Arcot™ TransFort™

Issuer Software

Reports Manual

Version 6.4.5.

ARCOT™

455, West Maude Avenue, Sunnyvale, CA 94085-3517

TransFort Issuer Software—Reports Manual
Version 6.4.5.
Publication Date: March 2008
Part Number: AT060-007DW-6400000

Arcot Systems makes no warranty of any kind with regard to this manual. This includes, but is not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. Arcot Systems shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance or use of this material.

Trademarks

Arcot, the Arcot logo, WebFort, AccessFort, TransFort, ArcotID, and “Securing e-Business Anywhere” are all trademarks of Arcot Systems, Inc.

SecureCode and MasterCard are trademarks of MasterCard. 3–D Secure and Visa are trademarks of Visa International. Other trademarks are the property of their respective owners.

Patents

This software is protected by United States Patent No. 6,170,058, 6,209,102 and other patents pending.

Arcot Systems, Inc., 455, West Maude Avenue, Sunnyvale, CA 94085-3517.

Third Party Software

The following third-party software components have been packaged with the TransFort Issuer Software:

libcurl

OpenSSL

MSXML Parser 3.0

Tomcat

Provided by the Jakarta Project, Apache Software Foundation.

Contents

Preface

Welcome to the Arcot TransFort Issuer Software Reports Manual. This manual explains the reports generated in the 3-D Secure program (also known as SecureCode by MasterCard and Verified by Visa). This manual also provides instructions for viewing the reports and lists all the reports codes in its appendix. Interpretations of the reports are also provided whereever possible.

About This Manual

This section describes the intended audience for this manual and lists the chapters included in the manual.

Intended Audience

This manual is intended for CSRs, Global Administrators and Master Administrators who are responsible for viewing, interpreting and analysing the various reports generated by the Issuer Software. Many topics discussed in this manual are written for administrators who have the following skills: intermediate cryptography knowledge, experience with the applicable RDBMS, and familiarity with Web server administration.

Information Included in this Manual

This manual is organized as follows:

- Chapter 1, “Registration Reports”,, describes the various cardholder enrollment reports in the online authentication program. This includes the following reports:
  - Successful Registrations
  - Failed Registrations
  - Individual Registration Status
  - All Registrations by Date
  - Registration Statistics
  - ADS Statistics
  - Cardholders Added by Administrators
  - Deactivated Cards
  - Locked Cardholders
  - Expriring Cards
- Chapter 2, “Transaction Reports”,, describes the various cardholder transaction reports in the online authentication program. This chapter contains the following reports:
  - Successful Transactions

  - Failed Transactions
  - Transaction Statistics
  - Attempts Transactions
  - Verify Enrollment
- Chapter 3, “Issuer Reports”, describes the various Issuer level reports availabel in the Issuer Software. This chapter includes the following reports:
  - Issuer Configuration Summary
  - View All Issuers
  - Billing Information
- Chapter 4, “Administrator Reports”,, describes the various administrator reports available in the Issuer Software. This chapter includes the following reports:
  - CSR System Access Reports
  - Issuer Administrator System Access Reports
  - Global Administrator System Access Reports
- Appendix A, “Adding New Reports” describes how to add other custom reports to the Issuer Software.
- Appendix B, “Report Codes”, contains tables that list the codes that appear on some of the administrator reports.

Related Publications

This manual references the following documents:

Arcot TransFort Issuer Software Introduction Manual	This manual explains the online authentication program and how it is implemented using TransFort Issuer Software.
Arcot TransFort Issuer Software Installation Manual	This manual describes how to install and configure the Issuer Software according to the desired deployment environment.
Arcot TransFort Issuer Software System Administration sand Operations Manual	This manual contains information for setting up Issuer accounts, tuning, configuring and maitaining the Issuer Software. This manual also decribes the Administrator (CSR) operations.
Arcot Data Upload Client Installation and User Manual	This manual contains instructions for installing and using the Arcot Data Upload Client for TransFort. The Data Upload Client is used to automatically upload certain cardholder data into the Issuer Software Database.

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Click the **Add** button. The changes will be added to the database.
Italic	Key Words	The *Broadcast Service* must be started before the *Authentication Server*.
	Names of Publications	For more information, consult the *Arcot TransFort Issuer Software Installation Manual*.
	Emphasis	*Never* give anyone your PIN number.
`Fixed-width`	Command-line input or output	`# cd /opt/arcot`
	Code Samples	`./authproxy start`

	Text File Content	`[arcot/NetscapeCMS]`
		`host=tupelo.arcot.com`
		`endEntityPort=443`
		`endEntityPortUsesSSL=0`
		`agentPort=8100`

	File names	`arcot.ini`

`Italic fixed-width`	Variable text. Replace italic text with the appropriate substitution.	`# cd` *`install_directory`*
		`/Install.tgz`

	Variable portions of file names. Replace italic text with the appropriate substitution.	`init`*`ORACLE_SID`*`.ora`
Bold fixed-width	Emphasized code sample to highlight discussed topic.	sub gatewayError { my ($msg, $errorCod) =@_; **print"Content-type: text/html\n\n"** ...

What's new in version 6.4.5.

Arcot Transfort Issuer Software version 6.4.5. has the following new feature:

- Enhanced Issuer Configuration Summary report. This report now indicates if the User Id is supproted and if Two-Step-Login is enabled for a given cardholder.

Chapter 1

Registration Reports

Cardholder Enrollment Reports contain information specific to the cardholder's enrollment in the 3-D Secure program. This chapter contains information on the following Cardholder Enrollment Reports:

- Successful Registrations
- Failed Registrations
- Individual Registration Status
- All Registrations by Date
- Registration Statistics
- Cardholders Added by Administrators
- Deactivated Cards

Successful Registrations

The Successful Registrations report displays information on cardholders who have successfully enrolled in the 3-D Secure program in a given time period. This report displays the following information for each cardholder:

Table 1-1 Successful Registration Report fields

Report Field	Description
Issuer Name	The name of the Issuer.
Cardholder name	The cardholder's name.
Card number	The card number associated with the corresponding cardholder.
Email address	The cardholder's e-mail address.
Response Code*	A two-character code indicating the result of a $1 Authorization screening. See Appendix B, "Report Codes", for a list of possible values for this field.
AVS Result Code*	A one-character code indicating the result of a $1 Authorization AVS screening. See Appendix B, "Report Codes", for a list of possible values for this field.
CVV2/CVC2 Result Code*	A one-character code indicating the result of a $1 Authorization CVV2/CVC2 screening. See Appendix B, "Report Codes", for a list of possible values for this field.
Issuer Test Score*	A score based on the number of correct responses to the Issuer's identification questions.
Failed Question Ids	The question id's of the questions to which the cardholder gave an incorrect response. This field is present only when the cardholder's responses are evaluated.
Status (Enrollment)	A code indicating the status of the cardholder's enrollment. See "Cardholder Status Code,", for a list of possible values for this field.
Date Logged	The date the enrollment took place.

Table 1-1 Successful Registration Report fields

Report Field	Description
Registration Type	This column indicates the enrollment method of the cardholder. Possible values: • Self • Abridged • AutoEnroll • Upload • Custom AutoEnroll • Secondary AutoEnroll
Preferred Language	The cardholder's preferred language.
CallOut Status	The status returned by the callouts configured. If there are more than one callouts configured, all the status returned are logged separated by a delimiter. See the *Arcot TransFort Issuer Software System Administration and Operations Manual* for more information on configuring the delimiter.

**.These fields only display data if the Issuer account has been setup to use these verification methods. Otherwise, they will be blank.*

To view the Successful Registrations report:

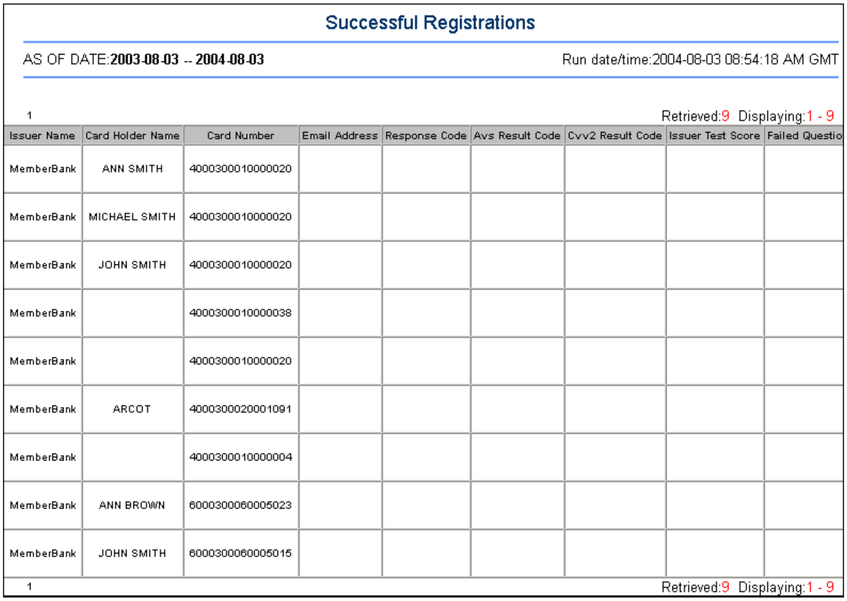
1. Click the **Successful Registrations** link.

   The *Successful Registrations* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Figure 1-1 Successful Registrations Report



Successful Registrations

AS OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 08:54:18 AM GMT

1 Retrieved:9 Displaying:1 - 9

Issuer Name	Card Holder Name	Card Number	Email Address	Response Code	Avs Result Code	Cvv2 Result Code	Issuer Test Score	Failed Questio
MemberBank	ANN SMITH	4000300010000020						
MemberBank	MICHAEL SMITH	4000300010000020						
MemberBank	JOHN SMITH	4000300010000020						
MemberBank		4000300010000038						
MemberBank		4000300010000020						
MemberBank	ARCOT	4000300020001091						
MemberBank		4000300010000004						
MemberBank	ANN BROWN	6000300060005023						
MemberBank	JOHN SMITH	6000300060005015						

1 Retrieved:9 Displaying:1 - 9

Failed Registrations

The *Failed Registrations* report displays all cardholders who were unable to successfully complete enrollment in a given period. See the **Table 1-1 "Successful Registration Report fields"** for a description of the information displayed by this report. There are two extra columns included in all the other Registration reports other than the Successful Registrations report:

Table 1-2 Failed Registrations Report Columns

After Num. Failed	This column is for cardholders who are configured for ADS method. This field indicates the number of times a cardholder failed authentication before failing registration.
Enrollment Steps	The different steps of the enrollment process are logged here. The steps are separated by |. Example: `CN|TERMS|ATTR|PWD|PG|` The possible values are: CN - Card number step TERMS - Accept Terms and Conditions step ATTR - Attributes step PWD - Setting password step PG - Choosing a Personal Greeting step.

To view the Failed Registrations report:

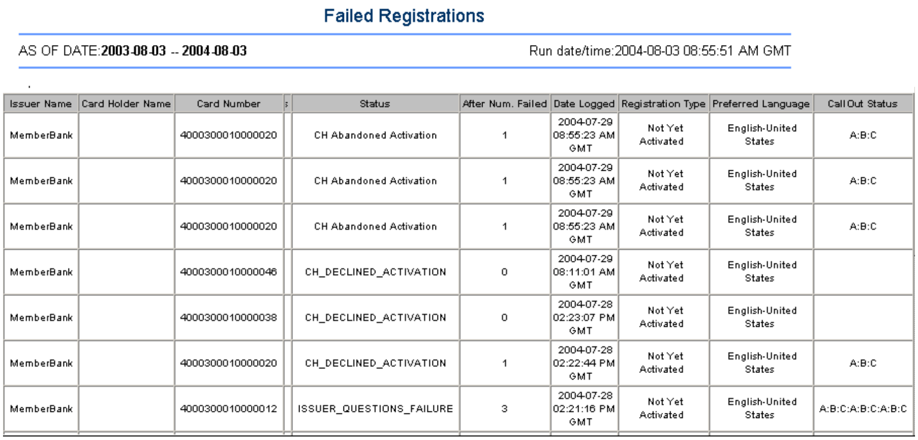
1. Click the **Failed Registrations** link.

   The *Failed Registrations* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Figure 1-2 Failed Registrations Report



Failed Registrations

AS OF DATE:**2003-08-03 -- 2004-08-03**	Run date/time:2004-08-03 08:55:51 AM GMT

Issuer Name	Card Holder Name	Card Number	:	Status	After Num. Failed	Date Logged	Registration Type	Preferred Language	Call Out Status
MemberBank		4000300010000020		CH Abandoned Activation	1	2004-07-29 08:55:23 AM GMT	Not Yet Activated	English-United States	A:B:C
MemberBank		4000300010000020		CH Abandoned Activation	1	2004-07-29 08:55:23 AM GMT	Not Yet Activated	English-United States	A:B:C
MemberBank		4000300010000020		CH Abandoned Activation	1	2004-07-29 08:55:23 AM GMT	Not Yet Activated	English-United States	A:B:C
MemberBank		4000300010000046		CH_DECLINED_ACTIVATION	0	2004-07-29 08:11:01 AM GMT	Not Yet Activated	English-United States	
MemberBank		4000300010000038		CH_DECLINED_ACTIVATION	0	2004-07-28 02:23:07 PM GMT	Not Yet Activated	English-United States	
MemberBank		4000300010000020		CH_DECLINED_ACTIVATION	1	2004-07-28 02:22:44 PM GMT	Not Yet Activated	English-United States	A:B:C
MemberBank		4000300010000012		ISSUER_QUESTIONS_FAILURE	3	2004-07-28 02:21:16 PM GMT	Not Yet Activated	English-United States	A:B:C:A:B:C:A:B:C

Individual Registration Status

The Individual Registration Status report displays enrollment information for a given card number. See Table 1-1 “Successful Registration Report fields” for a description of the information displayed by this report.

To view the Individual Registration Status report:

1. Click the **Individual Registration Status** link.

   The *Individual Registration Status* page appears.

2. Type the desired **card number** and click **Submit**.

   The system displays the report.

All Registrations by Date

The All Registrations by Date report displays a summary of all of the successful and failed enrollments in a given time period. The report includes all the columns in the Table 1-1 “Successful Registration Report fields” and Table 1-2 “Failed Registrations Report Columns”.

