions within the specified Duration to Look Back restricted to Maximum Transactions to Look Back. The rule is triggered if the calculated cumulative amount is greater than the configured Threshold Cumulative Amount.</p> <p>The fields that you can configure for the CUMULATIVE_AMOUNT operator are:</p> <ul style="list-style-type: none"> ▪ Threshold Cumulative Amount: Threshold amount (in the organization's base currency) that would trigger the rule. If you set this value to -1, it would be ignored.

Operator	Description
	<ul style="list-style-type: none"> ▪ Threshold Transaction Count: The number of transactions, exceeding which the rule will be triggered. ▪ Duration to Look Back: Maximum time period (in minutes) to consider for transaction history. ▪ Maximum Transactions to Look Back: Maximum number of transactions to consider for transaction history. ▪ Transactions to Consider: The type of transactions that you want to consider. Possible values are All, Approved, or Denied. ▪ Additional Filter: An optional custom history filter allows for additional filtering of the history data with the specified filter. The filter options available are: Reversed Transactions (REVERSAL_STATUS EQ 1), Issuer Approved Transactions (TXN_ACTION_CODE EQ 00), and Issuer Declined Transactions (TXN_ACTION_CODE NEQ 00). This additional history filter is not applicable to the current transaction and is applied to the history data fetched based on the normal history criteria prior to the actual data tabulation for rule triggering. <p>For an example of how this operator works, see “Transactions Exceeding Thresholds” in Example s of Using New Rules.</p>
GROUPED_CUMULATIVE_AMOUNT	<p>Fetches the transaction history and provides a cumulative total of the amount (in the organization's base currency), for the transactions whose transaction time is within the specified time frame (Time Frame Start Time and Time Frame End Time), grouped in time units of the specified duration (Amount Grouping Duration) and within the specified Duration to Look Back restricted to Maximum Transactions to Look Back. The rule is triggered if the calculated amount is greater than the configured Threshold Cumulative Amount for at least the configured Minimum Threshold Breach Count.</p> <p>The fields that you can configure for the GROUPED_CUMULATIVE_AMOUNT operator are:</p> <ul style="list-style-type: none"> ▪ Threshold Cumulative Amount: Threshold amount (in the organization's base currency) that would trigger the rule. If you set this value to -1, it would be ignored.

Operator	Description
	<ul style="list-style-type: none"> ▪ Grouping Period Count: The number of periods to group to perform the amount totaling. ▪ Minimum Threshold Breach Count: Number of grouping periods when the amount total exceeds the configured Threshold Cumulative Amount for triggering the rule. This threshold must not be greater than Grouping Period Count. ▪ Duration to Look Back: Maximum time period (in minutes) to consider for transaction history. ▪ Maximum Transactions to Look Back: Maximum number of transactions to consider for transaction history. ▪ Time Frame Start Time (HHMM): Start time of the day for the grouping period. ▪ Time Frame End Time (HHMM): End time of the day for the grouping period. ▪ Transactions to Consider: The type of transactions that you want to consider. Possible values are All, Approved, or Denied. ▪ Additional Filter: An optional custom history filter allows for additional filtering of the history data with the specified filter. The filter options available are: Reversed Transactions (REVERSAL_STATUS EQ 1), Issuer Approved Transactions (TXN_ACTION_CODE EQ 00), and Issuer Declined Transactions (TXN_ACTION_CODE NEQ 00). This additional history filter is not applicable to the current transaction and is applied to the history data fetched based on the normal history criteria prior to the actual data tabulation for rule triggering. <p>For an example of how this operator works, see “Daily Maximum Amount Check” in Examples of Using New Rules.</p>
ACTION_CUMULATIVE_AMOUNT	<p>Fetches the transaction history after the last occurrence of the specified action and provides a cumulative total of the amount (in the organization’s base currency) for transactions within the specified Duration to Look Back restricted to Maximum Transactions to Look Back. The rule is triggered if the calculated cumulative amount is greater than the configured Threshold Cumulative Amount or the number of transactions is greater than the Threshold Transaction Count. However, if the specified action did not occur within the duration, history is deemed to be zero.</p>

Operator	Description
	<p>The fields that you can configure for the ACTION_CUMULATIVE_ACCOUNT operator are:</p> <ul style="list-style-type: none"> ▪ Threshold Cumulative Amount: Threshold amount (in the organization's base currency) that would trigger the rule. If you set this value to -1, it would be ignored. ▪ Threshold Transaction Count: The number of transactions, exceeding which the rule will be triggered. If you set this value to -1, it would be ignored ▪ Duration to Look Back: Maximum time period (in minutes) to consider for transaction history. ▪ Maximum Transactions to Look Back: Maximum number of transactions to consider for transaction history. ▪ Transactions to consider: The type of transactions that you want to consider. Possible values are All, Approved, or Denied. ▪ Threshold Action: The action, after the last occurrence of which the transaction history is fetched. Possible values are PINCHANGE and FINANCIALINQUIRY. ▪ Additional Filter: An optional custom history filter allows for additional filtering of the history data with the specified filter. The filter options available are: Reversed Transactions (REVERSAL_STATUS EQ 1), Issuer Approved Transactions (TXN_ACTION_CODE EQ 00), and Issuer Declined Transactions (TXN_ACTION_CODE NEQ 00). This additional history filter is not applicable to the current transaction and is applied to the history data fetched based on the normal history criteria prior to the actual data tabulation for rule triggering. <p>For an example of how this operator works, see "Transactions Exceeding Thresholds for a Specified Action" in Examples of Using New Rules.</p>

Using Geolocation and Anonymizer Data in Rules

RA uses geolocation and IP verification to detect high-risk activities. These capabilities use the IP address of end users to:

- Verify that they are not accessing from a country or region that you have blacklisted.
- Verify that they are not moving faster than is actually possible.

- Verify that they are not hiding their location.
- Verify that they are not coming from an IP address that you have blacklisted.

Based on one of these checks, you can decide on the mitigating action that you want to take. This action can range from alerting your fraud or security team of possible compromise, requiring additional authentication from the end user, or denying access for the session.

This article discusses the use of IP geolocation data and Negative IP checks in RA. Together, these two capabilities together provide one of the major components of RA fraud and high risk detection. They support the following checks as a part of the RA out-of-the-box rule settings:

- Geolocation (Negative Country List)
- End user change in access location (Zone hopping)
- Anonymizer data (Negative IP Types)
- Administrator-defined negative IPs (Negative IP Address List)

This article covers the following topics:

- [What Is Geolocation Data](#)
- [How to Use Geolocation Data in Rules](#)
- [Using Anonymizer Data](#)
- [How to Use the Negative IP Address List](#)

What Is Geolocation Data

Neustar IP Intelligence, an industry leader in geolocation information, provide CA Risk Analytics the following types of data as a result of collaboration between the two organizations:

- **Geolocation data.**
This data classifies each IP address by latitude, longitude, continent, country, and city. By default, this data is used in the Negative Country Check rule and for calculating the distances in case of the Zone Hopping Check rule. You can also use this data for any custom rules that you create by using the Rule Builder.
The Country and City elements are both useful for checks on the point of access.
- **Connection information.**
Each IP address is classified by routing type, connection type, and line speed. This information, especially routing type, is useful in assessing the validity of the geolocation information. For example, if the connection type is Satellite, then the user's location is not reliable
In practice, you can ignore this information for geolocation purposes. However, fixed connection types, such as cable, DSL, and OCX are less likely to be origins of fraud. This is because their locations are more easily backtracked to Internet accounts.
You can use this data to evaluate fraud.

- **Anonymizer data.**
Neustar IP Intelligence perform rigorous testing of IP addresses to determine if their location information is reliable. As a part of this testing, they identify some IP addresses as **Anonymizers**.
- IP addresses with this status have tested positive as anonymous proxies that are used to hide the true location of an end user. While this does not necessarily indicate that the intent is fraudulent, it does clearly indicate that the user is hiding their location, and therefore represents a high risk access potential.

How to Use Geolocation Data in Rules

This topic describes the following:

- The geolocation information that is used in the following RA rules:
 - [Negative Country Check](#)
 - [Zone Hopping Check](#)
- The geolocation data that Neustar IP Intelligence provides for each routable IP address.
 - [IP Routing Type](#)
 - [Connection Type](#)
 - [Line Speed](#)
 - [Region](#)
 - [Continent](#)

Negative Country Check

You use the **Manage List Data** and **Category Mappings** pages in the Administration Console to configure the **Negative Country List**. You do so by adding to or removing countries to the list that you consider high risk.

Typically, you will define this to be a list of countries from where any access attempt is *always* verified by using some form of Increased Authentication. You can also use this as a Deny rule and list a small set of countries in the Negative Country List.

For financial transactions, you can combine the Negative Country Check rule with an Amount-based rule to reduce the number of cases marked for further investigation.

For general access control, the rule is defined as an Increase Authentication risk advice to trigger a more stringent login process. In these situations, cases are not created.

Zone Hopping Check

The location latitude and longitude are the most important information used in the **Zone Hopping Check** rule. This rule verifies the time and speed required for physically travelling between the points of origin of two successive transactions using the IP addresses that were used.

If two successive transactions are originating at a speed beyond what is reasonably possible within a short time span, then you must conclude that either two different people were accessing the same account from different locations or the user did something, either intentionally or inadvertently, to mask their true location. As a result, you can use this as a Deny rule.

It is highly recommended that you start by setting the values of the Zone Hopping Check rule to the default values provided. Based on the performance of this rule over time, you can tune the settings of this rule to make them more precise.

In its default settings, you should expect the rule to fire about 0.02% of the time. The false-positive rate for this rule is good at under 10:1.

IP Routing Type

IP Routing Type is an attribute of the IP addresses, and determines the likelihood that the user's location matches the location of the IP address. The following table describes the possible values that you can use for IP Routing Type.

IP Routing Type	Indication
Fixed	User IP is at the same location as the user.
Anonymizer	User IP is located within a network block that has tested positive for anonymizer activity. This means the user is potentially hiding their true location by using a service that deliberately proxies all user traffic.
AOL: AOL POP AOL Dialup AOL Proxy	User is a member of the AOL service; Neustar IP Intelligence can identify the user country in most cases; any regional info more granular than country is not possible. Please note that in GeoPoint AOL IPs are denoted by a simple Y/N (Yes/No).
POP	User is dialing into a regional ISP and is likely to be near the IP location; the user could be dialing across geographical boundaries.
Superpop	User is dialing into a multi-state or multi-national ISP and is not likely to be near the IP location; the user could be dialing across geographical boundaries.
Satellite	A user connecting to the Internet through a consumer satellite or a user connecting to the Internet with a backbone satellite provider where no information about the terrestrial connection is available. In both cases, the user can be anywhere within the beam pattern of the satellite, which typically spans a continent or more.
Cache Proxy	User is proxied through either an Internet accelerator or content distribution service; user could be in any location.
International Proxy	A proxy that contains traffic from multiple countries.

IP Routing Type	Indication
Regional Proxy	A Proxy (not Anonymizer) That Contains Traffic From Multiple States Within A Single Country.
Mobile Gateway	A Gateway To Connect Mobile Devices To The Public Internet. For Example, Wap Is A Gateway Used By Mobile Phone Providers.
Unknown	Routing method is not known or is not identifiable in the above descriptions.

Connection Type

Connection Type indicates the data connection between a device or private LAN to the public Internet provider. The following table describes the possible values that you can use for Connection Type.

Connection Type	Description
OCX	This represents OC-3 circuits, OC-48 circuits, etc. which are used primarily by large backbone carriers.
TX	This includes T-3 circuits and T-1 circuits still used by many small and medium companies.
Satellite	This Represents High-speed Or Broadband Links Between A Consumer And A Geosynchronous Or Low Earth Orbiting Satellite.
Framerelay	Frame Relay Circuits May Range From Low To High Speed And Are Used As A Backup Or Alternative To T-1. Most Often They Are High-speed Links, So Geopoint Classifies Them As Such.
DSL	Digital Subscriber Line Broadband Circuits, Which Include Adsl, Idsl, And Sdsl. In General, Ranges In Speed From 256k To 20mb Per Second.
Cable	Cable Modem broadband circuits, offered by cable TV companies. Speeds range from 128k to 36MB per second, and vary with the load placed on a given cable modem switch.
ISDN	Integrated Services Digital Network high-speed copper-wire technology, support 128K per second speed, with ISDN modems and switches offering 1MB per second and greater speed.
Dialup	This Category Represents The Consumer Dialup Modem Space, Which Operates At 56k Per Second. Providers Include Earthlink, AOL, And Netzero.
Fixed Wireless	Represents Fixed Wireless Connections Where The Location Of The Receiver Is Fixed. Category Includes Wdsl Providers, Such As Sprint Broadband Direct, As Well As Emerging Wimax Providers.

Connection Type	Description
Mobile Wireless	Represents Cellular Network Providers Such As Cingular, Sprint, And Verizon Wireless Who Employ Cdma, Edge, Ev-do Technologies. Speeds Vary From 19.2k Per Second To 3mb Per Second.
Unknown	GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the above descriptions.

Line Speed

This parameter indicates the speed of the Connection Type between the device (or a private LAN) and the public Internet provider. The following table describes the possible values that you can use for Line Speed for each of the Connection Types.

Line Speed	Corresponding Connection Type
High	OCX, TX, And Framereley
Medium	Satellite, DSL, Cable, Fixed Wireless, And Isdn.
Low	Dialup And Mobile Wireless.
Unknown	Neustar IP Intelligence was unable to obtain any line speed information.

Region

For convenience, Neustar IP Intelligence have divided the U.S. into 10 geographical regions:

- Northeast
- Mid Atlantic
- Southeast
- Great Lakes
- Midwest
- South Central
- Mountain
- Northwest
- Pacific
- Southwest

A complete listing can be found under Reference Data, in the **Download** section of the Neustar IP Intelligence Extranet. Refer to these text files for the latest information.

Continent

Neustar IP Intelligence recognize eight continents:

- Africa
- Antarctica
- Asia
- Australia
- Europe
- North America
- Oceania (Melanesia, Micronesia, Polynesia)
- South America

Using Anonymizer Data

IP addresses can also be classified with an anonymizer status. You can control the types of anonymizer IPs that you include in a rule. The different categories of negative IP types, as derived from the Neustar data, are:

- **Negative**
IP addresses with this designation have been sources of fraudulent transactions in the past.
- **Active**
IP addresses with this designation allegedly are anonymizing proxies that have been sources of fraudulent transactions and have been active in the last six months.
- **Suspect**
IP addresses with this designation allegedly are anonymizing proxies that have been active over the last two years, but not for the last six months.
- **Private**
IP addresses with this designation allegedly are anonymizing proxies that are not publicly accessible. These addresses typically belong to commercial ventures that sell anonymity services to the public.
- **Inactive**
IP addresses with this designation allegedly have been sources of fraudulent transactions, but have been found inactive in the last two years.
- **Unknown**
IP addresses with this designation allegedly are anonymizing proxies for which no results are currently available.

You must either set your rule to the defaults listed or you must clear Suspect IPs.

While the use of an anonymizer does not necessarily indicate intent to commit a crime, it is highly suspicious because the user might be masking their location. For example, users may be participating in marginal activities, such as accessing gaming from a country where it is not allowed or accessing video or music content from a region that is not licensed.

The hit rate for this rule is highly variable by customer because it is influenced by the portfolio of end users. However, the approximate review rate based on Anonymizers is 0.1% (one in 1000 transactions). False-positive rates tend to vary greatly from as low as 20:1 for US and European users to as high as 100:1 for less developed regions.

How to Use the Negative IP Address List

The **Negative IP Check** rule performs two functions *within* a single rule:

- The rule checks for the IP addresses of end users against the list of known anonymizer proxies.
- The rule consults the Negative IP Address list that you define to verify whether the incoming IP address is in one of the ranges defined in your table.

You use the **Manage List Data** and **Category Mappings** page in the Administration Console to add IP Addresses to the Negative IP Address list.

The rule performance for blacklisted IP addresses depends on how you manage your list. Typically, you add IP addresses to the list when you see fraudulent or risky access that you want to stop and you remove IPs from the list when it is found to be originating from a legitimate user.

Note: You can review the transaction report to determine why an end user was blocked or challenged.

Understanding Currency Conversion

This article provides an overview of currency conversion and describes the schema of the **ARRFCURRCONVRATES** table. It includes the following topics:

- [How Currency Conversion Works](#)
- [Currency Conversion Table](#)

How Currency Conversion Works

See [How is Currency Conversion Used](#) to understand how RA performs currency conversion.

Currency Conversion Table

The conversion data for all supported currencies is stored in the **ARRFCURRCONVRATES** table. This table contains the currency conversion data that is used to compare Amount field values when the transaction currency and the base currency of the organization differ. The following table describes the columns in the table.

Column	Description	Format
VERSION	Rate Version	Integer with a value of 1.
CURR_FROM		Integer with values between 0 and 1000.

Column	Description	Format
	The 3-digit ISO currency code for the transaction currency from which Amount is converted.	
CURR_FROM_STR	The 3-character ISO currency code for the transaction currency from which Amount is converted.	String with exactly three characters.
CURR_TO	The 3-digit ISO currency code for the currency to which Amount is converted.	Integer with values between 0 and 1000.
CURR_TO_STR	The 3-character ISO currency code for the currency to which Amount is converted.	String with a maximum length of three characters.
CONV_RATE	The rate of conversion between CURR_FROM and CURR_TO or CURR_FROM_STR and CURR_TO_STR.	Real number.
DTCREATED	Date and time when the CONV_RATE value was created.	
CURR_NAME_AND_NOTES	Additional notes.	

Guidelines for Using the ARRFCURRCONVRATES Table

Apply the following guidelines when you use the ARRFCURRCONVRATES table:

- By default, there is no data in the ARRFCURRCONVRATES table. You must populate this table with values after deploying RA.
- The currency conversion rates should be specified as the conversion value for one unit of the specified CURR_FROM or CURR_FROM_STR and CURR_TO or CURR_TO_STR.
- The conversion rates in the ARRFCURRCONVRATES table should be loaded with the CURR_TO or CURR_TO_STR as USD only.
- If a particular currency conversion is required, for example from EUR to JPY, then the Amount would be first converted from EUR to USD using the conversion rate from EUR to USD, and then the reverse of the USD to JPY conversion rate would be applied to get the Amount in JPY.

Managing Cases

This article introduces you to the basics of the Case Management module and covers the following topics:

- [Understanding Case Management](#)
- [Working with Case Queues](#)
- [Searching for Cases](#)
- [Customer Support Representatives Handling Cases](#)
- [Fraud Analysts Analyzing Transactions](#)

Understanding Case Management

This topic discusses the basics of the Case Management feature and includes the following sub-topics:

- [What Is a Case](#)
- [What Are the Different States a Case can Undergo](#)
- [What Is Case Management](#)
- [What Are the Components of Case Management](#)
- [Supported Case Management Roles that You Will Use](#)
- [Summary of Case Management Role Privileges](#)
- [Supported Case Management Workflows](#)

What Is a Case

The following is a gist of managed cases in RA:

- All transactions (login, wire transfer, or any transaction that your application is evaluating risk for) for a user that result in the **Deny** or **Alert** advice in the RA system are considered a *case*. In other words, one case can comprise multiple suspicious transactions for a user.
- Every case provides information related to the user, transactions details, and case history. In other words, there is a strict 1:1 mapping between a user and open cases. As a result if a case is already open for the user, then a new suspicious transaction is added to the existing case. A new case is *not* created if a user already has a case open.
- At any time, a user can only have one open case in the system.

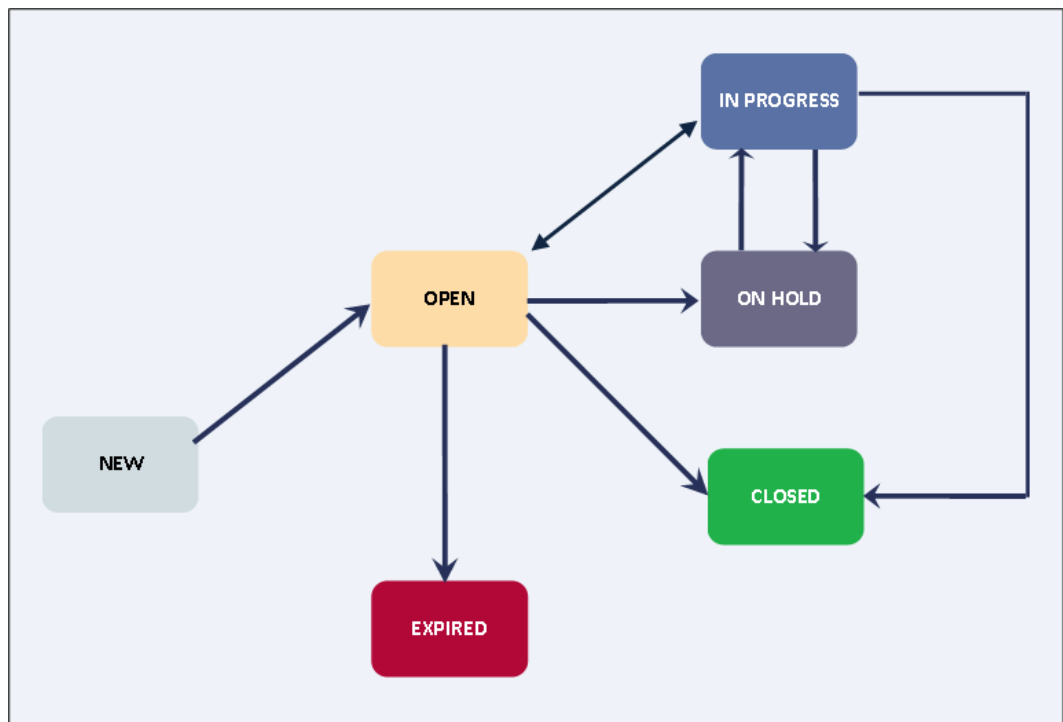
- At any time, a view into the case from Administration Console shows all the transactions within the case that have not been handled by an administrator and, therefore, their Fraud status is still undetermined.
- After a case is created in the system, it is recommended that a Customer Support Representative (CSR) handles all the transactions within a case and then close the case explicitly.
- If a case is closed, then any new warnings or suspect transactions for a given user result in the creation of a new case in the system. All new and future transactions are assigned to this new case.

What Are the Different States a Case can Undergo

During its lifecycle, a case can progress through the following states:

- New
- Open
- In Progress
- On Hold
- Expired
- Closed

The following figure illustrates how the states of a case change.



CAPMRA--15_c0004

New

When a user transaction results in **Alert** or **Deny** advice, then a new case is created for the user, if a corresponding case does not already exist.

The case remains in the **New** state until a CSR opens it or the case expires.

Open

When a CSR opens a new case assigned to them, the case is activated and its state changes to **Open**. When a case is in the **Open** state, new transactions or events can be added to the case.

Unless the case state is either **On Hold** or **Closed**, every case remains in the **Open** state.

In Progress

While a CSR is working on a case, the case state remains **In Progress**. In other words, when they click the **Cancel** button for the current case or click the **Go To Next Case** button to move to the next case assigned to them, the currently open case state changes to **Open**, or to the state that they explicitly changed the case to.

Note: A CSR and Queue Manager can change the status of a case from **On Hold** to **In Progress**.

On Hold

When a CSR postpones the further investigation of a case by specifying the **Next Action Date** for an **In Progress** case, the case state changes to **On Hold**.

Note: All events that are generated within the time frame of **Next Action Date** are appended to the case.

When the specified **Next Action Date** arrives, the case state automatically changes to **Open**.

Expired

When no CSR works on a **New** case within a pre-defined number of days, the case state changes to **Expired**.

Note: The time the last transaction was added to the case or was updated is considered as the *Starting Date* for the case. The case *Expiration Date* is calculated as the Starting Date + *N* days, where *N* is a configurable value. The default value for *N* is **10 days**.

New transactions cannot be added to an expired case. A new case (and therefore a new Case ID) is created, and the new transactions or events are added to this new case.

Closed

When a CSR resolves an **Open** case and explicitly marks it as **Closed**, the case state changes to **Closed**.

What Is Case Management

The *Case Management* feature of Risk Analytics provides your User Administrators (UAs) and Fraud Analysts (FAs) a single unified view of the data related to cases. This enables them to analyze the data more efficiently and take faster, better-informed decisions towards resolving the cases. In addition, analysts can also constantly track the status and progress of their cases and maintain complete case histories with instant access to all related information.

This feature enables you to:

- Efficiently manage customer service and support
- Manage large numbers of cases and investigations
- Create actions and tasks with due dates
- Assign actions with due dates
- Record investigation notes and the resolution provided to the user
- Handle cases and tasks more efficiently
- Keep clear audit trail or history of actions on a case
- Analyze trends
- Generate fraud-related reports

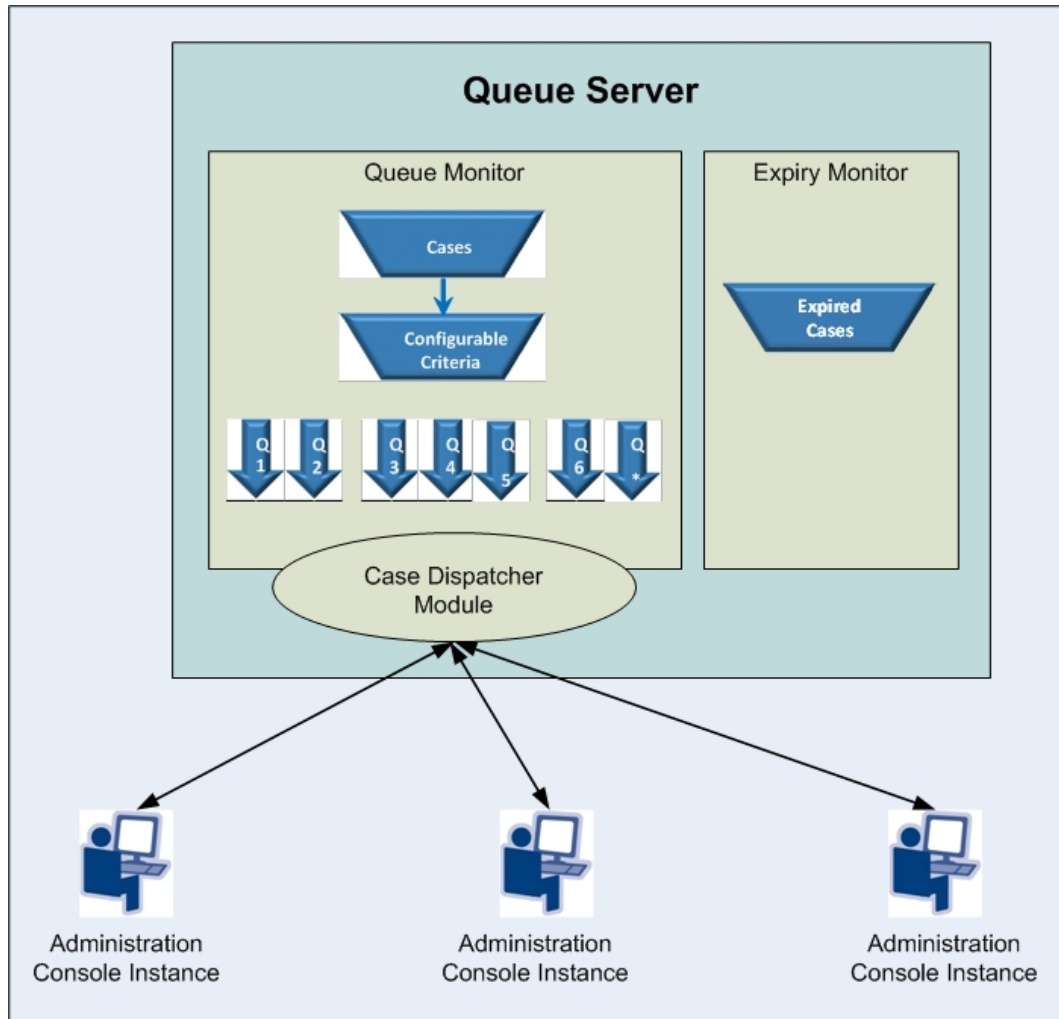
The Case Management feature enables you to investigate transactions, and intuitively and effectively manage the transactions that are marked suspicious. This feature simplifies the challenge of recording and documenting every phase of an investigation, creating a clear and comprehensive trail of activity. This feature also saves time by automatically creating a report of the findings, including a detailed listing of reason, recommendation, geolocation information, connection details, and risk assessment details.

What Are the Components of Case Management

The components of the Case Management module include:

- [Case Queues](#)
- [Queue Server](#)
- [Queue Monitor Thread](#)
- [Case Dispatcher Module](#)
- [Expiry Monitor Thread](#)

The following figure illustrates how these components work together.



CAPMRA--15_c0001

Case Queues

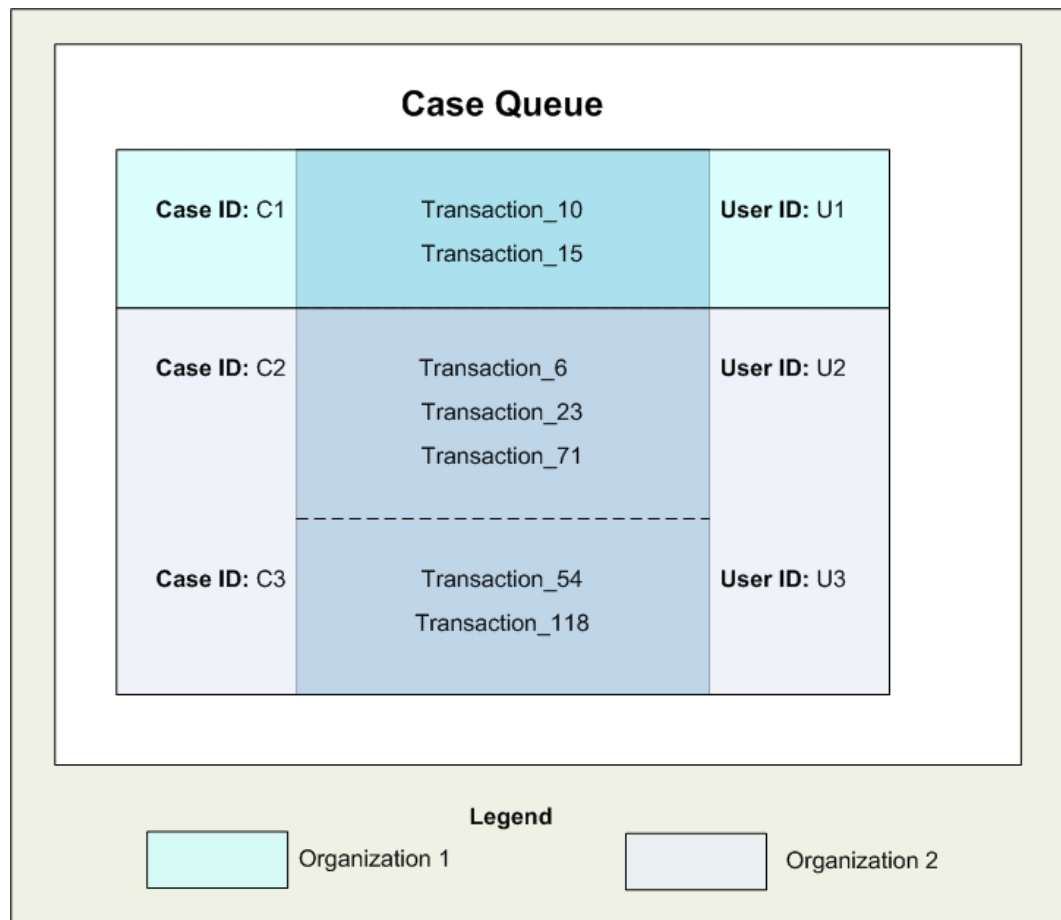
A *Case Queue* (or simply a *Queue*) is a list of cases that are grouped based on criteria, such as **Date Created**, **Date Updated**, **Number of Open Transactions**, and **Next Action Date**. RA supports multiple Queues for each organization in the system.

RA allows you to set levels for Queues. Each Queue is assigned to a level when the Queue is created. Queue levels help define how cases are escalated. For example, cases from Queues of Level 1 get escalated to Queues of Level 2 in the same organization.

Note the following points related to Queue levels:

- RA allows you to set up to four levels for Queues.
- Each Queue is associated with exactly one level.
- Once you assign the Queue level, you cannot edit it.
- There can be a maximum of only one Queue for levels other than Level 1.
- Queue Criteria is not applicable to Queues at levels greater than Level 1.

The following figure depicts what a typical Queue looks like.



CAPMRA--15_c0002

Queues are managed by Queue Managers, and are associated with a Queue Name, Case Order criteria in the Queue, and Case Priority. Queue Managers can define a new queue. New cases that are generated are added to the Queue when a Queue rebuild happens. By default, Queue rebuild

happens every 30 minutes. The GA can configure this frequency on the Miscellaneous Configuration screen. The Queue Manager for an organization can also issue a Queue rebuild request from Administration Console. Cases that do not fit into any individual Queue are assigned to the DEFAULT queue

The Queue Manager can assign Customer Service Representatives (CSRs) to work on each Queue, depending upon the skill of the CSR or other organization policies.

Note: More than one CSR can be allocated to a Queue in an organization. Also, if there are multiple organizations in a CSR's purview, the CSR can be allocated to multiple Queues.

Queue Server

The *Queue Server* is responsible for:

- Caching [Case Queues](#) and Queue-to-Administrator mapping with the help of the [Queue Monitor Thread](#).
- Dispatching the cases in the [Case Queues](#) to the active Administration Console instances with the help of [Case Dispatcher Module](#).