To view the All Registrations by Date report:

1. Click the **All Registrations by Date** link.

   The *All Registrations by Date* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Registration Statistics

The Registration Statistics report displays cardholder enrollment statistics for a given time period. This includes the number of activated and deactivated accounts, the number and a percentage of successful registrations, and failed registrations. It also provides a detailed break down of failed registrations. See "Cardholder Status Code," for a list of possible values for the failed registrations is field.

To view the Registration Statistics report:

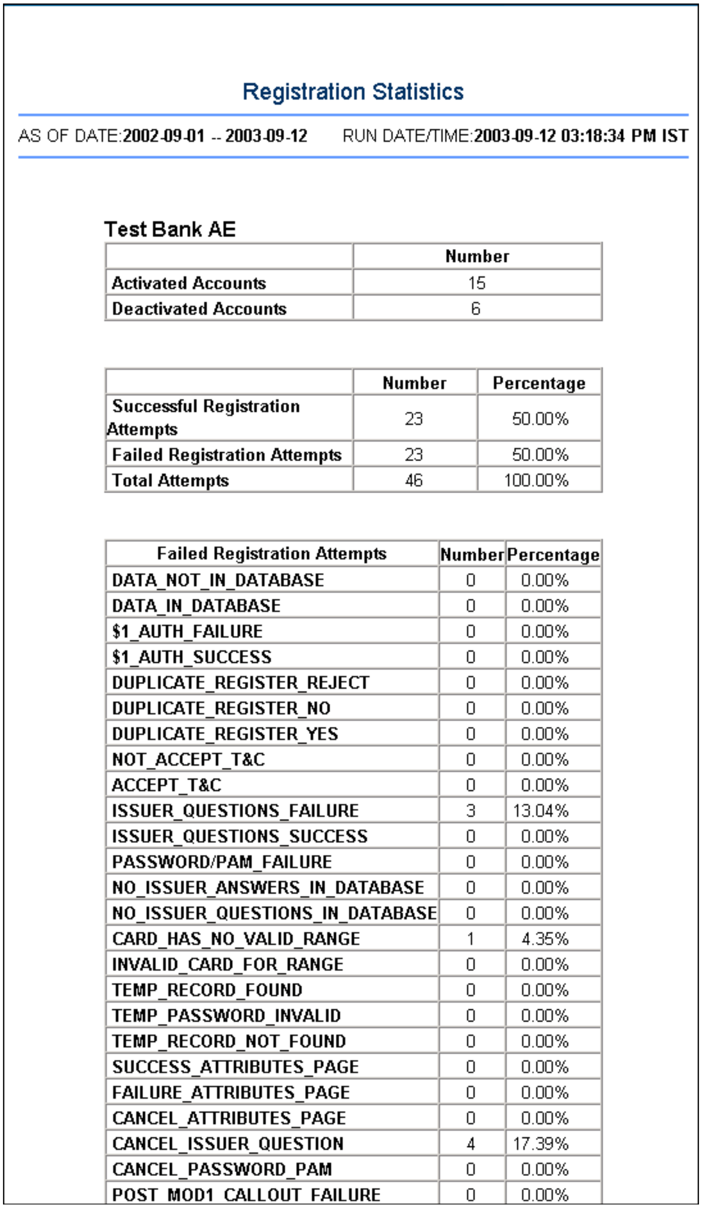
1. Click the **Registration Statistics** link.

   The *Registration Statistics* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Figure 1-3 Registration Statistics Report



Registration Statistics

AS OF DATE:**2002-09-01 -- 2003-09-12** RUN DATE/TIME:**2003-09-12 03:18:34 PM IST**

Test Bank AE

	Number
Activated Accounts	15
Deactivated Accounts	6

	Number	Percentage
Successful Registration Attempts	23	50.00%
Failed Registration Attempts	23	50.00%
Total Attempts	46	100.00%

Failed Registration Attempts	Number	Percentage
DATA_NOT_IN_DATABASE	0	0.00%
DATA_IN_DATABASE	0	0.00%
$1_AUTH_FAILURE	0	0.00%
$1_AUTH_SUCCESS	0	0.00%
DUPLICATE_REGISTER_REJECT	0	0.00%
DUPLICATE_REGISTER_NO	0	0.00%
DUPLICATE_REGISTER_YES	0	0.00%
NOT_ACCEPT_T&C	0	0.00%
ACCEPT_T&C	0	0.00%
ISSUER_QUESTIONS_FAILURE	3	13.04%
ISSUER_QUESTIONS_SUCCESS	0	0.00%
PASSWORD/PAM_FAILURE	0	0.00%
NO_ISSUER_ANSWERS_IN_DATABASE	0	0.00%
NO_ISSUER_QUESTIONS_IN_DATABASE	0	0.00%
CARD_HAS_NO_VALID_RANGE	1	4.35%
INVALID_CARD_FOR_RANGE	0	0.00%
TEMP_RECORD_FOUND	0	0.00%
TEMP_PASSWORD_INVALID	0	0.00%
TEMP_RECORD_NOT_FOUND	0	0.00%
SUCCESS_ATTRIBUTES_PAGE	0	0.00%
FAILURE_ATTRIBUTES_PAGE	0	0.00%
CANCEL_ATTRIBUTES_PAGE	0	0.00%
CANCEL_ISSUER_QUESTION	4	17.39%
CANCEL_PASSWORD_PAM	0	0.00%
POST_MOD1_CALLOUT_FAILURE	0	0.00%

Cardholders Added by Administrators

The Cardholders Added by an Administrator Report displays information about cardholders who were added to the system using the Abridged Enrollment method in a given time period.

To view the Cardholders Added by an Administrator report:

1. Click the **Cardholders Added by Administrator** link.

   The *Cardholders Added by an Administrator* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Deactivated Cards

The Deactivated Cards report displays information about cardholders who have cancelled their enrollment in the 3-D Secure program in a given time period.

To view the Deactivated Cards report:

1. Click the **Deactivated Cards** link.

   The *Deactivated Cards* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Chapter 2

Transaction Reports

The reports for online transactions are:

- Successful Transactions
- Failed Transactions
- All Transactions Report
- Transaction Statistics
- Attempts Transactions
- Verify Enrollment

Successful Transactions

The Successful Transactions report displays a list of all successful 3-D Secure transactions in a given time period. This report displays the following information for each transaction:

Table 2-1 Successful Transaction Report fields

Report Field	Description
Issuer name	The name of the Issuer.
Cardholder name **Card number**	The name and the card number of the cardholder.
Proxy PAN	A unique identifier of the card number. The value generated here is always the same for a card number.
Transaction Proxy PAN	Another identifier for the card number. There is a unique value generated for every transaction. This is the value sent in all the external communications instead of the actual card number.
Instance Id	The parameter determining the instance of the ACS from which this transaction originated.
Purchase XID	The XID is the transaction identifier that is generated by the merchant. This value along with the transaction proxypan is used to uniquely identify the transaction. The XID field is of the format : `Random number: Instance ID: Merchant XID.`
PARes Signing Time	The date and timestamp when the PARes is signed.
Authentication	The method used to identify the cardholder. The possible values are: • Core • Chip • Arcot Card • Hint • FYP • VIA
Currency	The currency used in the purchase.
Amount	The amount of the purchase.

Table 2-1 Successful Transaction Report fields

Report Field	Description
Merchant Name **Merchant URL** **Merchant ID** **Merchant Country**	All the details of the Merchant involved in the transaction. The name, URL, ID and country from which the Merchant submitted the transaction.
Device	The device used for the purchase.
ADS Parameters	This column is for cardholders who have completed their transactions in the ADS method.
After Num. Failed	This field indicates the number of times a cardholder failed authentication before completing the transaction.
After Num. Declines	This field indicates the number of times a cardholder declined to auto-enroll into the online authentication program before enrolling and completing the transaction.
Transaction Type	This indicates the type of transaction of the cardholder. The possible values are: • Regular • AutoEnroll. • ForgotPassword • SecondaryCardholder • ActivationAnyTime
Hex Encoded Transaction Proof	A calculated value used for dispute resolution. The hex encoded value of the transaction proof, which can be CAVV or AAV.
Base64 Encoded Transaction Proof	The base64 encoded value of the transaction proof, which can be CAVV or AAV.

To view the Successful Transactions report:

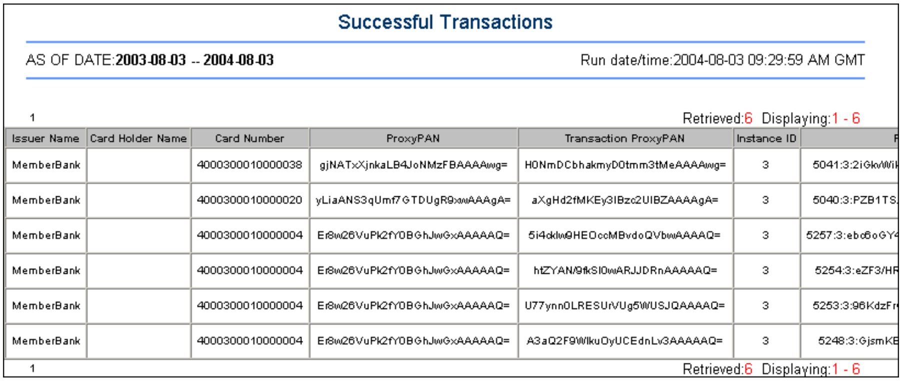
1. Click the **Successful Transactions** link

   The *Successful Transactions* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Figure 2-1 Successful Transactions Report



Successful Transactions

AS OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 09:29:59 AM GMT

1 Retrieved:6 Displaying:1 - 6

Issuer Name	Card Holder Name	Card Number	ProxyPAN	Transaction ProxyPAN	Instance ID	F
MemberBank		4000300010000038	gjNATxXjnkaLB4JoNMzFBAAAAwg=	H0NmDCbhakmyD0tmm3tMeAAAAwg=	3	5041:3:2iGkvWik
MemberBank		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	aXgHd2fMKEy3IBzc2UIBZAAAAgA=	3	5040:3:PZB1TS.
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	5i4dklw9HEOccMBvdoQVbwAAAAQ=	3	5257:3:ebc6oGY4
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	htZYAN/9fkSI0wARJJDRnAAAAAQ=	3	5254:3:eZF3/HR
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	U77ynn0LRESUrVUg5WUSJQAAAAQ=	3	5253:3:96KdzFr
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	A3aQ2F9WlkuOyUCEdnLv3AAAAAQ=	3	5248:3:GjsmKE

1 Retrieved:6 Displaying:1 - 6

Failed Transactions

The Failed Transactions report displays a list of all failed 3-D Secure transactions in a given time period. This report displays the following information for each transaction:

Table 2-2 Failed Transactions Report fields

Report Field	Description
Issuer Name	The name of the Issuer
Cardholder name	The name of the cardholder. This field can be empty if the cardholder name is not used.
Card number	The card number associated with the corresponding cardholder.
Proxy PAN	A unique identifier of the card number. The value generated here is always the same for a card number.
Transaction Proxy PAN	Another identifier for the card number. There is a unique value generated for every transaction. This is the value sent in all the external communications instead of the actual card number.
Instance Id	The parameter determining the instance of the ACS from which this transaction originated.
Purchase XID	The XID is the transaction identifier that is generated by the merchant. This value along with the proxypan is used to uniquely identify the transaction. The XID field is of the format : `Random number: Instance ID: Merchant XID.`
PARes Signing Time	The date and timestamp when the PARes is signed.
Authentication	The method used to identify the cardholder. The possible values are: • Core • Chip • Arcot Card • Hint • FYP • VIA
Currency	The currency used in the purchase.
Amount	The amount of the purchase.

Table 2-2 Failed Transactions Report fields

Report Field	Description
Merchant Name **Merchant URL** **Merchant ID** **Merchant Country**	All the details of the Merchant involved in the transaction. The name, URL, ID and country from which the Merchant submitted the transaction.
PwdInfo Status	This field indicates whether the transaction reached the password or OptIn page. Possible values are: • Successful • Failed • N/A - if the cardholder cancelled the transaction or the browser hanged before the page was displayed.
Verify Password Status	This field indicates whether the cardholder entered the password correctly. Possible values are: 1 - if the password is right. 0 - if the password is wrong N/A - Neither of the above two. The cardholder could have closed the password page or the internet link went down or the cardholder browser hangs at this time, etc. Basically the password is not entered in the page. So there is no verification of password done.
Hint Question Status	This field indicates whether the cardholder was asked to enter the response to the hint question
Verify Hint Answer Status	Indicates whether the cardholder's response to the hint question is correct. Possible values are: 1 - if the hint answer is right. 0 - if the hint answer is wrong N/A - Neither of the above two. The cardholder could have closed the hint answer page or the internet link went down or the cardholder browser hangs at this time, etc. Basically the response is not entered in the page. So there is no verification of hint answer done.
Transaction Status	Indicates the status of the transaction. Possible values are: • failed • unavailable

Table 2-2 Failed Transactions Report fields

Report Field	Description
CallOut Status	The status returned by the ACS CallOuts configured. If there are more than one callouts configured, all the status returned are logged separated by a delimiter. See the *Arcot TransFort Issuer Software System Administration and Operations Manual* for more information on configuring the delimiter.
Transaction Request Date	The date the purchase transaction was requested.
Device	The device used for the purchase.
After Num. Failed	This column is for cardholders who are configured for ADS. This field indicates the number of times a cardholder failed authentication before failing the transaction.
After Num. Declines	This field indicates the number of times a cardholder declined to auto-enroll into the online authentication program before failing the transaction.
Transaction Type	This indicates the type of transaction of the cardholder. The transaction can be either **Regular** or **AutoEnroll.**
Reason	This column summarizes the reason for which the transaction failed. See **Appendix B, "Report Codes"**, for possible values for this field.