- Maintaining the updated list of expired cases with the help of [Expiry Monitor Thread](#).

Queue Monitor Thread

The *Queue Monitor* (referred to as *Scheduler*) thread runs at the [Queue Server](#)-end and is responsible for creating the Case Schedule, populating the [Case Queues](#) with cases, and prepares the Queues for [Case Dispatcher Module](#).

This thread works as follows:

1. It wakes up at a pre-defined interval and fetches from the database a list of all the cases that meet the following criteria:
 - At least one transaction shows the Fraud Status as **Undetermined**.
 - The case has not expired.
2. Caches the Queues with cases.
3. Based on the case state and other criteria (such as **Transaction Date**, **Transaction Amount**, or **Next Action Date**), the thread assigns the cases into the [Case Queues](#).
4. For more information about case states, see [Case States](#).
5. When a case is assigned to the Queue, an in-memory list is created for the Queue.
6. On completion of the case assignment to a Queue, the state of all the assigned cases is changed to OPEN.
7. When the Customer Service Representatives (CSRs) click the **Save and Go to Next Case** or the **Go to Next Case** button:
 - a. A request to fetch the next case in the Queue is sent to the [Queue Monitor Thread](#) via [Queue Server](#).
 - b. In response, the [Case Dispatcher Module](#) picks the case from the memory queue and returns its Case ID to the Administration Console instance from where the request originated.
8. The state of the case is then changed to IN PROGRESS, and the CSRs can work on the case.
9. On receiving the Case ID, the Administration Console instance fetches all the transactions for the case from the database and displays the same to the CSR.
Based on the case review process, the case state can change. See [Case States](#) for more information.

Case Dispatcher Module

The *Case Dispatcher Module* (referred to as *Dispatcher*) listens to the case requests from the individual CSRs at the [Queue Server](#)-end and "pushes" the cases (as per their order in the Queue) from the [Case Queues](#) to the individual Administration Console instances on demand.

This module works as follows:

1. When CSR logs in, a request is sent to the Dispatcher to fetch the next case.

2. The Dispatcher fetches the next case from the Queue(s) assigned to this CSR.
3. The Dispatcher, then, acquires a lock on the selected case in the RA database.
4. The Dispatcher also changes the status of the case from OPEN to INPROGRESS, and updates the affected table with the name of the CSR from whose Administration Console instance the request originated.
5. The Dispatcher, then, sends the case details back to the Administration Console instance, which then fetches the transactions for the case and displays them on the screen for the CSR.
6. The Administration Console instance also sets a Timeout for the displayed case details. This prevents the CSR from opening a case page and then not working on it within the pre-defined time interval. If the current case allocation to the CSR times out, an appropriate message is displayed to the CSR. The case subsequently times out and its status is changed to OPEN.
7. If the currently displayed case does *not* timeout and the CSR moves to the next case in the Queue, the case status is changed from INPROGRESS back to OPEN.
The CSR can view the next case by clicking the **Go To Next Case** button on their screen.

Expiry Monitor Thread

The Expiry Monitor thread is responsible for escalating cases or marking all the cases that have expired since the last time the thread ran. It wakes up at a much lesser frequency than the [Queue Monitor Thread](#).

This thread works as follows:

1. It wakes up at a pre-defined and configurable interval and fetches a list of all cases that meet the following criteria:
 - The case is in the OPEN or NEW state.
 - The case update time is more than the configured expiration time.
- In other words, it looks for cases that have not been worked upon and for which no new alerts have been generated.
2. For all cases that have not been worked upon for the specified threshold duration and that currently belong to queues with Retention Policy **Auto Expire**, the thread updates the status as EXPIRED in the RA database. For all cases that have not been worked upon for the specified threshold duration and that currently belong to queues with Retention Policy **Auto Escalate**, the thread escalates the cases by adding them to the next higher level queue with IN PROGRESS status.
 3. The thread goes back to sleep.

Supported Case Management Roles that You Will Use

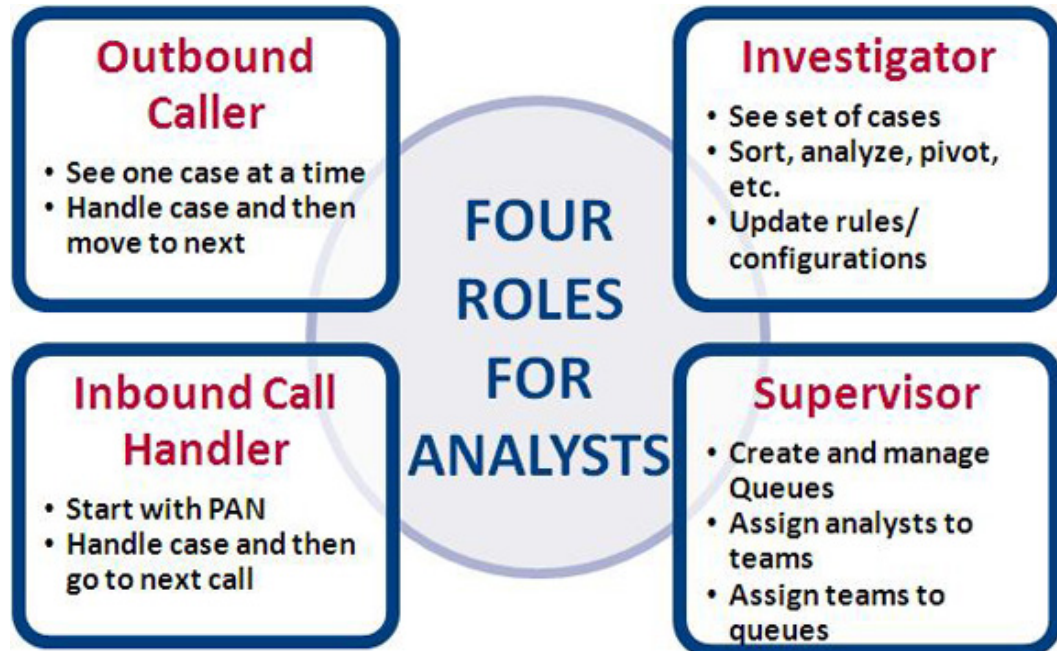
The Case Management feature supports the following broad categories of roles:

- [Customer Service Representatives](#)

- [Queue Managers](#)
- [Fraud Analysts](#)

[Summary of Case Management Role Privileges](#), summarizes the privileges available to these roles.

The following figure shows the different case roles and the tasks performed by each role.



CAPMRA--15_c0003

Customer Service Representatives (CSRs)

As the name suggests, *Customer Support Representatives* (CSRs) are your organization's interface with the end user. They are responsible for:

- [Working on Cases](#)
- [Handling Customer Calls](#)

Working on Cases

They typically review cases that are automatically allocated to them and work on these cases. When they start working on a case, the case is marked with their name. As a result, the case will not show in another CSR's screen. However, the [Queue Managers](#) can reassign the case to another CSR by assigning another CSR to the Queue.

CSRs can also call end users to confirm the authenticity of a suspect transaction. Their main activities include:

- If required, call the end users to verify if a transaction is fraudulent or not.
- Add users to the **Exception User List** for a specified duration, based on the user input. The default duration is 10 days, but they can change it as required.
- After reviewing a case, CSRs can update the case. As a result of which, they can change the case status from **In Progress** to one of the following:

- On Hold
- Closed
- They can also take appropriate notes in a free-form field to capture the progress of the investigation.

Handling Customer Calls

At times, the CSRs also handle incoming calls from the end users. In other words, they attend customer calls. For example, a customer might call the Call Center because they see transactions that they did not perform. In such cases, these operators record the input from the customer, if a case for the specified user already exists. If a case does not exist for the customer, then a case is generated automatically.

Note: The input collected by CSRs is used by the Fraud Analyst for analyses.

In this case, the CSRs:

- Handle user calls.
- Record user inputs.
They can take appropriate notes in a free-form field to capture the progress of the investigation.
- View recent activities of the user.
- Add users to the **Exception User List** for a specified duration, based on the user input.
The default duration is 10 days, but they can change it as required.
- Search for the transactions by the user in the given time period.

Queue Managers

Queue Managers (or simply, Supervisors) determine the order in which cases are assigned to the Queue. They can:

- Create new Queues and assign cases to one of several Queues for their organization.
See [How to Create a New Queue](#) for more information about how to create a Queue.
- Manage the Queues for all organizations in their scope.
See [Case Queues](#), for more information about Queues.
- Rebuild a Queue.
See [How to Rebuild a Queue](#) for more information.
- Assign and reassign CSRs to the Queues in their scope.

Note: By default, Queue Managers *cannot* perform the tasks of a Fraud Analyst. However, you can use **Custom Roles** to create a new role based on Queue Manager and assign the FA privileges to this role. For more information about how to create custom roles, see "Creating a Custom Role".

Fraud Analysts

Fraud Analysts (FAs) research and analyze fraud patterns in transactions to define anti-fraud strategies. They analyze the trends in transactions by using the truth data collected by other CSRs *and* the available filters, such as:

- Transactions by the same user in the given time period.
- Transactions from the same user device in the given time period.
- Transactions from the same IP address in the given time period.

Based on their analyses, FAs can then advise the system administrators on fine-tuning RA. In addition, if they suspect a transaction to be suspicious, they can raise a request for CSRs to call the end user and find more details related to the suspect transactions, even if the system had not suspected those transactions previously.

The following list describes the main functions performed by Fraud Analysts:

- They can log in and view the list of transactions in real time.
- They can set a combination of filter conditions to view transactions for all users over a period of time for those matching specific risk status values.
- As part of the investigation, the FA can also search for similar transactions. They can define the filter to detect similarity based on:
 - Transactions by the same user in the given time period.
 - Transactions from the same user device in the given time period.
 - Transactions from the same IP address in the given time period.
- If the transaction set is large, they can also export the data offline and then analyze it.
- If they locate suspicious patterns, they can raise alerts on those transactions for further investigation by the CSRs. The "alerted" transactions are automatically added to the case for the user in question.

Note: Fraud Analysts *cannot* update any cases.

Summary of Case Management Role Privileges

The following table summarizes the privileges available to the case roles discussed in the preceding topics.

Privilege	CSR	Queue Manager	Fraud Analyst
Manage Inbound Calls	Y	N	N
Work on Cases	Y	N	N
Manage Queues	N	Y	N
Rebuild Queues	N	Y	N
View Queue Status	N	Y	N

Analyze Transactions	N	N	Y
Add User to Exception List	Y	N	N
Delete User from Exception List	Y	N	N
Search Cases	N	Y	N
Decrypt Sensitive Information	N	Y	Y
Report Privileges			
View Fraud Statistics Report	N	N	Y
False Positives Report	N	N	Y
Rule Effectiveness Report	N	N	Y
Case Activity Report	N	Y	N
Average Case Life Report	N	Y	N

Supported Case Management Workflows

This topic covers the workflows for the following phases in the lifecycle of a case:

1. [Case Generation](#)
2. [Case Queuing](#)
3. [Case Assignment](#)
4. [Case Handling](#)
5. [Case Expiry](#)
6. [Case Escalation](#)
7. [Fraud Analysis](#)

Case Generation

Typically, cases are created automatically by the system. However, if a case operator manually flags a suspicious transaction for a user, or a Fraud Analyst discovers a suspicious pattern in user transactions, then they can add the suspicious transactions to the case.

A case is generated when:

- The advice for the risk evaluation for a transaction is either **Alert** or **Deny**.

Note: If a case is already open for the user, then this transaction is added to the existing case. You can configure this on the Miscellaneous Configurations page.

- A user contacts your Call Center to dispute a transaction.
In this case, the case operator can either refer the disputed transactions for further investigation or can mark the transaction as a fraud. In both the cases, the transaction is automatically added to a case.
- A Fraud Analyst suspects some transactions to be fraudulent (typically, based on patterns detected earlier) and marks them for further investigation.

Note: These transactions are then added to the existing case.

Case Queuing

When a case is created and transactions are added to the case, the cases need to be assigned to the Queue that belongs to the organization. In addition, CSRs who can work on these cases must also be assigned to each Queue. The [Queue Monitor Thread](#) plays the pivotal role in this case.

See [Queue Monitor Thread](#) for detailed information about how this thread queues cases.

Case Assignment

After a case has been queued, it then needs to be dispatched to each CSR's screen. The [Case Dispatcher Module](#) plays the pivotal role in this case.

See [Case Dispatcher Module](#) for detailed information about how this thread dispatches cases.

Notes Related to Case Assignment

Some points to remember on this topic are:

- A new case is assigned to a CSR from the organization to which the case belongs.
- The cases are assigned based on their order in the Case Queue. The order criteria can include:
 - Next Contact/Action Date
 - Number of open transactions in the case
 - Age of the case (Date Created)
 - How long ago the case was last updated
- Every case is eventually handled by a CSR in an organization.

Case Handling

Cases are handled by the CSRs as follows:

- A new transaction flagged by the FA or a Deny or Increase Authentication advice generated for a transaction creates a new case. The status of the case *before* the [Queue Monitor Thread](#) schedules it is **NEW**. The [Queue Monitor Thread](#) changes it to **OPEN**, and when a CSR finally views the case, the case status is changed to **INPROGRESS**.

Note: Even before the case is handled by a CSR, more flagged transactions might be added to the case.

- A CSR is automatically assigned to work on the case.

- Contact the user out of band, say by sending an email or by calling them on the specified contact number.
- Based on the ongoing investigation and the results of contacting the end user, the CSR can update the case, as it develops:
 - Search for transactions based on a specific time interval.
 - During the user interaction, add previously unsuspected transactions to the case.
 - Choose resolutions for one or more of the transactions in the case.
 - Mark the case for follow up and set the **Next Action Date**.
Typically, the **Case Status** of such cases is then updated to either **INPROGRESS** or **ONHOLD**, and the user is contacted by a CSR later.
 - Based on user input, add the user to the **Exception User List** for a specified period of time.
 - Resolve the case and change the **Case Status** to **CLOSED**.
- The [Queue Managers](#) can also reopen an expired case, if required.

Case Expiry

A case can expire if all of its transactions are not handled within the stipulated amount of time or if there is no activity on the case for a pre-defined time period.

Note: The default case expiry time is 48 hours.

See [Expiry Monitor Thread](#) for detailed information about how this thread manages expired cases.

Case Escalation

A case is automatically escalated to the next queue level if the case has not been worked upon for the specified threshold duration and if the case currently belongs to a queue with Retention Policy **Auto Escalate**.

See [Expiry Monitor Thread](#) for detailed information about how this thread manages expired cases.

Fraud Analysis

The gist of the fraud analysis workflow for transactions by Fraud Analysts is as follows:

- FAs can search for transactions based on criteria, such as Transaction Date, Secondary Authentication Status, Transaction type, Risk Advice and Case Status. For more information, see [How to View Transactions Summary](#):
 - All transactions are initially shown in the Transaction Summary view.
 - Initially, all transactions have the Case Status of **New**.
 - The list of transactions can be exported to a .csv file for processing in Microsoft Excel.
- The FAs can click a case to view its details. For more information, see [How to View Case Details](#).

- The FAs can also search for all transactions that are similar to a case. For more information, see [How to View Similar Transactions](#).
- If they find suspect transactions and potential fraud patterns during their analyses, FAs can mark the transactions for further investigations by CSRs. For more information, see [How to Mark Transactions for Further Investigation](#).

Working with Case Queues

A Case Queue (or simply a Queue) is a list of cases that are grouped based on criteria, such as **Date Created**, **Date Updated**, **Number of Open Transactions**, and **Next Action Date**. RA supports multiple Queues for each organization in the system.

This topic guides you through the following tasks:

- [How to Create a New Queue](#)
- [How to View Queue Status](#)
- [How to Update Queue Status](#)
- [How to Rebuild a Queue](#)
- [How to Disable a Queue](#)
- [How to Enable a Queue](#)
- [How to Delete a Queue](#)

How to Create a Queue

Important! Only a GA, an OA, or a Queue Manager (QM) can perform the tasks (for the organizations that are in their scope) described in this topic. The MA, UAs, FAs, and CSRs *cannot* perform these tasks.

A Queue Manager can create a new Queue by specifying the name, description, criteria, and priority for the queue. The Queue Manager also assigns administrators to a Queue. An administrator can be assigned to multiple Queues, and multiple administrators can be assigned to the same Queue.

To create a queue:

1. Log in to Administration Console as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, specify the Organization for which you want to create a Queue.
The updated page appears.

5. Click **Create New Queue**.
The updated page appears.
6. Specify the **Queue Name**.
7. Specify a **Display Name** for the queue.
8. Specify the **Queue Description**, if required.
9. In the **Assign Administrators** section:
 - a. From the **Administrators** list, select the required administrators that you want to assign to the queue.
 - b. Click the > button to move the selected administrators to the **Selected Administrators** list.

Note: If you want to move all the **Administrators** to the **Selected Administrators** list, then click the >> button to do so.

10. **Set the Queue Level.**

This release of RA allows you to set up to four levels for Queues. Queues that are created by default when an organization is created are assigned to Level 1. Before creating Queues at a level other than Level 1, you must ensure that a Queue exists at the preceding level.

Important! Once you assign the Queue level, you cannot edit it.

For more information about Queue levels, see [Case Queues](#).

11. In the **Retention Policy** list, select *one* of the following:

- **Auto Escalate:** The case is automatically escalated to the next queue level if the case has not been worked on for the specified number of Hours.
- **Auto Expire:** The case automatically expires if it has not been worked on for the specified number of Hours.

Important! A queue that is already at the highest level cannot have a **Retention Policy** of **Auto Escalate** because there is no higher level to which the case can be escalated.

12. (Only if you have **Set the Queue Level** to **1** in Step 10) In the **Criteria** section:

- a. Define the criteria (**Risk Advice** or **Matched Rule**) to determine which cases are added to the queue.
- b. Select the operator and value from the corresponding drop-down lists.
- c. Click **Add** to add the expression to the expression area.
- d. Use the AND, OR, (, or) operators to combine fragments and build the final criteria expression.
Cases that match this expression will be assigned to the queue you create.

Note: For queues at levels other than 1, Criteria is not required because there exists only one queue at those levels and all cases for that level would be assigned there.

13. In the **Order By** section:

a. Specify the element by which you want to sort the Queue. The options available are:

- Next Contact Date
- Date Created
- Date Updated
- Number of Open Transactions
- Risk Advice
- Risk Score

b. Specify the order by which you want to order the corresponding element. The options available are:

- Ascending
- Descending

14. Click **Save** to save the updates you made on the screen and create the Queue.

15. Refresh the organization cache for the changes to take effect.

a. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.

b. Activate the **Organizations** tab.

c. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.

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

A list of organizations matching the search criteria appears.

e. Select the organizations whose cache you want to refresh.

f. Click **Refresh Cache**.

g. Click **OK** in the dialog box to confirm your cache refresh request.

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

How to View Queue Status

On the Queue Status page, you can view the latest statistics related to the **DEFAULT** Queue. The statistics you can view are:

- Total Open Cases
- Total Diarized Cases
- In-Progress Cases
- Total Cases
- Number of Administrators Assigned

It also shows the details of the **Cases Handled in Last 8 Hours**.

To view a queue's status:

1. Log in to Administration Console with the necessary privileges to manage Queues.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **View Queue Status** link to display the Queue Status page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to view.
The page with the updated Queue details appears.

Note: Diarized cases (not in queue) appear separately along with **Inbound Cases (In-Progress)**.

How to Update Queue Status

You can update the status of the Queue by using any one of the following methods:

- By clicking the **View Queue Status** link to display the corresponding page, and then clicking the link in the **Queue Name** column corresponding to the queue you want to update.
- By using the **Manage Queues** link under the **Queue Management** section.

To update the status of the Queue by using the latter option:

1. Log in to Administration Console with the necessary privileges to manage Queues.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to manage.
The updated page appears.
6. Specify the **Queue Description**, if required.
7. In the **Assign Administrators** section:

- a. From the **Administrators** list, select the required administrators that you want to assign to the queue.

Note: To select more than one administrator, press the SHIFT key and click the required administrators.

- b. Click the > button to move the selected administrators to the **Selected Administrators** list.

Note: If you want to move all the **Administrators** to the **Selected Administrators** list, then click the >> button to do so.

8. Set the **Retention Policy** to **Auto Escalate** or **Auto Expire** and specify the required duration after which the case will be escalated or expired, respectively.

9. (If you chose a Queue other than DEFAULT Queue and if the queue level is 1) In the **Criteria** section:

- a. Define the criteria (**Risk Advice** or **Matched Rule**) to determine which cases are added to the queue.
- b. Select the data item, operator, and value from the corresponding drop-down lists to define the criteria.

10. In the **Order By** section:

- a. Specify the element by which you want to sort the Queue. The options available are:
 - Next Contact Date
 - Date Created
 - Date Updated
 - Number of Open Transactions
 - Risk Advice
 - Risk Score
- b. Specify the order (**Ascending** or **Descending**) by which you want to order the corresponding element.

11. Click **Save** to save the updates you made on the screen.

12. Refresh the organization cache for the changes to take effect.

- a. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
- b. Activate the **Organizations** tab.
- c. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.

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

A list of organizations matching the search criteria appears.

- e. Select the organizations whose cache you want to refresh.

- f. Click **Refresh Cache**.

- g. Click **OK** in the dialog box to confirm your cache refresh request.

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

How to Rebuild a Queue

The Case Management Server rebuilds the Queues at pre-configured intervals. The default value is 1800 seconds. The GA can change this value at the global level for all organizations by configuring the **Frequency of Automatic Queue Rebuild Schedule (in Seconds)** parameter in the Miscellaneous Configurations page.

There may be a need to rebuild a Queue before the automatic rebuild time in the following cases:

- A new Queue is defined.
- One or more Queue definitions have changed.
- When a Queue has been enabled, disabled, or deleted.

In such cases, the Queue Manager can rebuild the queue using the Rebuild Queues page.

Important! You can only rebuild Level 1 queues. Queues at other levels are rebuilt when the case is escalated or when the case expires.

Cases that are configured for escalation are marked with an internal case status of ESCALATED. After cases are marked as ESCALATED, queue rebuild for higher level queues, other than Level 1, is undertaken so that the escalated Cases are part of the next level queue and are available for working.

To rebuild a queue:

1. Log in as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Rebuild Queues** link to display the Rebuild Queues page.
4. Do one of the following:
 - Select **All Organizations** if you want the QM to rebuild the queues for all organizations in their purview.

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

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

5. Click **Rebuild** to rebuild the Queue for the selected organizations.

How to Disable a Queue

Note: To be able to disable a Queue, you must ensure that you have the appropriate privileges and scope to do so. Only GAs, OAs, and QMs can disable Queues.

To disable a queue:

Important! You can disable a lower level queue only after disabling the higher level queues. You cannot disable the DEFAULT Queue.

1. Log in as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to disable.
The updated page appears.
6. Click **Disable This Queue** to disable the queue.
7. Refresh the organization cache for the changes to take effect.
 - a. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
 - b. Activate the **Organizations** tab.
 - c. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
 - d. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
 - e. Select the organizations whose cache you want to refresh.
 - f. Click **Refresh Cache**.
 - g. Click **OK** in the dialog box to confirm your cache refresh request.

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

How to Enable a Queue

Note: To enable a Queue, you must ensure that you have the appropriate privileges and scope. Only the GAs, OAs, and QMs can enable Queues.

To enable a queue:

1. Log in as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to enable.
The updated page appears.
6. Click **Enable This Queue** to enable the queue.
7. Refresh the organization cache for the changes to take effect.
 - a. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
 - b. Activate the **Organizations** tab.
 - c. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
 - d. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
 - e. Select the organizations whose cache you want to refresh.
 - f. Click **Refresh Cache**.
 - g. Click **OK** in the dialog box to confirm your cache refresh request.

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

How to Delete a Queue

Note: You can delete a lower level queue only after deleting the higher level queues. Before you delete a queue, you must 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.

To delete a queue:

1. Log in as an OA or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to delete.
The updated page appears.
6. Click **Delete This Queue** to delete the Queue.
7. Refresh the organization cache for the changes to take effect.
 - a. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
 - b. Activate the **Organizations** tab.
 - c. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
 - d. Enter the complete or partial information of the organization you want to search and click **Search**.
A list of organizations matching the search criteria appears.
 - e. Select the organizations whose cache you want to refresh.
 - f. Click **Refresh Cache**.
 - g. Click **OK** in the dialog box to confirm your cache refresh request.

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

Important! You *cannot* delete the DEFAULT Queue.

Searching for Cases

You can search for specific transactions by using either the search criteria or Case ID. This topic guides you through the steps for:

- [How to Search for Cases Using Search Criteria](#)

- [How to Search for Cases Using Case ID](#)

[What are the Fields in the Transaction Summary Page](#) explains the fields that you will see in a typical Transactions Summary.

How to Search for Cases Using Search Criteria

To search for cases based on search criteria:

1. Ensure that you are logged in with proper credentials (GA or OA.).
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the **Search Cases** link.
4. From the **Select Organization** list, select the organization whose data you want to filter in the report.

Note: When the administrator has access to multiple perspectives in the system, the **ALL ISSUERS** and **ALL ACQUIRERS** options are available in the **Select Organization** drop-down list. Otherwise, you see the **ALL organizations** option.

The Search Cases page for criteria-based search appears.

5. Enter the user identification information.
The field differs based on the channel configured for the organization, as follows:

- Default, ATM, POS, ECOM: **Enter User Name**
- 3DSecure: **Enter Card Number**
- IMPS: **Enter User Name**
- Acquirer Organization ATM and POS: **Enter Terminal ID**

Important! If you selected **ALL ISSUERS**, **ALL ACQUIRERS**, or **ALL organizations** in Step 4, this field is not enabled.

6. From the **Case Status** list, select the status of the case that you want to view.
7. To filter the cases based on *one* of the following criteria:
 - Select the pre-defined date range based on which you want to filter the case data in the **Case Date From** and **To** fields.
 - Select the **Last Cases** option and then select the time interval (in minutes) for which you want to see the latest cases that were generated.
8. Select **Decrypt Sensitive Information** if you want to display the data in clear text.
9. Click **Submit** to generate the Cases Summary page.

For a description of the fields on the Cases Summary page, see [How to Use Cases Summary Page Fields](#).

How to Search for Cases Using Case ID

To search for cases based on case ID:

1. Ensure that you are logged in with proper credentials (GA or OA.)
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the **Search Cases** link.
4. From the **Select Organization** list, select the organization whose data you want to filter in the report.

Note: When the administrator has access to multiple perspectives in the system, the **ALL ISSUERS** and **ALL ACQUIRERS** options are available in the **Select Organization** drop-down list. Otherwise, you see the **ALL** organizations option.

5. Click **Switch to Case ID Based Search**.
The Search Cases page for case ID based search appears.
6. Enter the **Case ID** of the case that you want to search.
7. Select **Decrypt Sensitive Information** if you want to display the data in clear text.
8. Click **Submit** to generate the Cases Summary page.

For a description of the fields on the Cases Summary page, see [How to Use Cases Summary Page Fields](#).

What Are the Cases Summary Page Fields

The following table describes the fields listed in the Cases Summary page.

Field	Description
Case ID	Click the Case ID link to look into the details of the case.
User Name/Terminal ID/Beneficiary IMPSID	<ul style="list-style-type: none">▪ The card number of the user (Default, Ecom, and Issuer ATM and POS channels)▪ The Terminal ID from where the transaction was performed (Acquirer ATM and POS channels)▪ The Beneficiary IMPSID (IMPS channel)
Organization	The organization to which the user belongs.
Case Status	The status of the case. The possible values are: <ul style="list-style-type: none">▪ NEW▪ OPEN▪ INPROGRESS▪ CLOSED▪ ONHOLD▪ EXPIRED

Advice ID	The action suggested by RA after evaluating the Risk Score of the transaction. The possible values are: <ul style="list-style-type: none"> ▪ ALLOW ▪ ALERT ▪ INCREASEAUTH ▪ DENY
Queue Name	The name of the Queue to which the case belongs.
Matched Rule	The rule that matched and for which RA generated the case.

To view further details of the case and to work on the case, click the **Case ID** link on the Cases Summary page.

Customer Support Representatives Handling Cases

Important! Only the OAs and CSRs can work on cases that belong to the organizations that are in their scope. The MA, GAs, UAs, and FAs *cannot* perform these tasks.

This topic walks you through the following tasks that are related to handling cases and direct interaction with end users:

- [How to Work on Cases](#)
- [How to Manage Inbound Customer Calls](#)
- [How to Blacklist a Device](#)

How to Work on Cases

When RA marks a transaction as suspect or an FA marks a transaction for further investigation, the case *automatically* appears in the CSR's case list.

To work on the cases in your list:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Work On Cases** link.
The first case (in the order of the priority assigned to your cases) appears.
The fields in the page are explained in the following table.

Field	Description
User Name/Card Number/Beneficiary IMPSID/Terminal ID	<ul style="list-style-type: none"> ▪ The card number of the user (Default, Ecom, and Issuer ATM and POS channels)

	<ul style="list-style-type: none"> ▪ The Terminal ID from where the transaction was performed (Acquirer ATM and POS channels) ▪ The Beneficiary IMPSID (IMPS channel)
Next Action Date	The date when the user must be contacted the next time.
Case History	<p>The latest case Notes and Additional Notes entered by the previous call handler.</p> <p>If you want to review all the previous notes in this field, then click the More... link to do so.</p>
Case ID	The unique ID generated for the case.
Alerts on This Case	
Mark Selected As	<p>The fraud status of the transaction. The possible values in this field are:</p> <ul style="list-style-type: none"> ▪ Undetermined ▪ Confirmed Fraud ▪ Confirmed Genuine ▪ Assumed Fraud ▪ Assumed Genuine <p>If you have more than one alerted transaction that need your attention and after talking to the user you determine that all of their fraud status is the same (say Confirmed Fraud or Confirmed Genuine), then you can use this drop-down list to set the same in one action.</p>
Fraud Type	The type of fraud that occurred.
Device ID	The ID of the device used for the transaction.
Country	Based on the IP Address, the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the user transaction.
Merchant	The merchant involved in the transaction.
Currency	The currency used in the transaction.
Amount	The total transaction amount.
Organization's Base Currency	The base currency defined for the organization.
Amount in Organization's Base Currency	The transaction amount converted to the organization base currency.
Transaction Date	The timestamp when the given transaction was performed.
TXID	<p>The unique system-generated identifier for the user transaction.</p> <p>If required, you can click the Transaction ID to view its details.</p>
Model Score	The risk score returned by the Model for the transaction.

Processing Code	A series of digits that describes the type of transaction and the accounts affected by the transaction.
Datetime Local Txn	The local time at the ATM from where the transaction originated.
Transaction Datetime	Time (Hours-Mins) extracted from the date/time when the ISO 8583 message was constructed in and represented in GMT/UTC.
Transaction Amount	The total transaction amount.
Reversal Amount	The amount reversed during the transaction.
Secondary Auth Status	If the Risk Advice is INCREASE AUTHENTICATION, then this column specifies the result of the additional authentication that your application returned as feedback to RA.
Action	<p>The type of transaction performed by the user, which can be:</p> <p>ATM:</p> <ul style="list-style-type: none"> ▪ WITHDRAWAL ▪ FINANCIALINQUIRY ▪ PINCHANGE <p>POS</p> <p>PURCHASE</p>
Transaction Status	The status of the transaction.
Reversal Status	The status of the reversal transaction.
Transaction Action Code	The code assigned to the transaction action.
MTI	Message Type Identifier. This is a 4-digit field that classifies the high-level function of the ISO 8583 message (consisting of Message Version, Message Class, Message Function, and Message Origin).
Matched Rule	The rule that matched and for which RA flagged the transaction as risky.
Score	The overall risk score returned by RA for the corresponding transaction. This is a value between 0 and 100.
Merchant Category	Category code of the merchant involved in the transaction.
POS Entry Mode	Indicates the method used to enter the account number.
Acceptor Address	Address of the card acceptor.
Acceptor City	City from which the transaction originated.
Acceptor State	State from which the transaction originated.
Device Type	The type of device involved in the transaction.
OS	The operating system on the device that was used to perform the transaction.

Card Accept Country	The code identifying the country of the acquiring institution.
Browser	The browser that was used to perform the transaction.
Acquirer Country	Country where the acquiring institution for the POS is located.
Device ID Status	The status of the Device ID: <ul style="list-style-type: none"> ▪ READ: The Device ID was read from the device. ▪ NEW: The Device ID was assigned to the device. ▪ REVERSE LOOKUP: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
Acceptor Terminal ID	Code that identifies a card acceptor terminal or a POS.
Acceptor ID	ID of the card acceptor (merchant) operating the POS.
ACQ Bin	Acquirer BIN of the merchant where the transaction was made.
POS Condition Code	Indicates the transaction conditions at the POS.
RRN	Retrieval Reference Number that helps identify and track all messages related to a given cardholder transaction.
Response Code	The response code to a request for a transaction.
AFPN Advice	Displays the AFPN advice if AFPN was invoked during the transaction or later.
Advice	The action suggested by RA after evaluating the Risk Score of the transaction.
Channel	The channel on which the transaction was performed.
From	The pre-defined date range using which you want to filter the data.
To	
Show Transactions	The button to display the alerted transactions based on the preceding From and To fields.
Hide Transactions	The link to hide the displayed alerted transactions.
Case Status	The current status of the case. The possible values are: <ul style="list-style-type: none"> ▪ INPROGRESS ▪ ONHOLD ▪ CLOSED
Queue	The Queue to which this case has been assigned.
Note	The pre-determined reason for the update.