To view the Failed Transactions report:

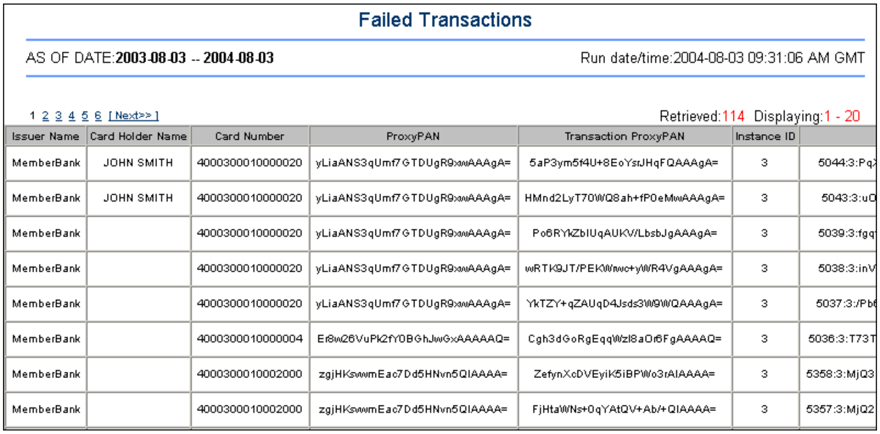
1. Click the **Failed Transactions** link.

   The *Failed Transactions* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Figure 2-2 Failed Transactions Report



Failed Transactions

AS OF DATE:**2003-08-03 -- 2004-08-03**

Run date/time:2004-08-03 09:31:06 AM GMT

1 2 3 4 5 6 [Next>>]

Retrieved:114 Displaying:1 - 20

Issuer Name	Card Holder Name	Card Number	ProxyPAN	Transaction ProxyPAN	Instance ID	
MemberBank	JOHN SMITH	4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	5aP3ym5f4U+8EoYsrJHqFQAAAgA=	3	5044:3:Pq
MemberBank	JOHN SMITH	4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	HMnd2LyT70WQ8ah+fP0eMwAAAgA=	3	5043:3:uO
MemberBank		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	Po6RYkZbIUqAUKV/LbsbJgAAAgA=	3	5039:3:fgq
MemberBank		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	wRTK9JT/PEKWwc+yWR4VgAAAgA=	3	5038:3:inV
MemberBank		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	YkTZY+qZAUqD4Jsds3W9WQAAAgA=	3	5037:3:/Pb
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	Cgh3dGoRgEqqWzl8aOr6FgAAAAQ=	3	5036:3:T73T
MemberBank		4000300010002000	zgjHKswmEac7Dd5HNvn5QIAAAA=	ZefynXcDVEyiK5iBPWo3rAIAAAA=	3	5358:3:MjQ3
MemberBank		4000300010002000	zgjHKswmEac7Dd5HNvn5QIAAAA=	FjHtaWNs+0qYAtQV+Ab/+QIAAAA=	3	5357:3:MjQ2

All Transactions Report

The All Transactions report displays a list of all 3-D Secure transactions in a given time period. This report displays the following information for each transaction:

Table 2-3 All Transactions Report fields

Report Field	Description
Issuer Name	The name of the Issuer
Begin Range	The first number of the card range for the card.
End Range	The last number of the card range for the card.
Business Id	The Bank Identification Number. The first six digits of a payment card account number that uniquely identifies the issuing financial institution.
Cardholder name	The name of the cardholder. This field can be empty if the cardholder name is not used.
Card number	The card number associated with the corresponding cardholder.
Proxy PAN	A unique identifier of the card number. The value generated here is always the same for a card number.
Transaction Proxy PAN	Another identifier for the card number. There is a unique value generated for every transaction. This is the value sent in all the external communications instead of the actual card number.
Instance Id	The parameter determining the instance of the ACS from which this transaction originated.
Purchase XID	The XID is the transaction identifier that is generated by the merchant. This value along with the proxypan is used to uniquely identify the transaction. The XID field is of the format : `Random number: Instance ID: Merchant XID.`
PARes Signing Time	The date and timestamp when the PARes is signed.
Authentication	The method used to identify the cardholder. The possible values are: • Core • Chip • Arcot Card • Hint • FYP • VIA

Table 2-3 All Transactions Report fields

Report Field	Description
Currency	The currency used in the purchase.
Amount	The amount of the purchase.
Merchant Name **Merchant URL** **Merchant ID** **Merchant Country**	All the details of the Merchant involved in the transaction. The name, URL, ID and country from which the Merchant submitted the transaction.
PwdInfo Status	This field indicates whether the transaction reached the password or OptIn page. Possible values are: • Successful • Failed • N/A - if the cardholder cancelled the transaction or the browser hanged before the page was displayed.
Verify Password Status	This field indicates whether the cardholder entered the password correctly. Possible values are: 1 - if the password is right. 0 - if the password is wrong N/A - Neither of the above two. The cardholder could have closed the password page or the internet link went down or the cardholder browser hangs at this time, etc. Basically the password is not entered in the page. So there is no verification of password done.
Hint Question Status	This field indicates whether the cardholder was asked to enter the response to the hint question
Verify Hint Answer Status	Indicates whether the cardholder’s response to the hint question is correct. Possible values are: 1 - if the hint answer is right. 0 - if the hint answer is wrong N/A - Neither of the above two. The cardholder could have closed the hint answer page or the internet link went down or the cardholder browser hangs at this time, etc. Basically the response is not entered in the page. So there is no verification of hint answer done.

Table 2-3 All Transactions Report fields

Report Field	Description
Transaction Status	Indicates the status of the transaction. Possible values are: • successful • failed • unavailable • Attempts
CallOut Status	The status returned by the ACS CallOuts configured. If there are more than one callouts configured, all the status returned are logged separated by a delimiter. See the *Arcot TransFort Issuer Software System Administration and Operations Manual* for more information on configuring the delimiter.
Transaction Request Date	The date the purchase transaction was requested.
Device	The device used for the purchase.
Verify Password Request Time	The timestamp when the password is authenticated.
Receipt Request Time	The time stamp when the ACS generated receipt is sent to the configured receipt server.
After Num. Failed	This column is for cardholders who are configured for ADS. This field indicates the number of times a cardholder failed authentication before failing the transaction.
After Num. Declines	This field indicates the number of times a cardholder declined to auto-enroll into the online authentication program before failing the transaction.
Transaction Type	This indicates the type of transaction of the cardholder. The transaction can be either **Regular** or **AutoEnroll.**
Reason	This column summarizes the reason for which the transaction failed. See Appendix B, "Report Codes", for possible values for this field.
Hex Encoded Transaction Proof	A calculated value used for dispute resolution. The hex encoded value of the transaction proof, which can be CAVV or AAV.
Base64 Encoded Transaction Proof	The base64 encoded value of the transaction proof, which can be CAVV or AAV.

To view the All Transactions report:

1. Click the **All Transactions** link.

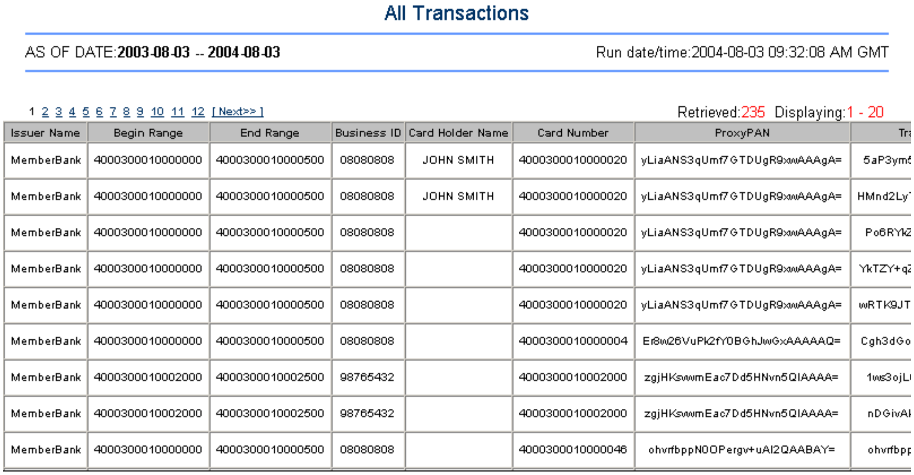
   The *All Transactions* page appears.

   NOTE:
   The global administrator should have the *Successful Transactions Report* privilege to view the All Transactions Report.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

Figure 2-3 All Transactions Report



All Transactions

AS OF DATE:**2003-08-03 -- 2004-08-03**   Run date/time:2004-08-03 09:32:08 AM GMT

1 2 3 4 5 6 7 8 9 10 11 12 [Next>>]   Retrieved:235 Displaying:1 - 20

Issuer Name	Begin Range	End Range	Business ID	Card Holder Name	Card Number	ProxyPAN	Tr
MemberBank	4000300010000000	4000300010000500	08080808	JOHN SMITH	4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	5aP3ym
MemberBank	4000300010000000	4000300010000500	08080808	JOHN SMITH	4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	HMnd2Ly
MemberBank	4000300010000000	4000300010000500	08080808		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	Po6RYk
MemberBank	4000300010000000	4000300010000500	08080808		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	YkTZY+q
MemberBank	4000300010000000	4000300010000500	08080808		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	wRTK9JT
MemberBank	4000300010000000	4000300010000500	08080808		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	Cgh3dGo
MemberBank	4000300010002000	4000300010002500	98765432		4000300010002000	zgjHKswwmEac7Dd5HNvn5QIAAAA=	1ws3ojL
MemberBank	4000300010002000	4000300010002500	98765432		4000300010002000	zgjHKswwmEac7Dd5HNvn5QIAAAA=	nDGivA
MemberBank	4000300010000000	4000300010000500	08080808		4000300010000046	ohvrfbppN0OPergv+uAI2QAABAY=	ohvrfbpp

Interpreting Transaction Reports

The Transaction reports are interpreted from values of multiple columns in the report. The reason column summarizes the transaction and the password, hint status columns provides a better understanding of the process.

This following tables provides some common scenarios and their interpretation:

Table 2-4 ADS based Interpretations

Num Auth Failures	Transaction Type	Reason	Interpretation
More than zero	AutoEnroll	Abandoned/Cancelled	The cardholder abandoned ADS transaction after trying to authenticate. CallOut status column can provide more information about the authentication failure.
More than zero	Optin_Decline	AutoEnroll	The cardholder declined to Optin after trying to authenticate and failing. CallOut status column can provide more information about the authentication failure.
0	AutoEnroll	Abandoned	If the PwdInfoStatus = 1, then the cardholder abandoned the ADS transaction without trying to authenticate even once after the Optin window was displayed. This can also be true if the cardholder has popup killers installed.

Table 2-5 Password and Hint based Interpretations

VerifyPwd Status	HintQuestionStatus	VerifyHint AnswerStatus	Transaction Status	Interpretation
N/A	N/A	N/A	N/A	The cardholder abandoned the transaction when presented with the Password screen.

Table 2-5 Password and Hint based Interpretations

VerifyPwd Status	HintQuestionStatus	VerifyHint AnswerStatus	Transaction Status	Interpretation
N/A	N/A	N/A	Failed	Cardholder cancelled out when presented with the Password screen. ACS sent back a failed PARes to the merchant.
Failed	N/A	N/A	Failed	Cardholder failed to provide correct password. Hint/Answer not configured for the range. ACS sent back failed PARes to the merchant
Failed	Successful	N/A	N/A	Cardholder failed to provide correct password. ACS presented the Hint/Answer page. The cardholder abandoned the transaction at this page.
Failed	Successful	N/A	Failed	Cardholder failed to provide correct password. ACS presented the Hint/Answer page. The cardholder cancelled out on this page. ACS sent a failed PARes to the merchant.
Failed	Successful	Failed	Failed	Cardholder failed to provide correct password. ACS presented the Hint/Answer page. The cardholder failed to provide the correct Answer to Hint. ACS sent back failed PARes to the merchant.
Successful	N/A	N/A	Failed	Cardholder provided the correct password. ACS unable to send a successful PARes to the merchant (signing certificate failure likely).
Failed	Successful	Successful	Failed	Cardholder failed to provide correct password, but provided correct Answer to Hint. ACS was unable to sent a successful PARes to the merchant (signing certificate failure likely).

Transaction Statistics

The Transaction Statistics report displays the volume of transactions that occurred in a given time period. The report classifies the transactions according to the type of transaction (See "Transaction Type"). The transactions are further classified according to the status of the transaction. See "PARes Status Code" for more information.

The statistics are displayed as percentages, with the actual numbers in parentheses next to them. You can also view the transaction statistics for all the card ranges per Issuer.

1. Click the **Transaction Statistics** link.

   The *Transaction Statistics* page appears.

2. Choose the Issuer from the drop-down list and type the desired **From/To date range** and click **Submit**. To select multiple Issuers press and hold the **Ctrl** key while selecting the Issuers.

   The system displays the report.

3. The report displayed is a two level report. The first level summarizes the transactions for the Issuers selected.

   NOTE:
   The statistics are displayed as percentages, with the actual numbers in parentheses next to them.

4. When you click any Issuer name in the report, the second level of the report is displayed. This page displays statistics for all the card ranges for that particular Issuer.

5. The following table explains the different columns displayed in the report:

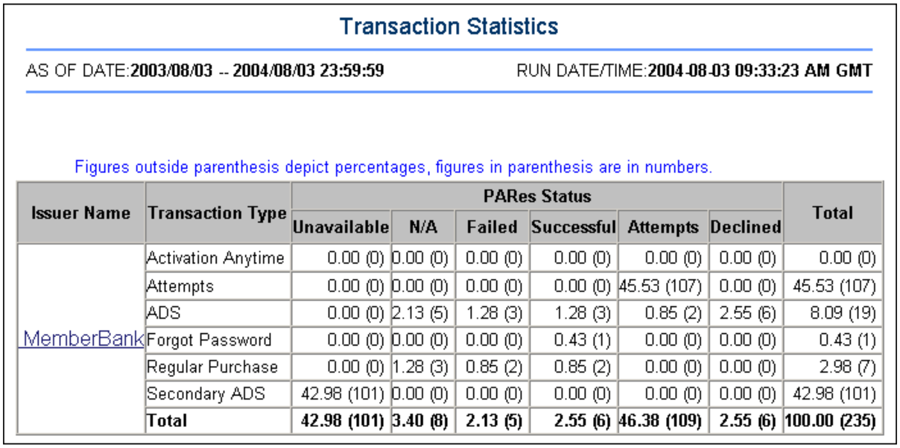
Table 2-6 Transaction Statistics Report

Report Field	Description
Issuer Name	The names of the Issuer selected for the report. This column is displayed in the first level of the report.
Card Ranges	The card ranges configured for the Issuer. This column is displayed only in the second level of the report, when you click on the Issuer name.
Transaction Type	The statistics are presented according to the following transaction types:
• Activation Anytime	Activation Anytime is a method of activating cardholders for the online authentication program. This is considered as a transaction without any amount exchanged.

Table 2-6 Transaction Statistics Report

Report Field	Description
• Attempts	This is a type of ADS, where the cardholders are not authenticated and the report can provide information of active online shoppers.
• ADS	The transactions which result from the Optin or Issuer Activation types of ADS are grouped together under this column.
• Forgot Password	When the cardholder is authenticated by the *Forgot Your Password* during transactions, the transaction type is set to Forgot Password.
• Regular Purchase	The regular transaction by a cardholder, where there is no ADS.
• Secondary ADS	The transaction where the secondary cardholder enrolls during ADS.
Transaction Status	The next six columns represent the transaction (PARes Status) status.
Unavailable	This is represented by the PARes status ‘U’. It means that the system was not available to authenticate the transaction.
N/A	This status is set when the PARes is not signed by the ACS. The PARes is not sent to the merchant, but the database is updated with this status.
Failed	This is represented by the PARes status ‘N’. This indicates a failed transaction.
Successful	This is represented by the PARes status ‘Y’. This indicates a successful transaction.
Attempts	This is represented by the PARes status ‘A’. This indicates that the range is configured for **Attempts** method of ADS.
Declined	This is represented by the PARes status ‘A’. This indicates that the range is configured for **Optin** method of ADS. The status indicates that the cardholder declined to optin to the ADS form of enrollment.
Total	The total number of transactions for the Issuer or card range.

Figure 2-4 Transaction Statistics Report - Level 1



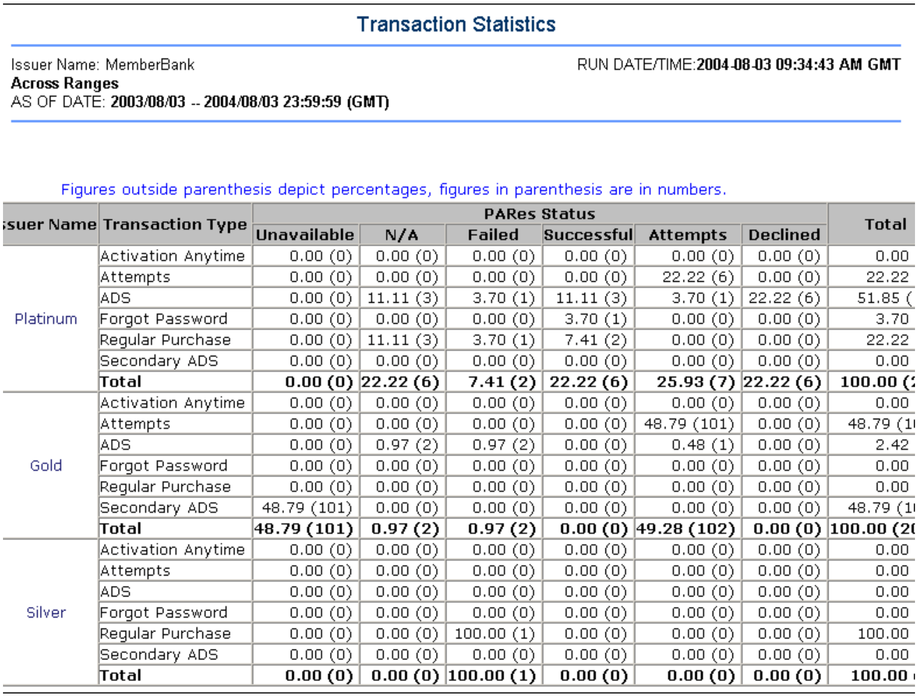
Transaction Statistics

AS OF DATE:**2003/08/03 -- 2004/08/03 23:59:59** RUN DATE/TIME:**2004-08-03 09:33:23 AM GMT**

Figures outside parenthesis depict percentages, figures in parenthesis are in numbers.

Issuer Name	Transaction Type	PARes Status						Total
		Unavailable	N/A	Failed	Successful	Attempts	Declined	
MemberBank	Activation Anytime	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)
	Attempts	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	45.53 (107)	0.00 (0)	45.53 (107)
	ADS	0.00 (0)	2.13 (5)	1.28 (3)	1.28 (3)	0.85 (2)	2.55 (6)	8.09 (19)
	Forgot Password	0.00 (0)	0.00 (0)	0.00 (0)	0.43 (1)	0.00 (0)	0.00 (0)	0.43 (1)
	Regular Purchase	0.00 (0)	1.28 (3)	0.85 (2)	0.85 (2)	0.00 (0)	0.00 (0)	2.98 (7)
	Secondary ADS	42.98 (101)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	42.98 (101)
	Total	**42.98 (101)**	**3.40 (8)**	**2.13 (5)**	**2.55 (6)**	**46.38 (109)**	**2.55 (6)**	**100.00 (235)**

Figure 2-5 Transaction Statistics Report - Level 2



Transaction Statistics

Issuer Name: MemberBank RUN DATE/TIME:**2004-08-03 09:34:43 AM GMT**
Across Ranges
AS OF DATE: **2003/08/03 -- 2004/08/03 23:59:59 (GMT)**

Figures outside parenthesis depict percentages, figures in parenthesis are in numbers.

suer Name	Transaction Type	PARes Status						Total
		Unavailable	N/A	Failed	Successful	Attempts	Declined	
Platinum	Activation Anytime	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Attempts	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	22.22 (6)	0.00 (0)	22.22
	ADS	0.00 (0)	11.11 (3)	3.70 (1)	11.11 (3)	3.70 (1)	22.22 (6)	51.85 (
	Forgot Password	0.00 (0)	0.00 (0)	0.00 (0)	3.70 (1)	0.00 (0)	0.00 (0)	3.70
	Regular Purchase	0.00 (0)	11.11 (3)	3.70 (1)	7.41 (2)	0.00 (0)	0.00 (0)	22.22
	Secondary ADS	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Total	**0.00 (0)**	**22.22 (6)**	**7.41 (2)**	**22.22 (6)**	**25.93 (7)**	**22.22 (6)**	**100.00 (**
Gold	Activation Anytime	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Attempts	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	48.79 (101)	0.00 (0)	48.79 (1
	ADS	0.00 (0)	0.97 (2)	0.97 (2)	0.00 (0)	0.48 (1)	0.00 (0)	2.42
	Forgot Password	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Regular Purchase	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Secondary ADS	48.79 (101)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	48.79 (1
	Total	**48.79 (101)**	**0.97 (2)**	**0.97 (2)**	**0.00 (0)**	**49.28 (102)**	**0.00 (0)**	**100.00 (2**
Silver	Activation Anytime	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Attempts	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	ADS	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Forgot Password	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Regular Purchase	0.00 (0)	0.00 (0)	100.00 (1)	0.00 (0)	0.00 (0)	0.00 (0)	100.00
	Secondary ADS	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00 (0)	0.00
	Total	**0.00 (0)**	**0.00 (0)**	**100.00 (1)**	**0.00 (0)**	**0.00 (0)**	**0.00 (0)**	**100.00**

Attempts Transactions

The Attempts Transactions Report displays all the transactions of the cardholders who have been configured for the Purchase Attempts type of ADS. The cardholders are not authenticated and the report can provide information of active online shoppers. This report also includes the transactions of cardholders who declined to activate themselves during ADS.

To view the Attempts Transactions report:

1. Click the **Attempts Transaction** link

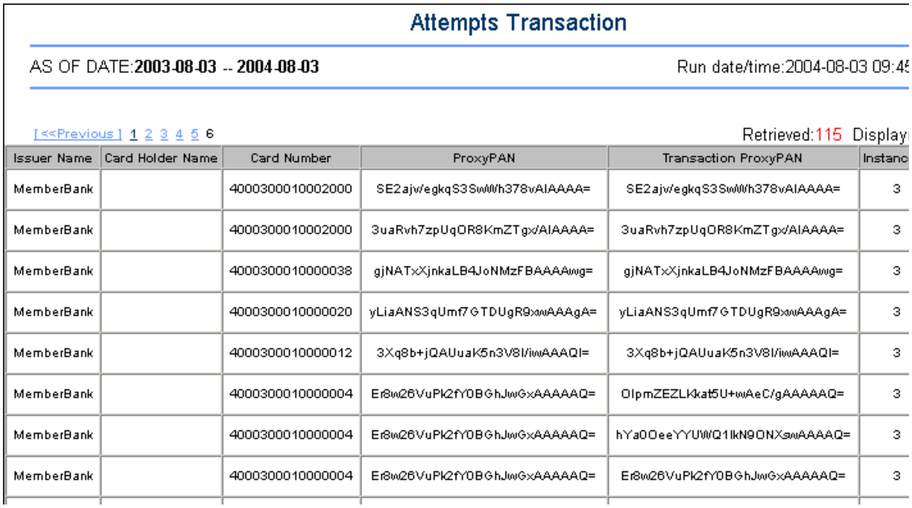
   The *Attempts Transaction* page appears.

2. Type the desired **From/To date range** and click **Submit**.

   The system displays the report.

3. The Table 2-3 explains the columns displayed in this report.

Figure 2-6 Attempts Transaction Report



Attempts Transaction

AS OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 09:4

[<<Previous] 1 2 3 4 5 6 Retrieved:115 Display

Issuer Name	Card Holder Name	Card Number	ProxyPAN	Transaction ProxyPAN	Instanc
MemberBank		4000300010002000	SE2ajv/egkqS3SwWh378vAIAAAA=	SE2ajv/egkqS3SwWh378vAIAAAA=	3
MemberBank		4000300010002000	3uaRvh7zpUqOR8KmZTgx/AIAAAA=	3uaRvh7zpUqOR8KmZTgx/AIAAAA=	3
MemberBank		4000300010000038	gjNATxXjnkaLB4JoNMzFBAAAAwg=	gjNATxXjnkaLB4JoNMzFBAAAAwg=	3
MemberBank		4000300010000020	yLiaANS3qUmf7GTDUgR9xwAAAgA=	yLiaANS3qUmf7GTDUgR9xwAAAgA=	3
MemberBank		4000300010000012	3Xq8b+jQAUuaK5n3V8I/iwAAAQI=	3Xq8b+jQAUuaK5n3V8I/iwAAAQI=	3
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	OIpmZEZLKkat5U+wAeC/gAAAAAQ=	3
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	hYa0OeeYYUWQ1lkN9ONXswAAAAQ=	3
MemberBank		4000300010000004	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	Er8w26VuPk2fY0BGhJwGxAAAAAQ=	3

Verify Enrollment

Arcot Transfort Issuer Software can log Verify Enrollment Requests (VEReqs) and Verify Enrollment Responses (VERes's) at a card range level. VEReqs and VERes's are sent during purchase transactions to check the enrollment status of a card number. A VEReq is sent from the Directory Server to the Access Control Server and the ACS sends the appropriate VERes to the DS.

A Global Administrator can view the Verify Enrollment Log if Verify Enrollment (VE) logging is enabled for an Issuer's card range(s). See the *Arcot TransFort Issuer Software System Administration and Operations Manual* for information on how to enable VE logging. The log displays all the VEReq's and VERes's logged during purchase transactions for the selected Issuer(s).

The columns in this report are listed in the following table:

Table 2-7 Verify Enrollment Log Report

Field Name	Description
Issuer Name	Name of Issuer.
DTD Version	The VEReq protocol version number.
Card Number	Card Number enrolled.
Proxy PAN	A unique identifier of the card number. The value generated here is always the same for a card number.
Transaction Proxy PAN	Another identifier for the card number. There is a unique value generated for every transaction. This is the value sent in the VERes instead of the actual card number.
Instance Id	The parameter determining the instance of the ACS from which this VE log originated.
Merchant ID	The Acquirer-defined Merchant ID for the purchase transaction corresponding to the cardholder's card number.
MerchantAcqBin	A 6-digit BIN assigned to the Acquirer by MasterCard or Visa.
Device Type	Indicates the type of the cardholder device. Possible values are: 0 for PC (HTML) 1 for mobile Internet device (WML)
User Agent	The exact content of the HTTP user-agent header as sent to the merchant from the cardholder's user agent.
HTTP Accept	The exact content of the HTTP accept header as sent to the merchant from the cardholder's user agent.

Table 2-7 Verify Enrollment Log Report

Field Name	Description
VEReq Time	The time at which the VEReq came to the ACS.
VERes Time	Time at which a corresponding VERes was sent from the ACS.
VERes Status	The status of the VERes. Possible values are: Y - Authentication Available N - Cardholder not participating U - Unable to authenticate.
IReq Code	An error code indicating the particular data which invalidates the VEReq. This field is included when the VEReq is syntactically correct, but business processing cannot be performed for some reason identified by the code. See **"Invalid Request Codes,"** in **Appendix B, "Report Codes"** for details of IReq Codes.
ACS URL	URL of the Access Control Server. Must be logged if the VERes Status is 'Y'.
Transaction Type	The type of enrollment of the cardholder. Possible values: • Regular • Attempts • AutoEnroll
PAReq Received	Indicates whether the PAReq was received after sending the VERes.

To view the Verify Enrollment Log report:

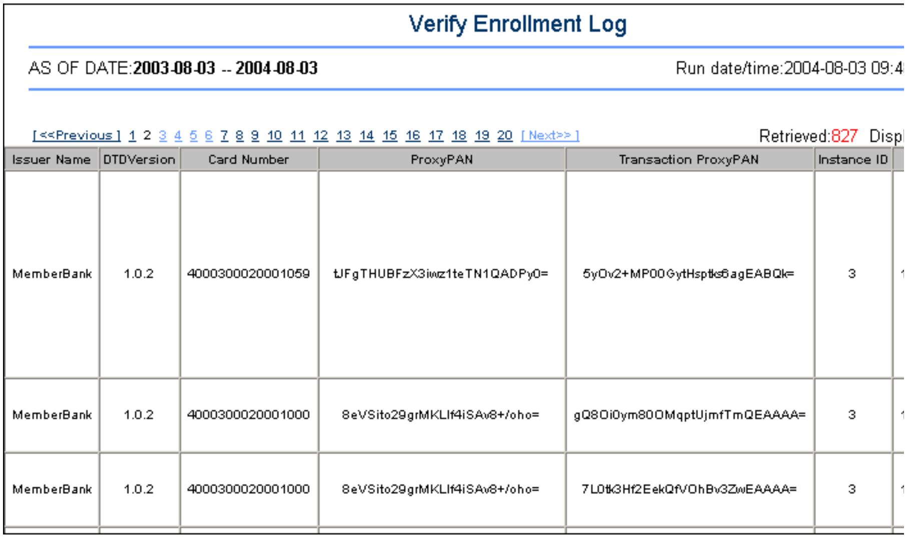
1. Click the **Verify Enrollment Log** link.