Additional Note	Any additional information (in addition to the preceding Note) that describes the reason for the change in the case status or any of the fields before. This field cannot accept more than 250 characters.
Next Action Date (GMT)	The date when the user must be contacted the next time for additional follow-up.
Select User State	<p>Note: This field is displayed only if you are viewing the alert for an Issuer organization.</p> <p>By default, each user has the state "UNDEFINED". Other states that the users can be set to are:</p> <ul style="list-style-type: none"> ▪ Positive ▪ Suspect ▪ BlackListed
From	The date range for which you want the user to remain in the configured user state.
To	
Predefined Duration	<p>The duration for which you want the user to remain in the user state. Possible values are:</p> <ul style="list-style-type: none"> ▪ 12 hours ▪ 1 Day ▪ 2 Days ▪ 4 Days
Reason	The reason for which the user is being added to the particular user state.
<p>If you have already set the user to a particular User State, then the next time you work on the case for that user the following fields are displayed:</p> <p>Current User State: The user state to which the user is assigned. You can choose to extend or shorten the time duration for which you want to keep the user in this user state by specifying the duration in the From and To fields.</p> <p>Note: The date and time specified here is always considered in the user's timezone. The value is stored in the database in GMT, but converted to user timezone when displayed to the user.</p> <p>Reset the User State: Resets the user state to the original state.</p>	
Add User to Exception List	<p>Note: This field is displayed only if you are viewing the alert for an Issuer organization.</p> <p>If based on user inputs, you want to temporarily exclude a user from risk evaluation for a specified time interval.</p> <p>For example, a user is traveling to a Negative Country and you do not want the user to be denied any transaction for the same. In this case, you can add the user to the Exception User</p>

	List. If the user is found in the Exception User List, then by default RA returns a low Score and the ALLOW advice for transactions originating from these users.
From	The date and time range for which you want the user to be exempted from RA risk evaluation.
To	
Predefined Duration	<p>The duration for which you want the user to be exempted from RA risk evaluation. The reason for which the user is being added to the Exception User List. Possible values are:</p> <ul style="list-style-type: none"> ▪ 12 hours ▪ 1 Day ▪ 2 Days ▪ 4 Days
Reason	The reason for which the user is being added to the Exception User List.
If you have already added a user to the Exception User List, the next time you work on the case for that user, the following fields appear.	
User Present in the Exception List	
Keep User in Exception List	<p>You can choose to extend or shorten the time duration for which you want to keep the user in the Exception User List. Select the date and time range for which you want to keep the user in Exception User List.</p> <p>Note: The date and time specified here is always considered in the user's timezone. The value is stored in the database in GMT, but converted to user timezone when displayed to the user.</p>
Remove User from Exception List	Remove the user from the Exception User List.
Reason	The reason for which the user is being kept in or removed from the Exception User List.

4. Perform the required actions to capture the user inputs by using the fields explained in the preceding table.

5. When done, click one of the following buttons on the page:

- **Save** to update your changes to the case.
- **Save and Go To Next Case** to update your changes to the case and go to the next case assigned to you.
- **Go To Next Case** to go to the next case assigned to you without saving the changes.
- **Cancel** to cancel any changes you just made on the page.

How to Manage Inbound Customer Calls

When an end user calls your Customer Support Center to dispute a transaction, then the attending CSR must use the Manage Inbound Calls page to capture the information provided by the user and make the required changes to the case based on this information.

To make the required changes to the case by using the Manage Inbound Calls page:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Manage Inbound Calls** link to display the Manage Inbound Calls page.
4. From the **Select Organization** list, select the required organization.
The updated Manage Inbound Calls page appears.
5. Enter the user identification information.
The field differs based on the channel configured for the organization, as follows:
 - Default, ATM, POS, ECOM: **Enter User Name**
 - 3DSecure: **Enter Card Number**
 - IMPS: **Enter User Name**
 - Acquirer Organization ATM and POS: **Enter Terminal ID**

If you have configured accounts for the organization, you will be prompted to enter the user identifier. You can filter based on user name or the account type from the drop-down list.
6. Click **Submit**.
The Manage Inbound Calls page is refreshed with the specified user's case information.
7. Perform the required actions to capture the user inputs by using the fields explained in the table in [How Customer Support Representatives Work on Cases](#).
8. When done, click **Save** to update your changes to the case.
If you do not want to save the changes you just made, click **Cancel**.

How to Add a User to the Exception User List

An *exception user*, in RA terminology, is an end user who is exempted from risk evaluation for a specified interval of time. RA always generates the ALLOW advice for such users.

For example, a known (and trusted) user might travel to a blacklisted country for 3 weeks. Because RA is configured to generate very high score (and therefore DENY) for transactions coming from a Negative Country, every time the user performs a transaction in these three weeks will be denied. This is a frustrating situation for an end user. To exempt the user from such

situation during their stay in the Negative country, you can configure the user as an exception user for these three weeks. In this case, all their transactions - genuine or fraudulent - will be allowed. Therefore, you must be careful with this feature and must add the user to VIP status only after talking to them.

You can add a user to the Exception User List in two ways:

- While Working on Cases
- While Handling Inbound Customer Calls

While Working on Cases

To add a user to the Exception User List:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Search Cases** link to display the Search Case page.
4. From the **Select Organization** list, select the required organization.
5. **Enter User Name** and click **Submit**.
The Case Summary page appears.
6. Click the numerical Case ID in the **Case ID** column.
The Case page appears.
7. Scroll down the Case page.
8. At the end of the page:
 - a. Select the **Add User to exception list** option.
 - b. In the **From** and **To** fields, specify the date and time interval for which you want the user to be exempted from risk evaluation.
If you want to add the user to the list for a short duration (**12 Hours, 1 Day, 2 Days, 4 Days**), then you can select the **Predefined Duration** option.
 - c. Specify the **Reason** you are adding the user to the list.
9. When done, click **Save** to update your changes to the case.

While Handling an Inbound Customer Call

To add a user to the Exception User List:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Manage Inbound Calls** link to display the Manage Inbound Calls page.

4. From the **Select Organization** list, select the required organization.
The updated Manage Inbound Calls page appears.
5. **Enter User Name** and click **Submit**.
If you have configured accounts for the organization, you will be prompted to enter the user identifier. You can filter based on user name or the account type from the drop-down list.
The Manage Inbound Calls page is refreshed with the specified user's case information.
6. Scroll down the Manage Inbound Calls page.
7. At the end of the page:
 - a. Select the **Add User to exception list** option.
 - b. In the **From** and **To** fields, specify the date and time interval for which you want the user to be exempted from risk evaluation.
If you want to add the user to the list for a short duration (**12 Hours, 1 Day, 2 Days, 4 Days**), then you can select the **Predefined Duration** option.
 - c. Specify the **Reason** you are adding the user to the list.
8. When done, click **Save** to update your changes to the case.

How to Blacklist a Device

From this release, RA allows CSRs working on cases to mark devices as risky. CSRs can add a Device ID to a blacklist or remove Device IDs from the blacklist. This feature simplifies the process of maintaining Device ID blacklists. Currently, the process requires RA users to export data for all transactions marked as fraud and extract the Device IDs to maintain the list.

To blacklist a device:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Work On Cases** link.
The first case (in the order of the priority assigned to your cases) appears.
4. Click the icon next to the Device ID.
5. In the dialog box that appears, click **OK** to add the Device ID to the blacklist as shown.

User Name: NEW_USER_1234 (TESTORG) Next Action Date:

Case History:

Case Note: ADMIN updated the Case on 10/10/2014 12:50:51 (GMT).
Called the Cardholder - Cardholder cc d5tg
ADMIN updated the Case on 10/10/2014 11:48:53 (GMT).
Called the Cardholder - Cardholder cc

Case ID: 91642770

Alerts on this Case:

Mark Selected As	Fraud Type	Device ID	Merchant	Currency	Amount	Organization's Base Currency	Amount in Organization's Base Currency	Transaction Date
Undetermined	Unknown	55EbpY8IOQWshH4XBnuozL26MjldZCM3ONtoD+eRvQRDnVing=	SPICEJET	INR	42	USD	0.8568	10/10/2014 12:58

From: 9/9/2014 To: 10/13/2014 Show Transactions Hide Transactions

Case Status: INPROGRESS Queue: DEFAULT

Note: -- Select --

Additional Note:

Next Action Date(GMT): 10/13/2014 Hrs: 00 Mins: 00

Select User State: UNDEFINED

From: 10/13/2014 To: 10/23/2014

Predefined Duration: --Select--

add_to_blacklist

- When done, click **Save** to update your changes to the case.
The Device ID is added to the blacklist. The ID is highlighted on the Administration Console, as shown.

Device ID

pPIVYg7YI+SsTM8bgUpJCwG2ayJ+48E4Nz2YIrfVxRI8nQbvQ8nBcSikGe1pWwX4

black_listed_element

Similarly, to remove a device from blacklist you must click the icon next to a highlighted Device ID and click **OK** in the Remove from Blacklist dialog box.

Fraud Analysts Analyzing Transactions

Important! Only GAs, OAs, and Fraud Analysts (FAs) can analyze the user transactions for the organizations that are in their scope. The MA, UAs, and CSRs cannot perform this task.

Analyzing transactions is a multi-step process that can involve:

- Viewing Transactions Summary
- Viewing Case Details
- Viewing Similar Transactions and Viewing Related Transactions
- Marking Transactions for Further Investigation

While looking at all the transactions based on the criteria that you specified in the Transactions Summary page, if you locate one or more suspect transactions, then you can further look into the details of these transactions ([Viewing Case Details](#)). You can further locate a pattern by viewing similar transactions ([Viewing Similar Transactions](#) and [Viewing Related Transactions](#)). After you have analyzed the details and discovered patterns, you can mark suspect transactions for further investigation by the CSRs ([Marking Transactions for Further Investigation](#)).

How to View Transactions Summary

Transactions can be filtered based on two criteria:

- **Generic search criteria**, such as Organization, Channel, Card Number, Date and Time, Rule used, Merchant details, and Device details.
See [How to Search for Transactions Based on Search Criteria](#) for more details on this.
- **Transaction ID**, in addition to Organization and Channel information. You should use this method only if you know the correct Transaction ID.
See [How to Search for Transactions Based on Transaction ID](#) for more details on this.

[What are the Fields in the Transaction Summary Page](#) explains the fields that are displayed in a typical transaction summary.

How to Search for Transactions Based on Search Criteria

To search for transactions based on search criteria:

1. Ensure that you are logged in with proper credentials (GA, OA, or Fraud Analyst.)
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the **Analyze Transactions** link.
4. From the **Select Organization** list, select the organization whose data you want to filter in the report.

Note: When the administrator has access to multiple perspectives in the system, the **ALL ISSUERS** and **ALL ACQUIRERS** options are available in the **Select Organization** drop-down list. Otherwise, you see the **ALL** organizations option.

The Analyze Transactions page for criteria-based search appears.

5. From the **Select Channel** drop-down list, select the channel for which you want to view the transactions. Possible values are:
 - All Channels
 - Default
 - 3D Secure
 - ATM
 - POS
 - ECOM
 - IMPS Beneficiary
 - IMPS Remitter
6. Enter the user identification information. The field differs based on the channel configured for the organization, as follows:
 - Default, ATM, POS, ECOM: **Enter User Name**
 - 3D Secure: **Enter Card Number**
 - IMPS: **Enter User Name**

- Acquirer Organization ATM and POS: **Enter Terminal ID**

Note: If you selected **ALL ISSUERS**, **ALL ACQUIRERS**, or **ALL** organizations in Step 4, this field is not enabled.

If you do not specify any user details, then all the transactions for the specified **Organization** are displayed.

7. To filter the transactions based on specific criteria, perform either of the following steps:
 - a. Select the pre-defined date range based on which you want to filter the transaction data in the **Transaction Date From** and **To** fields
 - b. Select the **Last Transactions** option and then select the time interval (in minutes) for which you want to see the latest transactions that were performed.
8. From the **Risk Advice** list, select the advices based on which you would like to filter the data.
9. From the **Secondary Authentication Status** list, select the statuses based on which you would like to filter the data.
10. From the **Fraud Status** list, select the statuses based on which you would like to filter the data.
11. From the **Rule** list, select the rule based on which you would like to filter the transaction data.

Note: If you want to see the transactions for all rules that matched, then ensure that the default **All Rules** option is selected.
12. **(Only for 3D Secure)** Enter the merchant name in the **Merchant** field, and select the criteria (**Exact**, **Starts with**, **Ends with**, **Contains**) based on which you want to filter the transaction data.
13. Enter the **Device ID** of the device for which you would like to filter the transaction data.

Note: This field is displayed only if you selected an Issuer Organization.

14. Select **Decrypt Sensitive Information** if you want to display the data in clear text.
15. Click **Submit** to generate the Transactions Summary page.

You can export the information directly to a CSV file by clicking the **Export** button.
For a description of the fields on the Transactions Summary page, see [What Are the Fields in the Transaction Summary Page](#).

How to Search for Transactions Based on Transaction ID

To search for transactions based on Transaction ID:

1. Ensure that you are logged in with proper credentials (GA, OA, or Fraud Analyst.)
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the **Analyze Transactions** link.

4. From the **Select Organization** list, select the organization whose data you want to filter in the report.

Note: When the administrator has access to multiple perspectives in the system, the **ALL ISSUERS** and **ALL ACQUIRERS** options are available in the **Select Organization** drop-down list. Otherwise, you see the **ALL** organizations option.

5. Click **Switch to Transaction ID Based Search**.
The Analyze Transactions page for transaction ID based search appears.
6. From the **Select Channel** drop-down list, select the channel for which you want to view the transactions.
7. Enter the **Transaction ID** of the transaction that you want to analyze.
8. Select **Decrypt Sensitive Information** if you want to display the data in clear text.
9. Click **Submit** to generate the Transactions Summary page
You can export the information directly to a CSV file by clicking the Export button.

Note: You can view transactions specific to a channel by clicking the specific channel tabs.

For a description of the fields on the Transactions Summary page, see [What Are the Fields in the Transaction Summary Page](#).

What Are the Fields in the Transaction Summary Page

The following table describes the fields listed in the Transactions Summary page for the **Default** channel.

Fields	Description
Details	Click the detail link to look into the details of the transaction.
User Name	The name of the user performing the transaction.
Fraud Status	The fraud status of the case. This field can have one of the following statuses: <ul style="list-style-type: none">▪ Assumed Fraud▪ Assumed Genuine▪ Confirmed Fraud▪ Confirmed Genuine▪ Undetermined
Fraud Type	The type of fraud.
Country	Based on the IP Address, the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the purchase transaction.
Matched Rule	The rule that matched and for which RA flagged the transaction as risky.
Transaction Date	The timestamp when the transaction was performed.

Fields	Description
Risk Score	The overall risk score returned by RA for the corresponding transaction. This is a value between 0 and 100.
Risk Advice	<p>The action suggested by RA after evaluating the Risk Score of the transaction. The possible actions are:</p> <ul style="list-style-type: none"> ▪ ALLOW ▪ ALERT ▪ DENY ▪ INCREASE AUTHENTICATION
Device ID	The ID of the device used for the transaction.
Model Score	The risk score returned by the Model for the transaction. This is a value between 0 and 100.
Secondary Auth Status	If the Risk Advice is INCREASE AUTHENTICATION , then this column specifies the result of the additional authentication that your application returned as feedback to RA.
Account Type	<p>The account type associated with the transaction.</p> <p>This column is displayed only if you have configured account types for the organization.</p>
Rule Results	The result of all the rules for the transaction. The result is Y or N .
Account ID	If there is an account ID associated with the user, then this column specifies the account ID that was used to perform the transaction.
Device Type	The type of device involved in the transaction.
Transaction ID	The unique ID generated for each user transaction.
OS	The operating system on the device that was used to perform the transaction.
Browser	The browser that was used to perform the transaction.
Device ID Status	<p>The status of the Device ID:</p> <ul style="list-style-type: none"> ▪ READ: The Device ID was read from the device. ▪ NEW: The Device ID was assigned to the device. ▪ REVERSE LOOKUP: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
Action	<p>The type of transaction performed by the user, which can be:</p> <ul style="list-style-type: none"> ▪ Login ▪ Wire Transfer

Fields	Description
	<ul style="list-style-type: none"> Any other value that you specify through your application
AFPN Advice	Displays the AFPN advice if AFPN was invoked during the transaction or later.
Organization	<p>The organization to which the user belongs.</p> <p>Note: This field is displayed only if you selected ALL organizations in your search.</p>

The following table describes the fields listed in the Transactions Summary page for the **3D Secure** channel.