   The *Verify Enrollment Log* page appears.

2. Select **All Issuers** or a specific **Issuer**, type the desired **From/To date range**, and click **Submit**.

   The system displays the report.

Figure 2-7 Verify Enrollment Log Report



Verify Enrollment Log

AS OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 09:4

[<<Previous] 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next>>] Retrieved:827 Displ

Issuer Name	DTDVersion	Card Number	ProxyPAN	Transaction ProxyPAN	Instance ID	
MemberBank	1.0.2	4000300020001059	tJFgTHUBFzX3iwz1teTN1QADPy0=	5yOv2+MP00GytHsptks6agEABQk=	3	1
MemberBank	1.0.2	4000300020001000	8eVSito29grMKLIf4iSAv8+/oho=	gQ8Oi0ym80OMqptUjmfTmQEAAAA=	3	1
MemberBank	1.0.2	4000300020001000	8eVSito29grMKLIf4iSAv8+/oho=	7L0tk3Hf2EekQfVOhBv3ZwEAAAA=	3	1

Chapter 3

Issuer Reports

The reports described in this chapter are:

- Issuer Configuration Summary
- View All Issuers
- Billing Information

Issuer Configuration Summary

The Global administrator can view the configuration of an Issuer. The Issuer configuration report provides a detail summary of the selected Issuer's configuration parameters. The parameters are broadly classified into Issuer level parameters and range level parameters. The following sections discuss the report in more detail:

- Issuer Level Parameters
- Range Level Parameters
- Viewing the Issuer Summary Report

Issuer Level Parameters

The Issuer level parameters are mainly the ACS configuration values, all the levels of administrators in the system and the password policy set for the administrators. The table below explains the Issuer level parameters in the Issuer Configuration Report:

Table 3-1 Issuer Level Parameters

Parameter	Description
ACS Parameters	
Password Locking Enabled	Indicates if the cardholder password will be locked after n- failed tries.
Date Format	The date format selected for reports.
CVV/CVC2 Key A	The encrypted value of the CVK A of the CVK pair. This value is generated on the HSM and is the first value of the pair generated.
CVV CVC2 Key B	The encrypted value of the CVK B of the CVK pair. This value is generated on the HSM and is the second value of the pair generated.
CVV Key Indicator	An indicator to specify the CVV key pair used during periodic transition of CVV keys.
Issuer Parameters	
Locales Supported	This field lists all the locales the Issuer supports.
Encryption Key	The encryption key of the issuer which is used to encrypt the cardholder data in the database.
Temp Password Duration	The duration of the temporary password given to the cardholder.

Table 3-1 Issuer Level Parameters

Parameter	Description
ESIssuerDirName	The Issuer account directory.
Status	The status of the Issuer. The possible values can be: • Active • Disabled
Verification Algorithm	The verification algorithm used to calculate the CAVV/AAV values.
Processor Name	The name of the transactions processor for the Issuer.
Sub Processor Name	The name of the sub-processor for the Issuer.
Processor Data	Specific data about the processor for the Issuer.
Processor Info	Any Additional information about the processor.
User Id Supported	Indicates if the User Id is supported for the cardholder.
Two-Step Login	Indicates if Two-Step_Login is enabled/disabled for the cardholder.
Password Policy for Administrators	The different parameters for setting the administrators password policy. The report displays the following parameters: • Admin Level • Max Tries Per Session • Max Tries Across Sessions • Password Renewal Frequency • Max. Inactivity Period • Password Format Restriction
Administrators Associated with the Issuer	The report displays the user ID's of the different levels of system administrators associated with the selected Issuer.

Range Level Parameters

The Range level parameters displayed in the report are ACS url's, the begin and end for the range, FI BIN, ADS options, ES configuration values etc.

Displaying Range Group Configurations

In the range level parameters, the Range Group names to which the ranges are associated are displayed in parenthesis next to the range names. If the configuration is at the Range Group level, the field has a * as an indicator.

The table below explains the Issuer level parameters in the Issuer Configuration Report:

Table 3-2 Range Level Parameters

Parameter	Description
Range Details	
Id	The unique numerical identifier for the range generated by the system.
FI Bin	The 6-digit BIN identifier assigned to the Issuer by MasterCard.
Business ID	The 8-digit member identifier used to identify this Issuer.
Begin Range	The first card number within the range of cards you are setting up.
End Range	The last card number within the range of cards you are setting up.
Status	The status of the range. The possible values can be: • Enabled • Disabled
CVV/CVC2 Key A	The encrypted value of the CVK A of the CVK pair. This value is generated on the HSM and is the first value of the pair generated.
CVV CVC2 Key B	The encrypted value of the CVK B of the CVK pair. This value is generated on the HSM and is the second value of the pair generated.
CVV Key Indicator	An indicator to specify the CVV key pair used during periodic transition of CVV keys.
ACS URL 1	The URL for the primary ACS to be used for authentication.
Card Type	Specifies the type of cards that this card range covers. Possible values are: • Visa Credit Card • Visa Debit Card • MasterCard Credit Card • MasterCard Debit Card
SecureCode Key ID	MasterCard's BIN Key ID for the card range used for calculating the AAV's. Its a numeric value from 0 to 15.
SecureCode Key Alias	The alias string corresponding to the MC Key ID.
Branding URL 1	The location of the branding image file that is placed in image area 1 of the authentication page during a purchase.
Branding URL 2	The location of the branding image file that is placed in image area 2 of the authentication page during a purchase.

Table 3-2 Range Level Parameters

Parameter	Description
Receipt Server URL	The URL to the Receipt Server or AHS that complies with the 3-D Secure protocol version 1.0.1 and version 1.0.2 DTD (or 1.0 messaging).
ADS Option	The ADS method for the particular card range.
Max Declines	The number of times the cardholder can decline the Opt-in page to the online payer authentication program. See the *Arcot TransFort Issuer Software Introduction Manual* for more information.
Max Welcome	The number of times the cardholder views the Welcome page to the online payer authentication program. See the *Arcot TransFort Issuer Software Introduction Manual* for more information.
Cardholder Password Policy	The report displays the parameters which are set to determine the cardholder password policy for the range: • Hint Required • Minimum Length • Maximum Length • Minimum Numeric • Minimum Alphabets • Minimum Special Characters • Max Auth Tries • Max Auth Tries Across Sessions
Question Policy	The report displays the parameters which are set to determine the question policy for the range: • Minimum Correct Answers • Evaluation Approach
Questions	The questions that the Issuer has configured for the particular card range: • Question • Mandatory • Case Sensitive
ACS-CAP Folder Configuration	The locale and the ACS-CAP Folder Name corresponding to the locale.

Table 3-2 Range Level Parameters

Parameter	Description
CallOut Configuration	The different callout parameters like: • CallOut Type • Config Path • CallOut Configuration Id • Destination URL • Connection Time Out • Status
Adaptive ADS Configuration	If you have configured Adaptive ADS for the range, this column displays **Yes**. You use the link **Adaptive ADS Configuration** to view the actual rules for the range. See *Arcot TransFort Issuer Software System Administrations and Operations Manual* for more information.
Parameters Configured for Enrollment	The enrollment parameters configured for the card range. The parameters displayed are: • Enrollment Directory/Folder • Enrollment UI Template • Mini-Enrollment Directory/Folder • Mini-Enrollment UI Template • Address Verification Service (AVS) • CVV2/CVC2 check • $1 Auth Required (MIP/IPGS) • $1 Auth Required for Abridged (MIP/IPGS)

Viewing the Issuer Summary Report

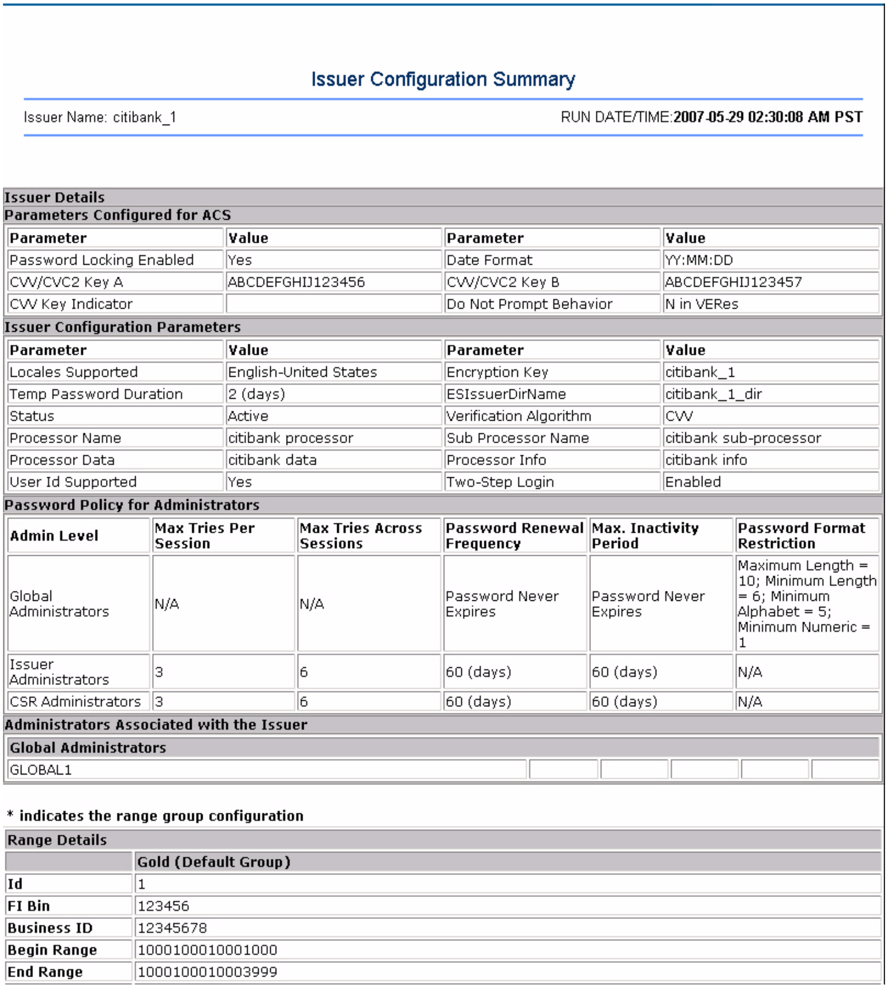
To view the Issuer Summary Report:

1. Click on the **Issuer Summary Report** link in the menu.
2. Choose the particular Issuer for whom you want to see the configuration report and click **Submit**.

   Select the **Range Details** check box if you want to view the range level details of the Issuer. Click Submit.

3. The system displays the *Issuer Configuration Summary*.

Figure 3-1 Issuer Configuration Summary Report



Issuer Configuration Summary

Issuer Name: citibank_1

RUN DATE/TIME:**2007-05-29 02:30:08 AM PST**

Issuer Details

Parameters Configured for ACS

Parameter	**Value**	**Parameter**	**Value**
Password Locking Enabled	Yes	Date Format	YY:MM:DD
CVV/CVC2 Key A	ABCDEFGHIJ123456	CVV/CVC2 Key B	ABCDEFGHIJ123457
CVV Key Indicator		Do Not Prompt Behavior	N in VERes

Issuer Configuration Parameters

Parameter	**Value**	**Parameter**	**Value**
Locales Supported	English-United States	Encryption Key	citibank_1
Temp Password Duration	2 (days)	ESIssuerDirName	citibank_1_dir
Status	Active	Verification Algorithm	CVV
Processor Name	citibank processor	Sub Processor Name	citibank sub-processor
Processor Data	citibank data	Processor Info	citibank info
User Id Supported	Yes	Two-Step Login	Enabled

Password Policy for Administrators

Admin Level	**Max Tries Per Session**	**Max Tries Across Sessions**	**Password Renewal Frequency**	**Max. Inactivity Period**	**Password Format Restriction**
Global Administrators	N/A	N/A	Password Never Expires	Password Never Expires	Maximum Length = 10; Minimum Length = 6; Minimum Alphabet = 5; Minimum Numeric = 1
Issuer Administrators	3	6	60 (days)	60 (days)	N/A
CSR Administrators	3	6	60 (days)	60 (days)	N/A

Administrators Associated with the Issuer

Global Administrators					
GLOBAL1					

*** indicates the range group configuration**

Range Details

	Gold (Default Group)
Id	1
FI Bin	123456
Business ID	12345678
Begin Range	1000100010001000
End Range	1000100010003999

View All Issuers

The View All Issuers Report provides a summary of all Issuer Accounts that have been added to the system. This report is a subset of the "Issuer Configuration Summary," described earlier in this chapter. This report includes the following information:

Table 3-3 View All Issuers Report fields

Field Name	Description
Issuer ID	The ID number assigned to the Issuer by the Issuer Software.
Issuer Name	The Issuer's name.
Country	The Issuer's country.
ESIssuerDirName*	The directory that contains the HTML pages and images used by the Issuer's Enrollment Server.
Hint Required?*	Whether or not a cardholder is required to enter a password hint during enrollment.
Password Locking?	Whether or not locking is enforced if a cardholder fails to enter the correct password a certain number of times.
Date Format	The date format used for the Issuer's cardholder password authentication page.
User Encoding	Language encoding of the Issuer's operating system (for example, ISO-8859-1)
IPGS Enabled*	Whether IPGS will be used during cardholder enrollment to verify the cardholder's identity.
Temp Password Duration (days)	The number of days for which a cardholder's temporary password is effective.
Encryption Key	The label of the Issuer encryption key created in the nCipher box.
Verification Algorithm*	The verification algorithm used to generate Cardholder Authentication Verification Values (CAVVs) that are included in a PARes.
CVV Key A*	The 16-digit encrypted value of the CVK A of the CVK pair. This value is generated on the HSM.
CVV Key B*	The 16-digit encrypted value of the CVK B of the CVK pair. This value is generated on the HSM.
Status	The status of the Issuer.
Dare Created	Date on which the Issuer was created.

Table 3-3 View All Issuers Report fields

Field Name	Description
Locales Supported	All the locales supported by the Issuer

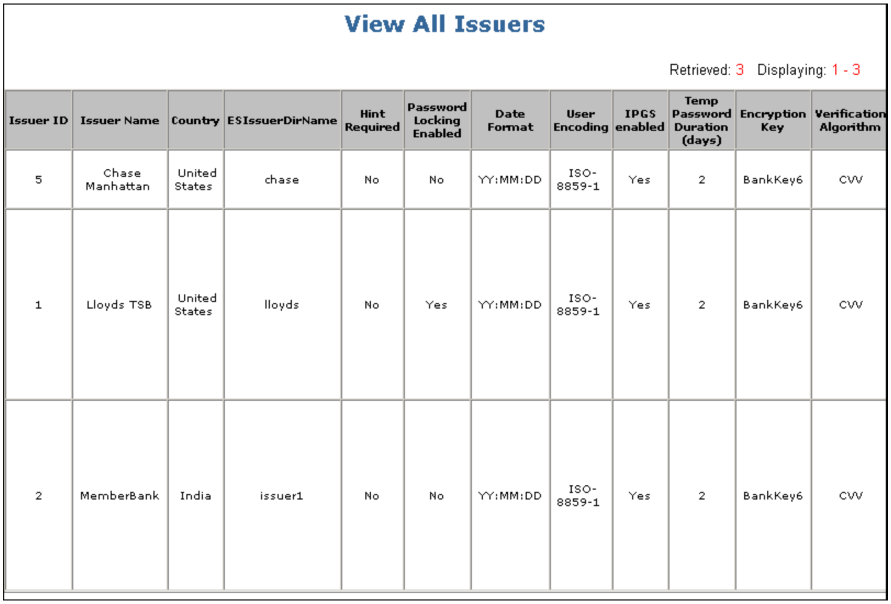
*. Applicable only in Visa configurations. Ignore these columns in MasterCard reports.

To view the View All Issuer Report:

- Click the **View All Issuers** link.

  The system displays the report.

Figure 3-2 View All Issuers Report



View All Issuers

Retrieved: 3 Displaying: 1 - 3

Issuer ID	Issuer Name	Country	ESIssuerDirName	Hint Required	Password Locking Enabled	Date Format	User Encoding	IPGS enabled	Temp Password Duration (days)	Encryption Key	Verification Algorithm
5	Chase Manhattan	United States	chase	No	No	YY:MM:DD	ISO-8859-1	Yes	2	BankKey6	CVV
1	Lloyds TSB	United States	lloyds	No	Yes	YY:MM:DD	ISO-8859-1	Yes	2	BankKey6	CVV
2	MemberBank	India	issuer1	No	No	YY:MM:DD	ISO-8859-1	Yes	2	BankKey6	CVV

Billing Information

A Global Administrator can view the Billing Information of Issuers report. The report takes an input of a calendar month (a number between 1 and 12), a calendar year (xxxx) and generates a report containing the following information:

Table 3-4 Billing Information Report

Field	Description
Calendar	Billing period.
Issuer Name	Name of the Issuer.
Issuer BIN	The six-digit BIN identifier assigned to the Issuer by MasterCard or Visa.
Successful Enrollments	Number of newly enrolled cards during the specified billing period for the particular Issuer.
Renewed Cardholders	Renewed cardholders are those who have completed one complete year after enrolling in the online authentication program. Number of renewed cardholders during the specified billing period for the particular Issuer.
Pre-Enrolled Cardholders	Number of pre-enrolled cardholders during the specified billing period for the particular Issuer. This represents the number of cardholders whose Issuer questions and answers are uploaded but who have not yet enrolled in he online authentication program.
Activated Cards	Number of active enrolled cards during the specified billing period for the particular Issuer.
Activated Cardholders	Number of active enrolled cardholders during the specified billing period for the particular Issuer.
Deactivated Cardholders	Number of cardholders deactivated during the specified billing period for the particular Issuer.
Not Activated Cardholders	This columns represents the number of cardholders that came into the system during the specified period but are not yet activated. This happens in cases such as: • Cardholder fails to authenticate during ADS • Cardholder declines/abandons to activate during ADS • Cardholder is uploaded in inactivated state
Processor Name	The name of the processor for the Issuer.
Sub Processor Name	The name of the sub-processor for the Issuer.

Table 3-4 Billing Information Report

Field	Description
Processor Data	Specific data about the processor for the Issuer.
Processor Info	Any additional information about the processor.
New Issuers	List of new Issuers.
Renewed Issuers	List of Issuers that have been on the service for a whole calendar year by the end of the specified billing period.

To view the Billing report:

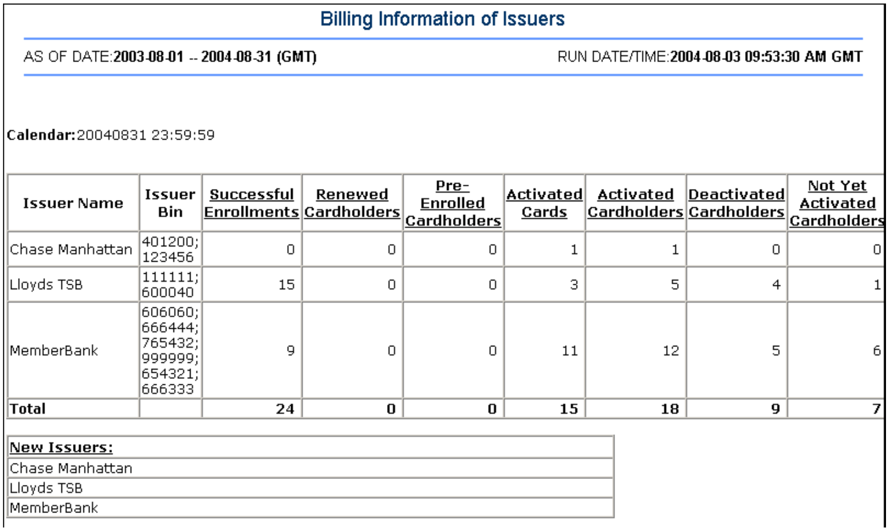
1. In the Administrative Console click the **Billing Information** link.

   The *Billing Information for Issuers* page appears.

2. Select the desired **From/To date range**, and click **Submit**.

   The system displays the report.

Figure 3-3 Billing Information



Billing Information of Issuers

AS OF DATE:**2003-08-01 -- 2004-08-31 (GMT)** RUN DATE/TIME:**2004-08-03 09:53:30 AM GMT**

Calendar:20040831 23:59:59

Issuer Name	Issuer Bin	Successful Enrollments	Renewed Cardholders	Pre-Enrolled Cardholders	Activated Cards	Activated Cardholders	Deactivated Cardholders	Not Yet Activated Cardholders
Chase Manhattan	401200; 123456	0	0	0	1	1	0	0
Lloyds TSB	111111; 600040	15	0	0	3	5	4	1

MemberBank	606060;
	666444;
	765432;
	999999;
	654321;
	666333
		9	0	0	11	12	5	6

Total		**24**	**0**	**0**	**15**	**18**	**9**	**7**

New Issuers:
Chase Manhattan
Lloyds TSB
MemberBank

Chapter 4

Administrator Reports

This chapter describes the reports which logs system access of all the administrators via the administrative console. All the administrator access to the Issuer Software system are recorded in two types of logs:

- Activities Log
- Report Access Log

The Issuer Administrator can view these reports to retrieve and display information about Administrators (CSRs) and Issuer Administrators system use.

You can choose to view a report online or export a report to a file to use in another software program.

> **NOTE:**
> This section provides instructions on how to view reports online. See the *Arcot TransFort Issuer Software System Administration and Operations Manual* for instructions on how to export a report.

The system displays reports according to the information set up in your Report Profile. See the *Arcot TransFort Issuer Software System Administration and Operations Manual* for information on how to change your Report Profile.

The reports according to the administration level fall into the following categories:

- Administrator (CSR) System Access Reports
- Issuer Administrator System Access Reports

This section describes the information contained in each report and provides instructions on how to access and view each report.

CSR System Access Reports

There are two reports that display information about Administrator (CSR) system access:

- Administrator Report Access Log
- Administrator Activities Log

Administrator Report Access Log

The Administrator Report Access Log displays the report access activities performed by Administrators (CSRs) in a given time period. This report displays the following information:

Table 4-1 Administrator Report Access Log fields

Report Field	Description
Issuer Name	The name of the Issuer.
Admin Name	The Administrator's User ID.
Report Type	The name of the report that the corresponding Administrator ran.
Card Number	The card number the Administrator defined when running the corresponding report (not applicable to all reports).
Start Date	The start date of the date range defined by the Administrator when running the report.
End Date	The end date of the date range defined by the Administrator when running the report.
Date Accessed	The date the Administrator ran the report.

To view the Administrator Report Access Log:

1. Click the **Administrator Report Access Log** link.

   The *Administrator Report Access* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

   The system displays the report.

Administrator Activities Log

The Administrator Activities Log displays information regarding the system activities performed by Administrators in a given time period. This report displays the following information:

Table 4-2 Administrator Activities Log fields

Report Field	Description
Issuer Name	The name of the Issuer.
Admin Name	The Administrator's User ID.
Action	The task performed by the Administrator (for example, Cardholder Account Enquiry)
Cardholder Name	The name of the cardholder associated with the corresponding Action (not applicable to all actions).
Card Number	The card number associated with the corresponding Action (not applicable to all actions).
Date Accessed	The date the action was performed.
Detail	Any system information regarding the action (for example, Admin Logged in Successfully).

To view the Administrator Activities Log:

1. Click the **Administrator Activities Log** link.

   The *Administrator Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

   The system displays the report.

Issuer Administrator Account Reports

There are two reports that display information about Issuer Administrator system access:

- Issuer Administrator Report Access Log
- Issuer Administrator Activities Log

Issuer Administrator Report Access Log

The Issuer Administrator Report Access Log displays the report access activities performed by Issuer Administrators in a given time period.

See Table 4-1 on page 54 for descriptions of the information displayed by this report.

To view the Issuer Administrator Report Access Log:

1. Click the **Issuer Admin Report Access Log** link.

   The *Issuer Admin Report Access Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

   The system displays the report.

Issuer Administrator Activities Log Report

The Issuer Administrator Activities Log displays information regarding the system activities performed by Administrators in a given time period. The report displays the following information:

Table 4-3 Issuer Administrator Activities Log Report

Report Field	Description
Issuer Name	The name of the Issuer
Admin Name	The Issuer Administrator's User ID.
Action	The task performed by the Issuer Administrator (for example, Admin Login).
Date Accessed	The date the task was performed.

Table 4-3 Issuer Administrator Activities Log Report

Report Field	Description
Detail	Any system information regarding the action (for example, Admin Logged in Successfully).

To view the Issuer Administrator Activities Log:

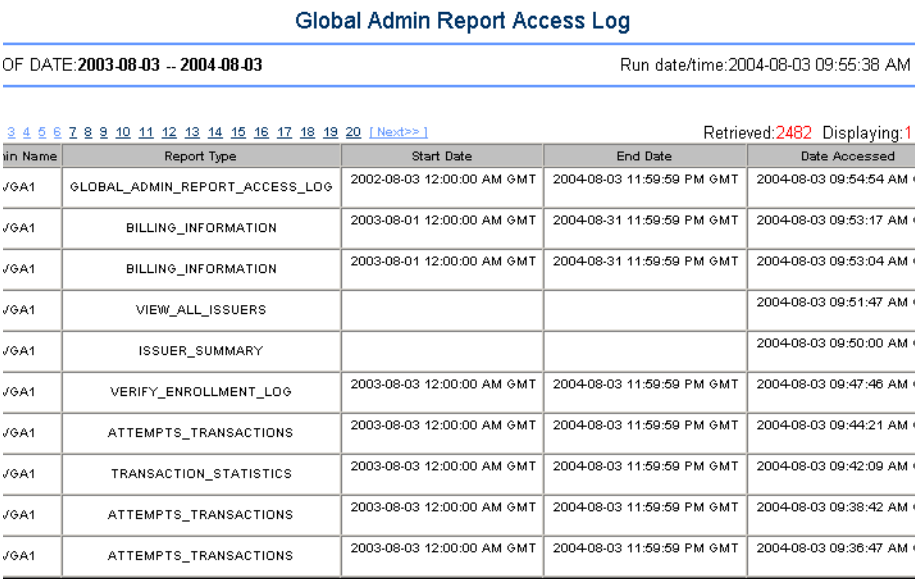
1. Click the **Issuer Admin Activities Log** link.

   The *Issuer Admin Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

   The system displays the report.