Fields	Description
Details	Click the detail link to look into the details of the transaction.
Card Number	The card number of the user performing the transaction.
Fraud Status	<p>The fraud status of the case. This field can have one of the following statuses:</p> <ul style="list-style-type: none"> Assumed Fraud Assumed Genuine Confirmed Fraud Confirmed Genuine Undetermined
Fraud Type	The type of fraud.
Country	Based on the IP Address, the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the purchase transaction.
Merchant	The merchant involved in the transaction.
Currency	The currency used in the transaction.
Amount	The total transaction amount.
Organization's Base Currency	The base currency defined for the organization.
Amount in Organization's Base Currency	The transaction amount converted to the organization base currency.
Matched Rule	The rule that matched and for which RA flagged the transaction as risky.
Transaction Date	The timestamp when the transaction was performed.
Risk Score	The overall risk score returned by RA for the corresponding transaction. This is a value between 0 and 100.
Risk Advice	<p>The action suggested by RA after evaluating the Risk Score of the transaction. The possible actions are:</p> <ul style="list-style-type: none"> ALLOW

Fields	Description
	<ul style="list-style-type: none"> ▪ ALERT ▪ DENY ▪ INCREASE AUTHENTICATION
Device ID	The ID of the device used for the transaction.
Model Score	The risk score returned by the Model for the transaction. This is a value between 0 and 100.
Secondary Auth Status	If the Risk Advice is INCREASE AUTHENTICATION , then this column specifies the result of the additional authentication that your application returned as feedback to RA.
Transaction Status	The status of the transaction.
Rule Results	The result of all the rules for the transaction. The result is Y or N .
Device Type	The type of device involved in the transaction.
Transaction ID	The unique ID generated for each user transaction.
OS	The operating system on the device that was used to perform the transaction.
Browser	The browser that was used to perform the transaction.
Device ID Status	<p>The status of the Device ID:</p> <ul style="list-style-type: none"> ▪ READ: The Device ID was read from the device. ▪ NEW: The Device ID was assigned to the device. ▪ REVERSE LOOKUP: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
Action	<p>The type of transaction performed by the user, which can be:</p> <ul style="list-style-type: none"> ▪ Login ▪ Wire Transfer ▪ Any other value that you specify through your application
AFPN Advice	Displays the AFPN advice if AFPN was invoked during the transaction or later.
Organization	<p>The organization to which the user belongs.</p> <p>Note: This field is displayed only if you selected ALL organizations in your search.</p>

The following table describes the fields listed in the Transactions Summary page for the **ATM** and **POS** channels.

Field	Description
Details	

	Click the detail link to look into the details of the transaction.
TXID	The unique ID generated for each transaction.
USERNAME/Terminal ID	The card number of the user performing the transaction (in the case of Issuer organizations) or the Terminal ID from where the transaction was performed (in the case of Acquirer organizations).
Fraud Status	The status of the fraud.
Fraud Type	The type of fraud.
Processing Code	A series of digits that describes the type of transaction and the accounts affected by the transaction.
PAN	Primary Account Number that indicates the valid cardholder account number.
Datetime Local Txn	The local time at the ATM from where the transaction originated.
Transaction Datetime	Time (Hours-Mins) extracted from the date/time when the ISO 8583 message was constructed in, represented in GMT/UTC.
Transaction Amount	Amount involved in the transaction.
Reversal Amount	Amount reversed during the transaction.
Action	<p>The type of transaction performed by the user, which can be:</p> <p>ATM:</p> <ul style="list-style-type: none"> ▪ WITHDRAWAL ▪ FINANCIALINQUIRY ▪ PINCHANGE <p>POS:</p> <p>PURCHASE</p>
Transaction Status	The status of the transaction.
Reversal Status	The status of the reversal transaction.
Transaction Action Code	The code assigned to the transaction action.
MTI	Message Type Identifier. This is a 4-digit field that classifies the high-level function of the ISO 8583 message (consisting of Message Version, Message Class, Message Function, and Message Origin).
Matched Rule	The rule that matched and for which RA flagged the transaction as risky.
Score	The overall risk score returned by RA for the corresponding transaction. This is a value between 0 and 100.
Merchant Category	Category code of the merchant involved in the transaction.

POS Entry Mode	Indicates the method used to enter the account number.
Acceptor Address	Address of the card acceptor.
Acceptor City	City from which the transaction originated.
Acceptor State	State from which the transaction originated.
Card Accept Country	The code identifying the country of the acquiring institution.
Acquirer Country	Country where the acquiring institution for the POS is located.
Acceptor Terminal Id	Code that identifies a card acceptor terminal or a POS.
Acceptor Id	ID of the card acceptor (merchant) operating the POS.
ACQ Bin	Acquirer BIN of the merchant where the transaction was made.
POS Condition Code	(Only POS) Indicates the transaction conditions at the POS.
RRN	Retrieval Reference Number that helps identify and track all messages related to a given cardholder transaction.
Response Code	The response to a request for a transaction.
Advice	The action suggested by RA after evaluating the Risk Score of the transaction. The possible values are: <ul style="list-style-type: none"> ▪ ALLOW ▪ ALERT ▪ INCREASEAUTH ▪ DENY
AFPN Advice	Displays the AFPN advice if AFPN was invoked during the transaction or later.
Organization	The organization to which the user belongs. Note: This field is displayed only if you selected ALL organizations in your search.

The following table describes the fields listed in the Transactions Summary page, specific to the **Beneficiary** and **Remitter** perspectives of the IMPS channel. All other fields are the same as those in ATM or POS channels.

Field	Description
Beneficiary Account Number	The bank account number of the Beneficiary. This field is applicable for transactions of type Person to Account (P2A). This value is a combination of IFSC-code and bank account number.
Beneficiary IMPSID	The user name used to identify the Beneficiary.
Beneficiary Mobile Number	The mobile number of the Beneficiary.

IMPS Mode	A 2-digit value that denotes the IMPS transaction type.
Remitter IMPSID	The user name used to identify the Remitter.
Remitter Mobile Number	The mobile number of the Remitter.

The following table describes the fields listed in the Transactions Summary page, specific to the ECOM channel. All other fields are the same as those in ATM or POS channels.

Field	Description
ECI Indicator	A 2-digit value that denotes how the eCommerce transaction was authenticated.
Shopper country	The shopper's country.

How to View Case Details

The Transactions Summary page can also be used to view details of any specific transaction or case.

To view details of a specific case, in the Transactions Summary page, click the required **detail** link in the corresponding **Details** column. The transaction details are displayed on the resulting (Transaction Details) page. This page lists the details of the selected transaction, and also allows you to further filter transactions on the basis of available parameters.

The following table describes the fields listed in the Transaction Details page.

Fields	Description	
Basic Transaction Details (Default and 3D Secure)		
Transaction ID	The unique identifier of the transaction.	
Transaction Date	The timestamp when the transaction was performed.	
Action	The type of transaction performed by the user, which can be: <ul style="list-style-type: none"> ▪ Login ▪ Wire Transfer ▪ Any other value that you specify through your application 	
User Name	(Only Default) The name of the user who performed the transaction.	
Card Number	(Only 3D Secure) The card number of the user who performed the transaction.	
Fraud Status	The current status of the fraud. Possible values are: <ul style="list-style-type: none"> ▪ Undetermined 	

Fields	Description	
	<ul style="list-style-type: none"> Assumed Fraud Assumed Genuine Confirmed Fraud Confirmed Genuine 	
Device ID	The ID of the device used for the transaction.	
Risk Advice	<p>An action suggested by the Risk Assessment module after evaluating the risk score of the selected transaction. The possible actions are:</p> <ul style="list-style-type: none"> ALLOW ALERT DENY INCREASEAUTH 	
Matched Rule	The rule that matched and for which RA flagged the transaction as risky.	
Secondary Auth Status	If the Risk Advice is INCREASE AUTHENTICATION , then this column specifies the result of the additional authentication that your application returned as feedback to RA. The possible values are Success and Failure.	
Transaction Status	(Only 3D Secure) The status of the transaction.	
Model Score	The risk score returned by the Model for the transaction.	
Risk Score	The overall risk score returned by RA for the corresponding transaction. This is a value from 0 through 100.	
User State	<p>The state assigned to the user by the Customer Support Representative (CSR). Possible values are:</p> <ul style="list-style-type: none"> UNDEFINED Positive Suspect BlackListed 	
Basic Transaction Details (ATM and POS)		
TXID	The unique ID generated for each transaction.	
USERNAME/Terminal ID	The card number of the user performing the transaction (in the case of Issuer organizations) or the Terminal ID from where	

Fields	Description	
	the transaction was performed (in the case of Acquirer organizations).	
Fraud Status	The current status of the fraud. Possible values are: <ul style="list-style-type: none"> ▪ Undetermined ▪ Assumed Fraud ▪ Assumed Genuine ▪ Confirmed Fraud ▪ Confirmed Genuine 	
Transaction Amount	Amount involved in the transaction.	
Reversal Amount	The reversal amount involved in the transaction.	
Action	The type of transaction performed by the user, which can be: <p>ATM:</p> <ul style="list-style-type: none"> ▪ WITHDRAWAL ▪ FINANCIALINQUIRY ▪ PINCHANGE <p>POS:</p> <p>PURCHASE</p>	
Transaction Status	The status of the transaction.	
Reversal Status	The status of the reversal transaction.	
Matched Rule	The rule that matched and for which RA flagged the transaction as risky.	
Score	The overall risk score returned by RA for the corresponding transaction. This is a value between 0 and 100.	
Merchant Category	(Only POS) Category code of the merchant involved in the transaction.	
POS Entry Mode	(Only POS) Indicates the method used to enter the account number.	
Acquirer Country	Country where the acquiring institution for the POS is located.	
Acceptor Terminal ID		

Fields	Description	
	Code that identifies a card acceptor terminal or a POS.	
Acceptor ID	ID of the card acceptor (merchant) operating the POS.	
ACQ Bin	Acquirer BIN of the merchant where the transaction was made.	
POS Condition Code	Indicates the transaction conditions at the POS.	
Advice	The action suggested by RA after evaluating the Risk Score of the transaction.	
User State	The state assigned to the user by the Customer Support Representative (CSR). Possible values are: <ul style="list-style-type: none"> ▪ UNDEFINED ▪ Positive ▪ Suspect ▪ BlackListed 	
Other Transaction Details (Only 3D Secure)		
Merchant ID	Unique identifier of the merchant involved in the transaction.	
Merchant	Name of the merchant involved in the transaction	
Merchant URL	URL of the merchant involved in the transaction.	
Currency	The currency in which the transaction was performed.	
Amount	The total transaction amount.	
Organization's Base Currency	The base currency defined for the organization.	
Amount in Organization's Base Currency	The transaction amount converted to the organization base currency.	
Location Details (Only Default and 3D Secure)		
IP Address	The IP address of the system or device used for the purchase transaction.	
City	The city where the transaction was performed by the user.	
State	The state to which the user belongs.	
Country	The country to which the user belongs.	

Fields	Description	
Connection Type	<p>The connection type between the user's device and their Internet Service Provider. The possible values are:</p> <ul style="list-style-type: none"> ▪ Satellite ▪ OCX ▪ Frame Relay ▪ TX ▪ Dialup ▪ Cable ▪ DSL ▪ ISDN ▪ Fixed Wireless ▪ Mobile Wireless 	
Line Speed	The speed of the user's internet connection. This is based on the Connection Type.	
IP Routing Type	<p>The IP routing method used for the connection. The possible values are:</p> <ul style="list-style-type: none"> ▪ Fixed: Cable, DSL, OCX ▪ AOL: AOL users ▪ POP: Dial up to regional ISP ▪ Super POP: Dial up to multi-state ISP ▪ Cache Proxy: Accelerator proxy, content distribution service ▪ Regional Proxy: Proxy for multiple states in a country ▪ Anonymizer: Anonymizing proxy ▪ Satellite: Consumer satellite or backbone satellite ISP ▪ International Proxy: Proxy funneling international traffic ▪ Mobile Gateway: Mobile device gateway to Internet ▪ Unknown: Cannot currently be determined 	
Anonymizer Type	The type of anonymizer, if any, used for the connection. The possible values are:	

Fields	Description	
	<ul style="list-style-type: none"> ▪ Private: Anonymous proxies that are not publicly accessible. These type of anonymizers typically belong to commercial ventures. ▪ Active: Anonymous proxies that tested positive within the last six months. ▪ Suspect: Anonymous proxies that tested positive within the last two years, but not the last six months. ▪ Inactive: Anonymous proxies that did not test positive in the last two years. ▪ Unknown: Anonymous proxies for which no positive test results are currently available. 	
Risk Assessment Details		
MFP Match %	<p>The match percentage of the incoming Machine FingerPrint (MFP) with the value stored in the RA database.</p> <p>This is a numeric value.</p>	
User Known	<p>Whether the User Known rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Exception User Check	<p>Whether the Exception User Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Negative Country Check	<p>Whether the Negative Country Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. 	

Fields	Description	
	<ul style="list-style-type: none"> ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Device MFP Match	<p>Whether the Device MFP Match rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Trusted IP/Aggregator Check	<p>Whether the Trusted IP/Aggregator Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Untrusted IP Check	<p>Whether the Untrusted IP Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
User Velocity Check	<p>Whether the User Velocity Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
DeviceID Known	<p>Whether the Device ID Known rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. 	

Fields	Description	
	<ul style="list-style-type: none"> ▪ N/A: If the information was not available during risk evaluation. 	
Device Velocity Check	<p>Whether the Device Velocity Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Zone Hopping Check	<p>Whether the Zone Hopping Check rule matched. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
User Associated with DeviceID	<p>Whether the User-Device Association was found in the RA database. The possible values are:</p> <ul style="list-style-type: none"> ▪ Yes: If the rule matched. ▪ No: If the rule did not match. ▪ N/A: If the information was not available during risk evaluation. 	
Device Details		
Device Type	Type of device involved in the transaction.	
OS	The operating system on the device that was used to perform the transaction.	
Browser	The browser that was used to perform the transaction.	
Device ID Status	<p>The status of the Device ID:</p> <ul style="list-style-type: none"> ▪ READ: The Device ID was read from the device. ▪ NEW: The Device ID was assigned to the device. ▪ REVERSE LOOKUP: The Device ID was determined by matching the input 	

Fields	Description
	device signature against the device signatures that were successfully associated with the user.

How to View Similar Transactions

The small table at the end of the transaction details enables you to specify filter criteria to extract fine-grained data for similar transactions from the RA database.

Transactions can be further filtered on the basis of the following parameters:

- **Same User Name:** (Only Default) By selecting this option, you can extract all transactions that belong to the same user whose data you are currently viewing.
- **Same Device ID:** (Default and 3D Secure) By selecting this option, you can extract all transactions done by using the same device that is used for the current transaction details that you are viewing.
- **Same IP Address:** (Default and 3D Secure) By selecting this option, you can extract all transactions that have the same IP address as the current transaction details that you are viewing.
- **Same Card Number:** (Only 3D Secure) By selecting this option, you can extract all transactions that have been made using the same card number as the current transaction details that you are viewing.
- **Same Merchant:** (Only 3D Secure) By selecting this option, you can extract all transactions that have been made at the same merchant as the current transaction details that you are viewing.
- **Same PAN:** (Only ATM and POS for Issuer organizations) By selecting this option, you can extract all transactions that belong to the same PAN as the current transaction details that you are viewing.
- **Same Terminal ID:** (Only ATM and POS for Acquirer organizations) By selecting this option, you can extract all transactions that were performed from the same terminal as the current transaction details that you are viewing.
- **Transaction Date:** By specifying a date range (using the **From** and **To** fields), you can further filter all transactions that were performed in the specified time period.
- **Last Transactions:** By selecting the required time interval (in minutes), you can further filter all the latest transactions that were performed in the specified interval.

How to View Related Transactions

To view the related transactions:

1. In the Transaction Details page, select from the following options depending on the channel:

- Same User Name
 - Same Device ID
 - Same IP Address
 - Same Card Number
 - Same Terminal ID
 - Same Merchant
 - Same PAN
2. Perform either of the following steps:
 - Enter a date range in the **Transaction Date From** and **To** fields.
 - Select the **Last Transactions** option and then select latest time interval for which you want to see the related transactions.
 3. Click **Show**.

The Transactions Summary page appears, displaying the records that matched the criteria.

How to Mark Transactions for Further Investigation

After you have analyzed the details of suspect transactions or discovered patterns, you can mark suspect transactions for further investigation by the CSRs. To do so:

1. Ensure that you are logged in with the required privileges (GA, OA, or Fraud Analyst.)
2. Display the Transactions Summary page, as discussed in [How to View Transactions Summary](#).
3. Review the transactions that are displayed based on the criteria that you specified. See [How to View Case Details](#).
4. If you want to display similar patterns, follow the steps in [How to View Similar Transactions](#).
5. Scroll back to the Transactions Summary table.
6. Select the transactions that you suspect by selecting the check boxes corresponding to the transaction in the table.
7. Click the **Mark for Investigation** button to generate cases for the transactions you marked. These cases will now appear in the case lists for the CSRs to work on.

Managing Reports

Reports provide the business intelligence that you need to manage your end users and research high-risk events. Section, ["Summary of Reports Available to Administrators"](#) provides an at-a-glance summary of all reports that are available to the different administrators. As an administrator, the reports available to you are:

- [Administrator Reports](#)
- [Risk Analytics Reports](#)
- [Case Management Reports](#)

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

- Date Range
- Administrator Name
- Organizations
- User Name

Section, [Generating Reports](#) walks you through the generic process to generate activity reports for administrators and RA-specific reports.