Figure 4-1 Administrator Report Access Log



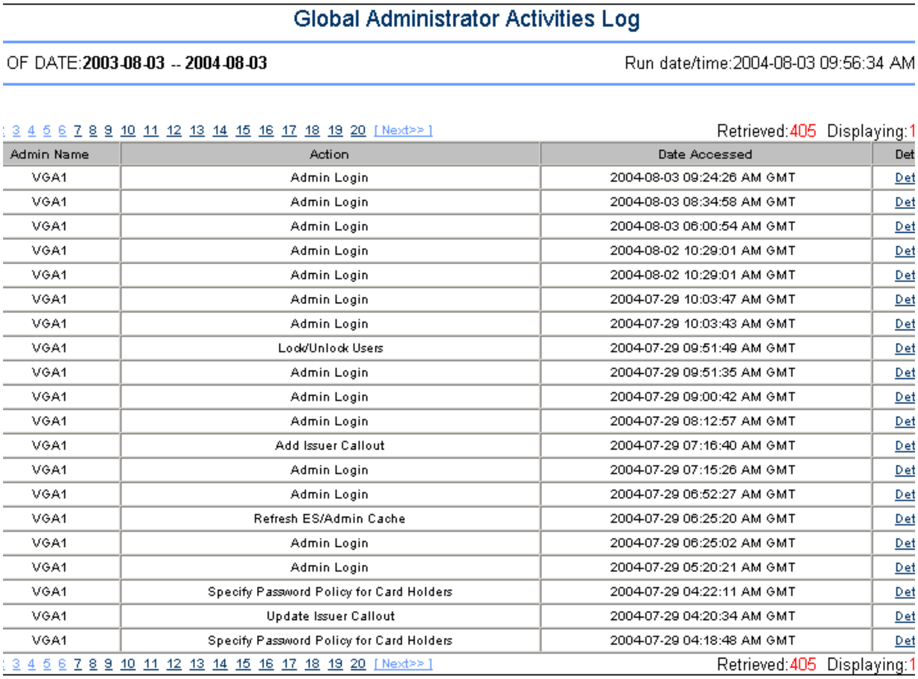
Global Admin Report Access Log

OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 09:55:38 AM

3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next>>] Retrieved:2482 Displaying:1

in Name	Report Type	Start Date	End Date	Date Accessed
VGA1	GLOBAL_ADMIN_REPORT_ACCESS_LOG	2002-08-03 12:00:00 AM GMT	2004-08-03 11:59:59 PM GMT	2004-08-03 09:54:54 AM
VGA1	BILLING_INFORMATION	2003-08-01 12:00:00 AM GMT	2004-08-31 11:59:59 PM GMT	2004-08-03 09:53:17 AM
VGA1	BILLING_INFORMATION	2003-08-01 12:00:00 AM GMT	2004-08-31 11:59:59 PM GMT	2004-08-03 09:53:04 AM
VGA1	VIEW_ALL_ISSUERS			2004-08-03 09:51:47 AM
VGA1	ISSUER_SUMMARY			2004-08-03 09:50:00 AM
VGA1	VERIFY_ENROLLMENT_LOG	2003-08-03 12:00:00 AM GMT	2004-08-03 11:59:59 PM GMT	2004-08-03 09:47:46 AM
VGA1	ATTEMPTS_TRANSACTIONS	2003-08-03 12:00:00 AM GMT	2004-08-03 11:59:59 PM GMT	2004-08-03 09:44:21 AM
VGA1	TRANSACTION_STATISTICS	2003-08-03 12:00:00 AM GMT	2004-08-03 11:59:59 PM GMT	2004-08-03 09:42:09 AM
VGA1	ATTEMPTS_TRANSACTIONS	2003-08-03 12:00:00 AM GMT	2004-08-03 11:59:59 PM GMT	2004-08-03 09:38:42 AM
VGA1	ATTEMPTS_TRANSACTIONS	2003-08-03 12:00:00 AM GMT	2004-08-03 11:59:59 PM GMT	2004-08-03 09:36:47 AM

Figure 4-2 Administrator Activity Log



Global Administrator Activities Log

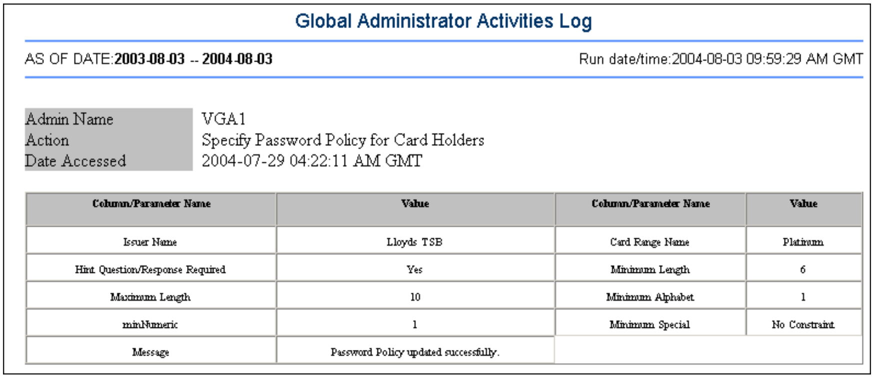
OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 09:56:34 AM

3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next>>] Retrieved:405 Displaying:1

Admin Name	Action	Date Accessed	Det
VGA1	Admin Login	2004-08-03 09:24:26 AM GMT	Det
VGA1	Admin Login	2004-08-03 08:34:58 AM GMT	Det
VGA1	Admin Login	2004-08-03 06:00:54 AM GMT	Det
VGA1	Admin Login	2004-08-02 10:29:01 AM GMT	Det
VGA1	Admin Login	2004-08-02 10:29:01 AM GMT	Det
VGA1	Admin Login	2004-07-29 10:03:47 AM GMT	Det
VGA1	Admin Login	2004-07-29 10:03:43 AM GMT	Det
VGA1	Lock/Unlock Users	2004-07-29 09:51:49 AM GMT	Det
VGA1	Admin Login	2004-07-29 09:51:35 AM GMT	Det
VGA1	Admin Login	2004-07-29 09:00:42 AM GMT	Det
VGA1	Admin Login	2004-07-29 08:12:57 AM GMT	Det
VGA1	Add Issuer Callout	2004-07-29 07:16:40 AM GMT	Det
VGA1	Admin Login	2004-07-29 07:15:26 AM GMT	Det
VGA1	Admin Login	2004-07-29 06:52:27 AM GMT	Det
VGA1	Refresh ES/Admin Cache	2004-07-29 06:25:20 AM GMT	Det
VGA1	Admin Login	2004-07-29 06:25:02 AM GMT	Det
VGA1	Admin Login	2004-07-29 05:20:21 AM GMT	Det
VGA1	Specify Password Policy for Card Holders	2004-07-29 04:22:11 AM GMT	Det
VGA1	Update Issuer Callout	2004-07-29 04:20:34 AM GMT	Det
VGA1	Specify Password Policy for Card Holders	2004-07-29 04:18:48 AM GMT	Det

3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next>>] Retrieved:405 Displaying:1

Figure 4-3 Administrator Activity Details



Global Administrator Activities Log

AS OF DATE:**2003-08-03 -- 2004-08-03** Run date/time:2004-08-03 09:59:29 AM GMT

Admin Name	VGA1
Action	Specify Password Policy for Card Holders
Date Accessed	2004-07-29 04:22:11 AM GMT

Column/Parameter Name	Value	Column/Parameter Name	Value
Issuer Name	Lloyds TSB	Card Range Name	Platinum
Hint Question/Response Required	Yes	Minimum Length	6
Maximum Length	10	Minimum Alphabet	1
minNumeric	1	Minimum Special	No Constraint
Message	Password Policy updated successfully.		

Appendix A

Adding New Reports

Reporting is the most important usability aspect of any world class enterprise software. A world class enterprise software should not only provide out of the box reporting but should allow for report creation on the fly without requiring a code change.

Arcot has state of the art XML based reporting engine which allows it to not only offer great out of the box reporting but makes adding custom reports very easy. You can generate reports for various functions like transaction, enrollment, configuration, administration, etc.

You can add a new report to TransFort by editing the file `report.xml`. `Report.xml` is a file which defines all the reports provided by TransFort. You can edit the `report.xml` which is in the following location

For Windows C:\Program Files\Common Files\Arcot Shared\conf\

For Solaris $ARCOT_HOME\conf\

to customize the existing reports.

You can customize an already existing report for:

- Title and description
- Hide columns
- Alter the display strings
- Change the display criteria
- Change the sorting order

The following sections explain the different elements found in `report.xml` and how you can alter them for customization. The procedure to add a new report is also described.

NOTE: The statistics reports are not defined in the report.xml

Elements of a Report

The report.xml contains different elements which define a report. The following table lists and describes these elements.

Table A-1 Elements and attributes in report.xml

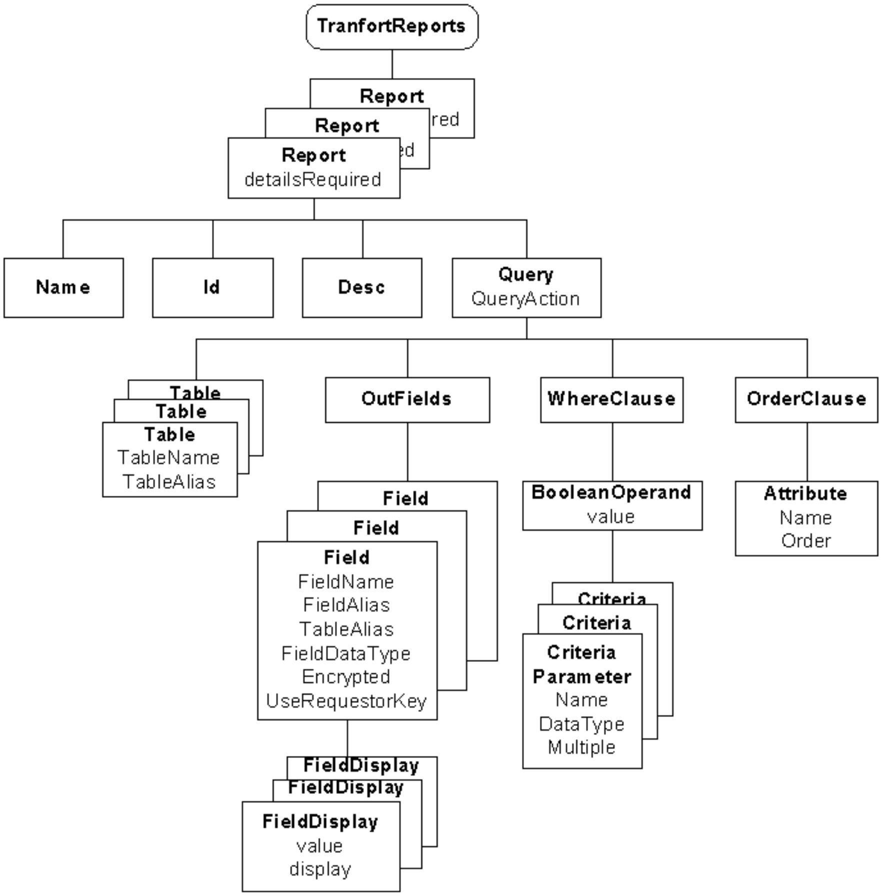
Element	Attribute	Description
Report		This parent element contains all the other elements for a report.
	detailsRequired	An attribute indicating the presence of the Details link in the report.
Name		Indicates the title of the report displayed on the administrative console.
Id		An unique indentifier for the report.
Desc		The description of the report as seen on the administrative console.
Query		This element defines the query for the report.
	QueryAction	The attribute defines the action of the query.
Table		There can be more than one Table element. This element defines the database table used to generate the report.
	TableName	The name and alias of the database table.
	TableAlias	
OutFields		This element contains all the fields which are displayed in the report.
Field		This element is a child of the OutField. It defines the field displayed in the report. There is one element for every field displayed in the report.
	FieldName	The name of the column in the table which you want to display.
	FieldAlias	The column heading as displayed in the report.
	TableAlias	The alias of the table from which the field is extracted.
	FieldDataTyped	The data type of the field. If you specify the data type to be of type 'date', the value will be converted from the database time zone to the time zone of the administrator who is running the report.

Table A-1 Elements and attributes in report.xml

Element	Attribute	Description
	Encrypted	Indicates if the column in the database is encrypted. The bankid field is used to decrypt an encrypted field.
	UseRequestorKey	This value indicates that the data needs two keys for decryption - the administrator key and the issuer key. For example, in the case where the cardholder is added by administrator. The record is encrypted using the adminsitrator key and the issuer key.
Field		This element defines the display for the particular value of the field
	value	The value of the field.
	display	The display string in the report for the above value.
WhereClause		This element defines the criteria to display the report. It contains elements which are defined by the input parameters for the report.
BooleanOperand		This element takes the boolean operand of the report criteria.
	value	The value of the boolean operand.
Criteria		The report can have several criteria. This element defines the criteria.
Parameter		The input parameters for the criteria.
	Name	The name of the parameter.
	DataType	The data type of the parameter.
	Multiple	
OrderClause		This element defines the order in which the report is displayed.
Attribute		The element takes the different attributed required for the ordering of the report.
	Name	The name of the column by which the report is sorted. The name corresponds to the FieldAlias - the column heading.
	Order	This attribute defines the sort order - ascending or descending.

The figure below gives a graphical representation of the different elements in the report.xml.

Figure A-1 Elements in report.xml



The following sections describe how to customize the reports by editing the report.xml.

Changing the Report Title

The report title and the description below the title as displayed on the administrative console can be changed. The elements Name and Desc in the report.xml have to be changed. The values these element takes are defined in the `StaticMessages.properties` file in the same path as the `report.xml`.

Editing StaticMessages.properties

When you edit the `StaticMessage.properties` file, Arcot recommends the following rules:

- If new strings are to be added to the `StatisMessages.properties` file use new string ids greater than the maximum used.
- Do not change the message of any existing string id because many of them are used in multiple files.
- Do not remove any existing string id.

Changing Column Headings

You can also change the column headings of the reports. The element FieldAlias defines the column heading in the report.xml. This element takes its value from the `StaticMessage.properties` file. You can add new entries in this file and update the report.xml with the appropriate values. The rules described in the section "Editing StaticMessages.properties," must be followed.

Hiding Columns

You can hide the column in the TransFort reports. Commenting the Field element will not display the fields. For example, in the Failed Registrations report, if you do not want to display the InWallet and OutWallet scores (used in Third-Party cardholder verification) you can comment them and they will not be displayed.

> **NOTE:**
> You have to follow the valid commenting styles as in html. The comments should be within '<!--' and '-->'.

This is shown in the sample code below:

```
- <Report>
    <Name>S5320</Name>
    <Id>FailedRegistration</Id>
    <Description>S5321</Description>
      .
      .
      <!-- Field FieldName="InWalletScore" FieldAlias="S3726"
      TableAlias="A" FieldDataTyped="String" />
        <Field FieldName="OutWalletScore" FieldAlias="S3727"
      TableAlias="A" FieldDataTyped="String" /-->
        <Field FieldName="stepModuleOrder" FieldAlias="S3731"
      TableAlias="A" FieldDataTyped="String" />
```

Altering the display strings

You can also alter the display strings for the columns in the reports. The display strings are used instead of the values from the database. For example the '**Status**' field in the Failed Registrations report can have many values. The display strings for two possible values are defined as shown below:

```
      <FieldDisplay value="NOT_ACCEPT_T&C" display="S6817" />
      <FieldDisplay value="ACCEPT_T&C" display="S6818" />
```

The strings id's are defined in the `StaticMessages.properties` file. In this example they correspond to:

```
  S6817 = NOT_ACCEPT_T&C
  S6818 = ACCEPT_T&C
```

NOTE:
Follow the rules described in the "Editing StaticMessages.properties," section.