You can also export all generated reports to a local file. See ["Exporting Reports"](#) for detailed instructions to do so.

Summary of Reports Available to All Administrators

The following table summarizes the reports in *all categories* (Administrator Reports, RA Reports, and Case Management Reports) that are available to *all administrators* in the system. These reports are then covered in detail in the following topics.

Administrator	Report Category		
Administrator Reports	RA Reports	Case Management Reports	
Master Administrator	My Activity Report	Instance Management Report	
	Administrator Activity Report		
	Organization Report		
Global Administrators	My Activity Report	Risk Evaluation Detail Activity Report	Case Activity Report

Administrator	Report Category			
	Administrator Activity Report	Risk Advice Summary Report	Average Case Life Report	
	User Activity Report	Exception User Report	Fraud Statistics Report	
	User Creation Report	Rule Configurations Report	Rule Effectiveness Report	
	Organization Report	Rules Data Report	False Positives Report	
		Device Summary Report	Reviewer Efficiency Report (Case Status)	
			Reviewer Efficiency Report (Fraud Status)	
			Rule Effectiveness(Fraud) Report	
Organization Administrators	My Activity Report	Risk Evaluation Detail Activity Report	Case Activity Report	
	Administrator Activity Report	Risk Advice Summary Report	Average Case Life Report	
	User Activity Report	Exception User Report	Fraud Statistics Report	
	User Creation Report	Rule Configurations Report	Rule Effectiveness Report	
	Organization Report	Rules Data Report Device Summary Report	False Positives Report	
User Administrators	My Activity Report	Risk Evaluation Detail Activity Report	Fraud Statistics Report	
	Administrator Activity Report	Risk Advice Summary Report	Rule Effectiveness Report	
	User Activity Report	Exception User Report	False Positives Report	
	User Creation Report			
Fraud Analysts	My Activity Report		Fraud Statistics Report	
	User Creation Report		Rule Effectiveness Report	

Administrator	Report Category	
		False Positives Report
Customer Support Representatives	My Activity Report	Exception User Report
	User Creation Report	

The following section explains in detail the reports that are in your purview.

Administrator Reports

In RA terminology, an *administrator* is someone who has the ability to log in to the Administration Console. Administrators then use reports to audit the activities they perform and the administrators in their purview perform. You access these reports from the **Administrator Reports** submenu under the **Reports** main menu.

All Administrator reports available in this category include:

- [My Activity Report](#)
- [Administrator Activity Report](#)
- [User Activity Report](#)
- [User Creation Report](#)
- [Organization Report](#)

My Activity Report

This report lists all operations performed by the current administrator. You use this report to list the actions and operations you have performed for the defined data range.

The following table explains the fields of this report.

Report Field	Description
Date	The date and time when the event was performed.
Administrator ID	The name of the administrator who is generating the report.
Administrator Organization	The name of the organization to which you are currently logged in as an administrator.
Transaction ID	The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to Transaction Server.

Report Field	Description
	<p>Note: You can use this ID to isolate information about a specific transaction in the log files.</p>
Event Type	<p>The type of administrator activity (such as, administrator login, view records, and update user and organization information) that you performed.</p> <p>Some possible event types are:</p> <ul style="list-style-type: none"> ▪ Search Users ▪ Search Organization ▪ Admin Login ▪ Update AdminProfile ▪ Set Preferred Locale ▪ Create Organization ▪ Create User ▪ Create Ruleset ▪ Create AccountType ▪ Get AccountType Details ▪ System and Organization Cache Refresh ▪ Set Organization Authentication Mechanism ▪ Migrating to Production ▪ View Report: <report name> ▪ Export Transaction Summary ▪ Update Global Password Policy ▪ Session Expired ▪ View Queue Status ▪ Show Next Case ▪ Add User to Exception List
Status	<p>The status of the transaction:</p> <ul style="list-style-type: none"> ▪ Success: If the action was completed successfully. ▪ Failure: If the administrator failed to complete the action.
Reason	The reason why the transaction failed.
User ID	If the transaction involved modification of user attributes, then this field specifies the name of the user whose attributes were updated or modified.
Target Organization	The name of the organization on which the activity was performed.
Component	<p>The system resource that was used to perform the task. The column values can be:</p> <ul style="list-style-type: none"> ▪ Administration Console ▪ Risk Analytics ResourcePack
Session ID	

Report Field	Description
	The unique numerical identifier created each time you log in to Administration Console. This session lasts until you log out.
Instance ID	If there are multiple instances of Transaction Server are running, then this field uniquely identifies the instance that you logged in to.
	Note: This data is used by CA Arcot Support personnel to diagnose problems.

Administrator Activity Report

This report lists all activities performed by a specified administrator, or by all administrators from a specified organization. Typically, Global Administrators use this report to monitor activity across organizations, while Organization Administrators use this report to monitor the activity within their organizations.

By using this report, administrators can view the activity in its entirety or drill down to a single administrator.

This report is most useful for Organization Administrators in managing the activity of their administrative team. It includes information, such as administrator login and logout timestamps, organization search, administrator account updates, and related details.

The fields of this report are the same as those of My Activity Report. See the table in [My Activity Report](#) for more information about the field details.

User Activity Report

A *user* is a generic term for an end user if RA is assessing risk in an Enterprise, eBanking, or ePortal application, or for a card holder in the case of an eCommerce and 3D Secure application.

The User Activity Report specializes in the reporting of activities performed on user attributes, which include creating users, updating users, setting Personal Assurance Messages (PAMs), deleting users, updating user status, and authenticating users.

The report contains details, such as user name, status of the user, type of operations performed, and also the IP address of the user system. Therefore, it is most applicable in the Enterprise or ePortal applications, where users are explicitly created by administrators before they are allowed access to protected resources. It is less applicable in case of eCommerce applications, where users are typically auto-created. Although it reports the type of activity, it gives you an idea of the rate of first-time transactions from cardholders.

To generate this report, you must specify:

- The **Date Range**.
- (Optional) The **User Name**.
- The required **Organization Name**.

The following table explains the fields of this report.

Report Field	Description
Date	The date and time when the event was performed.
User ID	The name of the user whose attributes were updated or modified.
Account Type	The account type associated with the organization to which the user belongs.
Account ID	The account ID of the user.
Event Type	The type of administrator activity (such as, administrator login, view records, and update user and organization information) that you performed.
Organization	The organization name to which the user belongs.
Status	The status of the operation: <ul style="list-style-type: none">▪ Success: If the operation was completed successfully.▪ Failure: If the user failed to complete the operation.
Transaction ID	The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to Transaction Server. Note: You can use this ID to isolate information about a specific transaction in the log files.
Reason	The reason why the Operation failed.
Client IP Address	The IP address of the end user's system.
Caller ID	The unique identifier set by the calling application. Note: The Caller ID can be blank if the calling application did not set the value.

User Creation Report

The User Creation Report displays details of the users created in the RA system.

To generate this report, you must specify:

- The **Date Range**.
- (Optional) The **User Name**.
- The required **Organization Name**.

The following table explains the fields of this report.

Report Field	Description
Date Created	The date and time when the user was created.
User ID	The name of the user who was created.
Organization	The organization name to which the user belongs.
User Status	<p>The status of the user:</p> <p>Active: If the user is an active user.</p> <p>Inactive: If the user is deactivated.</p> <p>Initial: If the user is created, but not yet activated.</p>
First Name	First name of the user.
Middle Name	Middle name of the user.
Last Name	Last name of the user.
Email Address	Email address of the user.
Telephone Number	Phone number of the user.

Organization Report

This report provides the details of all operations performed on the specified organization. Irrespective of any rules and configurations, this report displays *all* the activities in the organization under the administrator's purview.

To generate this report, you must specify:

- The **Date Range**.
- The **Organization Name**.

The following table explains the fields of this report.

Report Field	Description
Date	The date and time when the activity was performed.
Administrator ID	The name of the administrator who performed the activity.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	<p>The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to Transaction Server.</p> <p>Note: You can use this ID to isolate information about a specific transaction in the log files.</p>

Report Field	Description
Event Type	The type of administrator activity (such as, administrator login, view records, and update user and organization information) that you performed.
Status	<p>The status of the action taken:</p> <ul style="list-style-type: none"> ▪ Success: If the action was completed successfully. ▪ Failure: If the administrator failed to complete the action.
Reason	The reason why the operation failed.
User ID	If the transaction involved modification of user attributes, then this field specifies the name of the user whose attributes were updated or modified.
Target Organization	The organization to which the user belongs.
Component	<p>The resource that was used to perform the task. The column values are:</p> <p>Administration Console (Admin Console)</p> <p>Risk Analytics (Risk AnalyticsResourcePack)</p>
Session ID	The unique numerical identifier created each time you log in to Administration Console. This session lasts until you log out.
Instance ID	<p>In case there are multiple instances of Transaction Server are running, then this field uniquely identifies the instance that you logged in to.</p> <p>Note: This data is used by CA Arcot Support personnel to diagnose problems.</p>

Risk Analytics Reports

All the RA configuration-related reports available in the system include:

- [Risk Evaluation Detail Activity Report](#)
- [Risk Advice Summary Report](#)
- [Exception User Report](#)
- [Rule Configurations Report](#)
- [Rules Data Report](#)
- [Device Summary Report](#)

Risk Evaluation Detail Activity Report

This report displays *all* transactions performed by Transaction Server.

To generate this report, you must specify:

- The **Organization Name**.
- The **Channel**.
- The **User Identification**, if required.
This can be based on either the user name or account type.
- The **Date Range**.

The following table lists the information included in a Risk Evaluation Detail Activity.

Fields	Description
Date Logged	The timestamp when risk evaluation was performed for the user.
User Name	The unique ID of the user who performed the risk-evaluation activity.
Organization Name	The organization to which the user belongs.
Transaction Type	The type of risk-evaluation activity that was performed by Transaction Server. These activities include: <ul style="list-style-type: none">▪ Evaluate Risk▪ Update Attributes▪ Create Associations▪ Delete Associations
Status	The status of the event action taken and can be: <ul style="list-style-type: none">▪ Success: RA was able to perform the risk evaluation activity successfully.▪ Failure: RA was not able to perform the risk evaluation activity successfully.
Score	The score generated for the given transaction.
Advice ID	The advice generated by RA, depending on the score generated. The advice can be one of the following: <ul style="list-style-type: none">▪ Allow▪ Deny▪ Alert▪ Increase Authentication
Matched Rule	The rule that matched.
Secondary Authentication Result	The result of secondary authentication that was returned to RA by your application, if the Risk Advice generated by RA was "Increase Authentication".
Transaction Status	The status of the transaction.

Fields	Description
Configuration Name	The ruleset configured for the organization to which the user belongs.
Action	The corresponding action (for example, Login) that was performed for the current Event.
Caller ID	<p>A unique identifier passed to the RA APIs by your calling application.</p> <p>Note: Caller ID can be blank, if your calling application does not set the value.</p>
Transaction ID	<p>The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to Transaction Server.</p> <p>Note: You can use this ID to isolate information about a specific transaction in the log files.</p>
Session ID	The unique numerical identifier created each time you log in to Administration Console. This session lasts until you log out.
Instance ID	<p>If there are multiple instances of Transaction Server are running, then this field uniquely identifies the instance that you logged in to.</p> <p>Note: This data is used by CA Arcot Support personnel to diagnose problems.</p>
Country	<p>The country where the transaction originated.</p> <p>Note: This is derived from the Client IP Address value.</p>
Client IP Address	The IP address of the end user's system.
HTTP DeviceID	<p>Whether the HTTP Device ID was found on the user's end system.</p> <p>If the rule was applied, then the result (Yes or No) indicates whether the rule returned a match or not.</p>
Flash DeviceID	<p>Whether the Flash Device ID was found on the user's end system.</p> <p>If the rule was applied, then the result (Yes or No) indicates whether the rule returned a match or not.</p>
Outgoing DeviceID	The corresponding Device ID that was generated during the transaction, if this is the first transaction from the end user's system.
Device Type	The type of device involved in the transaction.
Device ID Status	<p>The status of the Device ID:</p> <ul style="list-style-type: none"> ▪ READ: The Device ID was read from the device.

Fields	Description
	<ul style="list-style-type: none"> NEW: The Device ID was assigned to the device. REVERSE LOOKUP: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
All Rules Result	The result of all rules applied.
	If a rule was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Account Type	The account type configured for the organization.
Account ID	The account ID of the user who performed the risk-evaluation activity.

Risk Advice Summary Report

The Advice Summary Report provides an overall summary of advices that were returned by the RA over the specified period of time. It also displays a separate table with the detailed summary of all the secondary authentication results.

Note: RA returns a risk advice for every transaction attempted by the user. Depending on the advice sent by RA, your application may allow the user to complete a transaction or deny the transaction.

To generate this report, you must specify:

- The **Date Range**.
- The **Channel**
- The **Organization Name**, if required.

The following table lists the information included in a RA Advice Summary Report:

Fields	Description
Channel	The channel on which the transaction was performed.
Allow	The total number of transactions for which RA generated the Allow advice.
Increase Authentication	The total number of transactions for which RA generated the Increase Authentication advice, and your application prompted the user for an additional authentication.
Alert	The total number of transactions for which RA generated the Alert advice.
Deny	The total number of transactions for which RA generated the Deny advice.

Fields	Description
Total	The total number of risk advices generated.

The following table lists the information included in a Secondary Authentication Results Summary Report:

Fields	Description
Channel	The channel on which the transaction was performed.
Success	The total number of all secondary authentication attempts that were successful.
Failure	The total number of all failed secondary authentication attempts by the user.
Undetermined	The total number of all instances when the result of the secondary authentication was not forwarded by your application to RA.
Total	The total number of secondary authentications performed, irrespective of the result generated.

Exception User Report

This report displays the list of all Exception users configured in the RA system.

To generate this report, you must specify:

- The **Date Range**.
- The required **Organization Name**.
- The **User Name**.

The following table lists the information included in a RA Exception Users Report:

Fields	Description
Start Date	The date and time from which the user is considered an exception user in the system.
End Date	The date and time when the user stops being an Exception User in the system.
User ID	The unique user identifier.
Reason	The reason for making the user an Exception User in the system.
Organization	The organization to which the administrator belongs.

Rule Configurations Report

The Rule Configurations Report displays the overall summary of all the rules deployed for an organization. To generate this report, you must specify:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Status** of the target information.

The following table lists the information included in a Rule Configurations Report.

Fields	Description
Rule Name	The name of the rule.
Enabled	Indicates whether the rule is enabled or not.
Priority	The priority of the rule.
Score	The score generated for the given transaction.
Advice	The advice generated by RA, depending on the score generated. The advice can be one of the following: <ul style="list-style-type: none"> ▪ Allow ▪ Deny ▪ Alert ▪ Increase Authentication
Rule Expression	The rule expression that is evaluated.
Channels	The channel for which the rule is deployed.
Actions	The actions that are permissible for the rule.
Rule Mnemonic	The short name of the rule.
Description	The description of the rule.

Rules Data Report

The Rules Data Report displays the summarized data for the selected list that has been uploaded for an organization.

To generate this report, you must specify:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Rulelist Type**.
- The uploaded **List** name.
- The **Status** of the target information.

Device Summary Report

This report displays the total number of transactions by device type and method of device ID determination.

To generate this report, you must specify:

- The required **Organization Name**.
- The **Channel**.
- The **Date Range**.

The following table lists the information included in a Device Summary Report.

Fields	Description
Device Type	The type of device from which the transaction originated.
DeviceID Read	Number of transactions where the Device ID was read from the device involved in the transaction.
New Device	Number of transactions where the Device ID was assigned to the device involved in the transaction.
Reverse Lookup	Number of transactions where the Device ID was recovered using the Reverse Lookup mechanism.
Total	Total number of transactions generated from a specific Device Type.

Case Management Reports

The Case Management module supports the reports explained in the following table.

Report	Description	Who Can Generate this Report
Case Activity Report	Displays the cumulative count of all cases that were opened, closed, or were acted upon (any other activity that was performed on cases) in a specified period of time. Note: This report is sorted by the Queues to which the individual cases belong, and by the CSR who worked on the cases.	<ul style="list-style-type: none">▪ GAs▪ OAs▪ Queue Managers
Average Case Life Report	Displays the statistics related to how long an average case lives in the system. In other words, it summarizes how much activity a case worker expends on a typical case.	<ul style="list-style-type: none">▪ GAs▪ OAs▪ Queue Manager

Report	Description	Who Can Generate this Report
	This report also displays how many cases were closed automatically because they timed out.	
Fraud Statistics Report	<p>Displays the overall statistics for each risk advice that RA generated in the specified time period.</p> <p>Note: Along with the Rule Effectiveness Report and the False Positives Report, this report helps the Fraud Analysts track the performance of their rule set as a function of time.</p>	<ul style="list-style-type: none"> ▪ GAs ▪ OAs ▪ UAs ▪ Fraud Analysts
Rule Effectiveness Report	<p>Displays what rules are firing so that Fraud Analyst can decide whether rules are working properly, if trend changes are observed, and if they need to be updated or deprecated.</p> <p>Note: Along with the Fraud Statistics Report and the False Positives Report, this report helps the Fraud Analysts track the performance of their rule set as a function of time.</p>	<ul style="list-style-type: none"> ▪ GAs ▪ OAs ▪ UAs ▪ Fraud Analysts
False Positives Report	<p>Displays the statistics on the ratio of transactions flagged by RA as suspicious, as compared to the number of transactions that are actually fraudulent.</p> <p>This report aids Fraud Analysts in evaluating the potential performance of deployed rules. This report shows the potential outcome of all rules, essentially reporting each of them independently.</p> <p>Note: Focusing on false-positives can prevent an organization from finding the right solution to stem its increasing fraud losses.</p>	<ul style="list-style-type: none"> ▪ GAs ▪ OAs ▪ UAs ▪ Fraud Analysts
Reviewer Efficiency Report (Case Status)	Presents a CSR-wise summary for the specified time duration by Case Status, and also provides CSR-wise transaction details.	GAs

Report	Description	Who Can Generate this Report
Reviewer Efficiency Report (Fraud Status)	Presents a CSR-wise summary for the specified time duration by Fraud Status, and also provides CSR-wise transaction details.	GAs
Rule Effectiveness(Fraud) Report	Presents a triggered rule-wise summary of transactions analyzed by fraud status.	GAs

The following topics explain the fields in these reports and walk you through the steps to generate these reports.

Case Activity Report

The Case Activity Report displays information related to the overall activity on cases in the system, as explained in the following table.

Field	Description
Cases Handled Through	<p>Specifies the Queue to which the case belongs. Typically, these cases are handled by Customer Service Representatives Working on Cases.</p> <p>The entries in the Inbound Calls row summarize the activity details for cases that were handled by Customer Service Representatives Handling Customer Calls.</p>
Period	<p>Indicates the period for which the report was generated. This report can be generated for the following periods:</p> <p>By Month</p> <p>Last 7 Days</p> <p>Yesterday</p> <p>By Date Range</p> <p>Note: You can see the day-to-day activity details for the period you specified by clicking the Down Arrow button.</p>
Cases Opened	Indicates the total number of new cases that were opened in the specified Period.
Cases Closed	Indicates the total number of existing cases that were closed in the specified Period.
Case Activity Count	Indicates the total number of activities that were performed on the cases in the specified Period.

Average Case Life Report

The Average Case Life Report displays information related to the average time it takes for a case to close in the system, as explained in the following table. These cases are grouped based on the fact whether the cases were closed manually (by a case worker) or automatically, through aging.

Field	Description
Cases Handled Through	<p>Specifies the Queue to which the case belongs. Typically, these cases are closed:</p> <p>By Customer Service Representatives</p> <p>or</p> <p>Automatically, because they timed out</p> <p>The entries in the Inbound Calls row summarize the activity details for cases that were handled by Customer Service Representatives Handling Customer Calls.</p>
Period	<p>Indicates the period for which the report was generated. This report can be generated for the following periods:</p> <ul style="list-style-type: none">▪ By Month▪ Last 7 Days▪ By Date Range
Cases Closed	<p>Indicates the total number of existing cases that were closed in the specified Period.</p>
Case Activity Count	<p>Indicates the total number of activities that were performed on the cases in the specified Period.</p>
Average Time Required for Case Closure	<p>Indicates the average time taken to close the cases in the system.</p>

Fraud Statistics Report

As explained in the following table, the Fraud Statics report displays statistics for each Risk Advice generated by RA in the specified time period.

Parameter	Description
Risk Advice	<p>Specifies the action suggested by RA after evaluating the risk of each transaction.</p> <p>The generated risk advice can be one of the following:</p> <ul style="list-style-type: none">▪ Allow▪ Alert▪ Increase Authentication▪ Deny

Parameter	Description
Fraud	Specifies the total number and percentage of all transactions that were reported by RA as fraudulent.
Genuine	Specifies the total number and percentage of all transactions that were considered genuine by RA.
Undetermined	Specifies the total number and percentage of all transactions for which RA did not have sufficient data to generate a risk advice.
Total	Specifies the total for all transactions for each "Risk Advice". It also specifies the overall Total .

Rule Effectiveness Report

Rule efficacy changes, and generally degrades with time. Fraudsters find new avenues of attack that circumvent the rules. The business evolves, opening new paths of access or commerce previously unprotected. System changes modify the meaning of data creating subtle downstream effects. For all these reasons, Fraud Analysts find that a major part of their job is the monitoring of the existing rule set. They can use this report to assess the effectiveness of the configured rules and their scores.

The Rule Effectiveness Report tabulates which rules established the outcome for the risk evaluation, as explained in the following table.

Parameter	Description
Rule Name	Lists the rules currently configured in the system.
Advice	Specifies the action suggested by RA after evaluating the risk of each transaction. The generated risk advice can be one of the following: <ul style="list-style-type: none"> ▪ Increase Authentication ▪ Alert ▪ Deny
Yesterday Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the last 24 hours of the report generation.
Last 7 Days Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the last 7 days of report generation.
Last 7 Days Daily Average	Specifies the average number of times the corresponding Rule Name was triggered in the last 7 days of report generation.

Parameter	Description
Last 30 Days Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the last 30 days of report generation.
Last 30 Days Daily Average	Specifies the average number of times the corresponding Rule Name was triggered in the last 30 days of report generation.

False Positives Report

The False Positives Report tabulates which rules established the outcome for the risk evaluation, as explained in the following table.

Parameter	Description
Rule Name	Lists the rules currently configured in the system.
Advice	Specifies the action suggested by RA after evaluating the risk of each transaction. The generated risk advice can be one of the following: <ul style="list-style-type: none"> ▪ Increase Authentication ▪ Alert ▪ Deny
Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the specified time period.
Fraud	Specifies the total number of all transactions for which the corresponding Rule Name generated a false positive result on fraudulent transactions.
Genuine	Specifies the total number of all transactions for which the corresponding Rule Name generated a false positive result on genuine transactions.
Undetermined	Specifies the total number of all transactions for which the corresponding Rule Name did not have sufficient data to generate a risk advice.

Reviewer Efficiency Report (Case Status)

As explained in the following table, the Reviewer Efficiency Report (Case Status) displays the summary for the specified time duration by Case Status for each CSR, and also provides CSR-wise transaction details.

Parameter	Description
Reviewer	The CSR handling the case.
Organization	The organization to which the case belongs.
Cases Skipped	The number of cases skipped by the CSR.

Cases Open	The number of cases remaining open in the specified time period.
Cases Closed	The number of cases closed by the CSR in the specified time period.
Cases OnHold	The number of cases kept on hold by the CSR in the specified time period.
Cases TimedOut	The number of cases that timed out in the specified time period because of CSR inactivity.
Cases Worked	The number of cases worked on by the CSR in the specified time period.
Unique Cases Handled	The number of unique cases handled by the CSR in the specified time period.

Reviewer Efficiency Report (Fraud Status)

As explained in the following table, the Reviewer Efficiency Report (Fraud Status) displays the summary for the specified time duration by Fraud Status for each CSR, and also provides CSR-wise transaction details.

Parameter	Description
Reviewer	The CSR handling the case.
Organization	The organization to which the case belongs.
Alerts Handled	The number of alerts reviewed by the CSR in the specified time period.
Marked Undetermined	The number of alerts that were marked Undetermined by the CSR in the specified time period.
Marked Confirmed Fraud	The number of alerts that were marked Confirmed Fraud by the CSR in the specified time period.
Marked Assumed Genuine	The number of alerts that were marked Assumed Genuine by the CSR in the specified time period.
Unique Txns Handled	The number of unique transactions handled by the CSR in the specified time period.
Unique Cases Handled	The number of unique cases handled by the CSR in the specified time period.
Confirmed	Percentage of alerts with fraud status marked as (Confirmed Fraud, Assumed Fraud, and Confirmed Genuine) over total alerts reviewed by the CSR.
Judgement	Percentage of alerts marked as Assumed Genuine over total alerts reviewed by the CSR.
Noncontactable	Percentage of alerts with Undetermined fraud status over total alerts reviewed by the CSR.

Rule Effectiveness (Fraud) Report

As explained in the following table, the Rule Effectiveness (Fraud) Report presents a triggered rule-wise summary of transactions analyzed by fraud status. This report runs for data prior to the last 14 days (current date - 14) with a date range of 7 days.

Note: For the Rule Effectiveness (Fraud) Report to show the updated data, the UPDATE_RULEEFFECTIVE_STATS procedure should be scheduled as a DB job to run once a day, during non-peak hours.

Parameter	Description
RuleMnemonic	The rule mnemonic that is configured for the rule.
Trigger Count	Number of transactions where the rule was triggered and hit.
Matched Count	Number of transactions where the transaction was alerted as a result of this rule being hit.
FSCountAssumedFraud	The number of transactions where the corresponding rule was hit and the transaction was marked "Assumed Fraud".
FSCountAssumedGenuine	The number of transactions where the corresponding rule was hit and the transaction was marked "Assumed Genuine".
FSCountConfirmedFraud	The number of transactions where the corresponding rule was hit and the transaction was marked "Confirmed Fraud".
FSCountConfirmedGenuine	The number of transactions where the corresponding rule was hit and the transaction was marked "Confirmed Genuine".
FSCountUndetermined	The number of transactions where the corresponding rule was hit and the transaction fraud status was undetermined.
FSCountUnknown	The number of transactions where the corresponding rule was hit and the transaction fraud status was unknown to the system.

Generating Reports

This topic covers:

- [Notes for Generating Reports](#)
- [How to Generate Reports](#)

Notes for Generating Reports

While generating reports, remember that:

- The administrator can *only* generate the reports of the organizations on which they have the scope.
- The administrator can generate the report of their subordinate or peers.
For example, an Organization Administrator (OA) can generate the reports of an OA and User Administrator (UA).
- If you are using Oracle database, then ensure that you have enabled the UNLIMITED TABLESPACE privilege.

How to Generate Reports

To generate any of the administrator- or RA-specific reports:

1. Ensure that you are logged in with proper credentials (MA, GA, OA, or UA.)
2. Activate the **Reports** tab in the main menu.
3. If you want to generate:
 - Administrator activity report, then click the **Administrator Reports** submenu.
 - RA-specific report, then click the **Risk Analytics** submenu.

The corresponding links for the report type appear in the left-handle task panel.

4. Based on the report you want to generate, click the required link from the left-hand submenu.

Note: RA allows you to choose to display either clear text data or encrypted data in Administrator Reports. For all Administrator Reports, select **Decrypt Sensitive Information** if you want to display the data in clear text in the report.

5. Specify one or more of the following criteria, as applicable, to view the report:
 - The **Date Range** from the drop-down list.
 - A pre-defined date range in the **From** and **To** fields.
6. Depending on the report, additionally you might have to specify the following:
 - **Organization Name** for the required organizations whose data you want to include in the report.
 - **User Name** (or **Administrator Name**), based on the report you want to generate:
 - Enter a user name (for User Activity reports.)

or

 - Enter the administrator name (for Administrator Activity reports.)
 - **Ruleset Name** for the required ruleset whose data you want to include in the report.

7. Click **Display Report** to generate the report based on the criteria you specified.

How to Export Reports

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

The exported reports are generated in the comma-separated value (CSV) format that can be viewed by using text editors and spreadsheet applications, such as Microsoft Excel. The export option is available through the **Export** button, which appears at the top-right of every rendered report.

To export a report to a local file:

1. Generate the required report. See "How to Generate Reports" for detailed instructions to do so.
The report opens.
2. Click **Export**.
You are prompted to save or open the report.
3. Click **Open (with)** or **Save (file)**. If you choose to save the report, then you must specify the download location.
This file can later be viewed by using the appropriate application.

How to Use the Report Download Tool to Export Reports

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.

This topic includes the following sub-topics:

- [Using the Tool](#)
- [List of Report Identifiers](#)
- [List of Report URLs](#)
- [Examples of Using the Tool](#)

Using the Tool

The arreporttool.jar file is available at the following location:

On Windows:

```
<install_location>\Arcot Systems\tools\common\arreporttool
```

On UNIX Platforms:

```
<install_location>/arcot/tools/common/arreporttool
```

Syntax:

Run the following command to see the help associated with the tool:

```
java -jar arreporttool.jar --help
```

Run the following command to use the tool:

```
java -jar arreporttool.jar - -protocol <protocol> --host <host>
--port <port_number> --admin-orgid <admin-organization>
--admin-id <admin-user-id> --admin-password <password>
[--report-type hour | day | month [duration] | range]
--report-id <Report ID> --reporturl <Url of the report>
--is-filter-req <true | false> --data-type <Data Type>
--reportdata [Report Data] --start-date-time <date-and-time> [--end-date-time
<date-andtime>] [--logfile <logfile>]
[--log-level <loglevel>][log-file-max-size] <logfilesize>] [--organizations <target
orgNames>] [--userName <User/Admin Name>] [--output-file <output-file>.CSV]
[--is-url-encoded [true|false]]
```

The following table describes the options supported by the tool.

Option	Description
protocol	The protocol that is used for communication. The possible values are http and https. The default protocol is http.
host	The host name or the IP address of the system where you have deployed Administration Console.
port	The port at which the console is listening.
admin-orgid	The organization to which the administrator belongs.
admin-id	The unique administrator ID.
admin-password	The administrator password.
report-type	Specify hour, day, month, or range. Hour, day, month can be followed by a numeric number. For example, --report-type day 2 indicates two days of records from the start-date-time is specified. Range: If range is specified, end-date-time is mandatory.
report-id	Identifier of the report to be fetched. See List of Report Identifiers for the list of report identifiers that you can use.
reporturl	Administrator URL of the report. See List of Report URLs for the list of report URLs that you can use.
is-filter-req	

Option	Description
	This is true by default. Set this value to false for reports that do not have a filter page, for example, RA reports.
data-type	This is applicable only for RA reports. This option specifies whether data type is ACTIVE or STAGING.
reportdata	In addition to start and end dates, certain reports need additional filters. These additional filters can be specified as report data. The report data must be in the 'key=value' format. You can use a semicolon to separate multiple key-value pairs. The report data must be URL-encoded if it contains ; or =. Ensure that you set the is-url-encoded parameter to true if an URL-encoded value is passed.
start-date-time	Specify the data or time after which report content must be fetched. Format: MM/dd/yyyy HH:mm:ss Hour (HH) and Minutes (mm) are optional and are used only for hourly reports. For daily and monthly reports, only the date part is used. Example: 03/21/2010 09:10:20
end-date-time	[Optional] Specify the end date and time till which report content should be selected.
logfile	[Optional] Specify the location of the log file. If no log file is specified, the file is automatically created in the current directory.
log-level	[Optional] Specify the log level. Default log level is INFO.
log-file-max-size	[Optional] Specify the maximum size of the log file. The default value is 10 MB.
organizations	[Optional] Specify semicolon-separated target organization names for the report. You <i>must</i> specify this value for reports that have organizations as a mandatory parameter. The value must be URL-encoded if the organization name contains a semicolon(;). Ensure that you set the is-url-encoded parameter to true if a URL-encoded value is passed.
userName	[Optional] Specify the user or administrator name.
output-file	

Option	Description
	[Optional] Specify the output file where the report content must be written. <reporttype>-timestamp.CSV is used.
is-url-encoded	[Optional] Set this value to true or false depending on whether your report data and organizations contain URL-encoded information. The default value is false.

List of Report Identifiers

The following table lists the report identifiers that you can use for the report-id argument.

Report	Report ID
My Activity Report	AAC.ViewMyActivityReport
Administrator Activity Report	AAC.ViewActivityReport
User Activity Report	AAC.ViewUserActivityReport
Organization Report	AAC.ViewOrgActivityReport
User Creation Report	AAC.ViewUserCreationReport

List of Report URLs

The following table lists the report URLs that you can use for the reporturl argument.

Report	Report URL
My Activity Report	/Ac_AdminMyActivity/view.htm
Administrator Activity Report	/Ac_Adminreport/view.htm
User Activity Report	/Ac_AdminUserActivity/view.htm
Organization Report	/Ac_AdminOrgActivity/view.htm
User Creation Report	/Ac_AdminUserCreation/view.htm

Examples of Using the Tool

To download the User Activity report:

```
java -jar arreporttool.jar --protocol http --host localhost --port 8080 arcot
--admin-id ga --admin-password gal23 --report-id AAC.ViewUserActivityReport
--report-url /Ac_AdminUserActivity/view.htm --startdate-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log ARCOT - -userName ua
```

To download the Organization report:

```
java -jar arreporttool.jar --protocol http --host localhost --port 8080 arcot
--admin-id ga --admin-password gal23 --report-id AAC.ViewOrgActivityReport -
report-url /Ac_AdminOrgActivity/view.htm --start-date-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log --organizations ARCOT;TEST
```