Changing the display criteria

The display criteria of a report is defined by the input parameters of the report. The input parameters are those which you enter in the first screen when click on a report link. The parameters can be:

- Start and end dates
- Administrator user id's
- Issuer names
- Card numbers, etc.

The element WhereClause defines the display criteria of a report. The element Criteria defines each criteria based on the input parameters and the BooleanOperand element defines the boolean operation of all the criteria.

You can change the criteria for display. For example, you can run the administrator reports for all the administrator every time even though you choose only one administrator in the input screen.

In the following example, the WhereClause of the Adminstrator Report Access is defined. You can changes the criteria

```
- <Report>
    <Name>S5070</Name>
    <Id>AdministratorReportAccessLog</Id>
```

```
  .
  .
  .
- <WhereClause>
    - <BooleanOperand value="AND">
      - <Criteria>
          A.BankID IN (
          <Parameter Name="$USER.IssuerID" DataType="Integer"
        Multiple="1" />
          )
      </Criteria>
      - <Criteria>
          A.AdminLevel =
          <Parameter Name="$USER.Level" DataType="Integer" />
        </Criteria>
        <Criteria>A.Action = 'REPORT'</Criteria>
      - <Criteria>
          A.DateAccessed BETWEEN to_date(
          <Parameter Name="$USER.DateFrom" DataType="String"
        />
          , 'yyyymmdd hh24:mi:ss') AND to_date(
          <Parameter Name="$USER.DateTo" DataType="String" />
          , 'yyyymmdd hh24:mi:ss')
        </Criteria>
      - <Criteria>
          A.AdminName IN (
          <Parameter Name="$USER.AdminName" DataType="String"
        Multiple="1" />
          )
        </Criteria>
        <Criteria>A.BankID = B.BankID</Criteria>
      </BooleanOperand>
    </WhereClause>
```

Changing the sorting order

The reports displayed are sorted by an order defined by the **OrderClause** element. The OrderClause element contains two attributes **Name** - which is the heading of the column used for sorting and **Order** - which defines the type of sort - ascending or descending.

You can change the column on which a report is sorted and the order. The report is sorted only on any one selected column.

Adding a new report

You can edit the report.xml file as described in the earlier sections to define the structure of a new report. For example, consider you have added a new failed registrations report called ‘MY Bank Failed Registration Report’.

The report displays the card number, cardholder name, enrollment steps completed and status of the cardholder for a chosen Issuers for a duration defined in days. The report is sorted according to the cardholder name.

To add a new report, you must:

1. Edit the report.xml to define the new report.
2. Add a new privilege for the new report.
3. Add a new link on the administrative console for the new report.
4. Map the new link to the new report.

The following sections describe the tasks in detail.

Changing Report.xml

The elements of the new report are added at the end of the report.xml. See the code sample below:

```
- <Report>
  <Name>S5320</Name>
  <Id>FailedRegistration</Id>
  <Description>S5321</Description>
  <Query QueryAction="SELECT">
    <Table TableName="ARESLog" TableAlias="A" />
    <Table TableName="ARLocale" TableAlias="B" />
    <Table TableName="ARBankInfo" TableAlias="C" />
    <OutFields>
      <Field FieldName="CardholderName" FieldAlias="S3051"
      TableAlias="A" FieldDataTyped="String" Encrypted="1" />
      <Field FieldName="CardNumber" FieldAlias="S3052"
      <Field FieldName="stepModuleOrder" FieldAlias="S3731"
      TableAlias="A" FieldDataTyped="String" />
      + <Field FieldName="Status" FieldAlias="S3728"
      TableAlias="A" FieldDataTyped="String">
    </OutFields>
    <WhereClause>
```

```
      <BooleanOperand value="AND">
          <Criteria>(A.Status != 'ENROLLMENT_SUCCESS' AND
        A.Status != 'MINI_ENROLLMENT_SUCCESS' AND A.Status !=
        'ENROLL_REPLACE' AND A.Status != 'ENROLL_COPY' AND
        A.Status != 'ENROLL_NAME_CHANGE')</Criteria>
          <Criteria>A.LocaleID = B.LocaleID</Criteria>
          <Criteria>A.BankID = C.BankID</Criteria>
      - <Criteria>
          A.DateLogged BETWEEN to_date(
          <Parameter Name="$USER.DateFrom" DataType="String" />
          , 'yyyymmdd hh24:mi:ss') AND to_date(
          <Parameter Name="$USER.DateTo" DataType="String" />
          , 'yyyymmdd hh24:mi:ss')
      </Criteria>
      - <Criteria>
          A.BankID IN (
          <Parameter Name="$USER.IssuerID" DataType="Integer"
        Multiple="1" />  )
        </Criteria>
        <Criteria>A.IsAbridgedRegistration between 0 and
      99</Criteria>
      </BooleanOperand>
    </WhereClause>
    <OrderClause>
      <Attribute Name="S3051" Order="Desc" />
    </OrderClause>
  </Query>
</Report>
```

Adding a new privilege

You have to add a new privilege to the database to access the new report. You can do this by running the following query:

```
INSERT INTO ARADMINPRIVILEGE
  ( PRIVILEGEID, ADMINLEVEL, DESCRIPTION, PRIVILEGETYPE,
  NUMBEROF_ADMINS, PRIVIDTYPE )
VALUES
  ( 'S6225', 2, 'MY_Bank_Failed_Registration', 10, 1, 0);
```

The following table defines the parameters in the query:

Table A-2 Parameters to add a new privilege

Parameter	Description
`PRIVILEGEID`	This is an unique id for the privilege. There is a convention for this parameter. It begin with S6. The next number identifies the level of the administrator: • 1 – Master Administrator • 2 – Global Administrator • 3 – Issuer Administrator • 4 – Administrator (CSR) The next two numbers identify the nth privilege of the administrator. For example S6225 means the privilege is the 25th privilege for a global administrator. **IMPORTANT:** You should also make a new entry for the new `PRIVILEGEID` in the staticMessages.properties file.
`ADMINLEVEL`	The level of administrator as defined in the row above.
`DESCRIPTION`	The description of the report.

Table A-2 Parameters to add a new privilege

Parameter	Description
PRIVILEGETYPE	This defines the tree on the left menu in the administrative console under which the report link will be displayed. The values this parameter can take and the meaning: 1 = System Configurations 2 = Issuer Reports 3 = Issuer Configurations 4 = Global Admin Configurations 5 = Issuer Admin Configurations 6 = Admin Configurations 7 = Cardholder Configurations 8 = Callout Configurations 9 = Enrollment Process Configurations 10 = Registration Reports 11 = Transaction Reports 12 = Admin Reports 13 = Cardholder Reports
NUMBEROF_ADMINS	This field indicates if the privilege needs dual control from administrators. 1 - no need of dual control 2 - dual control required
PRIVIDTYPE	This parameter always takes a value of ‘0’.

Adding a Link for the Report

You have to edit the `index.jsp` file under `$Arcot_Home/webapps/vpas/admin/index.jsp` to add a new link in the administrative console. Locate the lines of code where the report links are defined and add the following lines of code:

```
else if ( privid.equalsIgnoreCase("S6225") )
link =
"ReportByDate.jsp?report=<My_Bank_Failed_Registrations>&adminTy
pe=<level of admin>&" + QString;
```

Parameters The input screen *.jsp from which you provide the report criteria. See WhereClause. The existing screens supported are:

- ReportByCardNumber.jsp
- ReportByDate.jsp
- ReportByDateFromDateTo.jsp
- ReportByExpiryDate.jsp
- ReportByMonths.jsp
- ReportByNameAndDate.jsp

report	The link displayed for the report
adminType	The level of administrator defined in Table A-2.

Mapping the new link to the new report

You have to edit the input *.jsp file to map the new link to the new report you added. In the above example, you have to add the following lines to the `ReportByDate.jsp`.

```
if(report.equals("My_Bank_Failed_Registrations"))
    privilegeID = "S6225";
```

The new link you have defined will open the specified input jsp screen.

NOTE:
You have to refresh the ES/Admin cache to update the cache with the changes.

Appendix B

Report Codes

This appendix contains the following tables that contain codes listed on the various administrator reports:

- $1Pre-Authorization Response Codes
- AVS Result Codes
- CVV/CVC2 Result Code
- Cardholder Status Code
- Invalid Request Codes
- Reason Column Codes for Failed Transactions Report

$1Pre-Authorization Response Codes

The $1 Pre-Authorization Response Code is a two-character code that indicates the status or the result of the cardholder's Pre-Authorization screening (also known as $1 Authorization).

A Response Code of **00** represents a Pre-Authorization approval. A response code of **85** represents a successful card verification. All other response codes represent non-approved requests.

The following table provides descriptions for the Pre-Authorization Response Codes you may see in the Cardholder Enrollment reports:

Table B-1 Pre-Authorization Response Codes

Code	Visa Description	MasterCard Description
00	Approved and completed	Approved and completed
01	Refer to issuer	Refer to issuer
02	Refer to issuer-Special condition	Invalid Merchant
03	Invalid merchant ID	Invalid merchant ID
04	Pick up card	Capture Card
05	Authorization declined	Do not honor
06	General error	--
07	Pick up card-special condition. Response indicates fraudulent use other than lost or stolen.	--
11	Approval; VIP	Approval; VIP
12	Invalid transaction	Invalid transaction
13	Invalid amount	Invalid amount
14	Invalid card number	Invalid card number
15	No such issuer	Invalid Issuer
19	Re-enter transaction	--
30	--	Format Error
39	No credit account	--
41	Pick up card-lost	Lost Card
43	Pick up card-stolen	Stolen Card

Table B-1 Pre-Authorization Response Codes

Code	Visa Description	MasterCard Description
51	Insufficient funds	Insufficient funds
52	No checking account	--
53	No savings account	--
54	Expired card	Expired card
55	Incorrect PIN	Invalid PIN
57	Transaction not permitted to cardholder	Transaction not permitted to issuer/cardholder
58	--	Transaction not permitted to acquirer/terminal
61	Exceeds approval amount limit	Exceeds withdrawal amount limit
62	Restricted card	Restricted card
63	--	Security violation
65	Withdrawal frequency limit exceeded (Activity amount limit exceeded)	--
75	PIN tries exceeded	Allowable number of PIN tries exceeded
76	--	Unable to locate, no match
77	--	Inconsistent data, rev. or repeat
78	--	No account
81	Cryptographic error	--
82	Incorrect Card Verification Value	--
84	Time limit for pre-authorization exceeded	Invalid Authorization Lifecycle
85	No reason to decline	Not declined
86	Unable to verify PIN	--
91	Service unavailable	Authorization System or Issuer System inoperative
92	Routing not successful	Unable to Route transaction
94	--	Duplicate transaction detected
96	--	System error

*. Code not applicable

AVS Result Codes

The AVS Result Code is a one-character code that indicates the result or the status of a cardholder's Address Verification Screening (AVS). The AVS determines the identity of a cardholder based on whether or not the cardholder correctly enters the card billing address when enrolling in the 3-D Secure program.

The following table provides definitions for the AVS Result Codes you may see in the Cardholder Enrollment reports. It also displays the Pre-Authorization Response Code associated with the corresponding AVS Result Code.

Table B-2 AVS Result Codes

AVS Result Code	Description	Pre-Authorization Response Code
A	Address matches but ZIP code does not	00 or 85
E	Error response for Merchant Category code	00 or 85
N	Address and ZIP code do not match	00 or 85
R	Retry; system unavailable or timed out	00 or 85
S	Issuer does not support AVS	00 or 85
U	Address information is not available	00 or 85
W	9-digit ZIP code matches but address does not match	00 or 85
X	Exact match, address and 9-digit ZIP code match	00 or 85
Y	Address and 5-digit ZIP code match	00 or 85
Z	5-digit ZIP code matches, but address does not match	00 or 85
0	Authentication problem	

CVV/CVC2 Result Code

The CVV/CVC2 Result Code is a one-character code that indicates the result or the status of a cardholder's CVV/CVC2 authentication screening. The CVV/CVC2 screening determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature block on the back of the debit or credit card.

The following table provides definitions for the CVV/CVC2 Result Codes you may see in the Cardholder Enrollment reports:

Table B-3 CVV/CVC2 Result Codes

Code	CVV Description	CVC2 Description
M	CVV match	CVC2 match
N	CVV No match	CVC2 No match
P	Not Processed	Not Processed
S	Merchant has indicated that CVV is not present on card	Merchant has indicated that CVC2 is not present on card
U	Issuer is not certified and/or has not provided MasterCard or Visa. encryption keys	Issuer is not certified and/or has not provided MasterCard or Visa. encryption keys

Cardholder Status Code

The Cardholder Status Code is a summary of the state of the cardholder's enrollment authentication. This code is based on the combined status and/or decisions of the authentication methods your Issuer is using for cardholder enrollment.

The following table lists the Cardholder Status Codes that you may find in the Cardholder Enrollment reports:

Table B-4 Cardholder Status Codes

Code	Meaning
$1_AUTH_FAILURE	The cardholder failed the Pre-Authorization verification check.
$1_AUTH_SUCCESS	The cardholder passed the Pre-Authorization check, however, the individual aborted the enrollment process before completing it.
ACCEPT_T&C	The cardholder accepted the Terms & Conditions, however, the individual aborted the enrollment process before completing it.
ATTRIBUTES_CALLOUT_FAILURE	Post Verification (Attributes) Step CallOut failed.
ATTRIBUTES_CALLOUT_SUCCESS	Post Verification (Attributes) Step CallOut success.
AVS_FAILURE	AVS verification was unsuccessful.
BAD_RESPONSE_CODE	A Pre-Authorization response code other than 00 or 85 was returned by the AVS verification.
CANCEL_ATTRIBUTES_PAGE	The cardholder cancelled the Attributes Page.
CANCEL_ISSUER_QUESTION	The cardholder cancelled the Issuer QA Page.
CANCEL_PASSWORD_PAM	The cardholder cancelled the Set Password/PAM page.
CARD_HAS_NO_VALID_RANGE	The card number does not belong to any range in the enrollment website.
CH_ABANDONED_ACTIVATION	Cardholder abandoned activation during ADS. No PARes sent.
CH_CANCELLED_ACTIVATION	Cardholder cancelled the activation page during ADS.
CH_DECLINED_ACTIVATION	Cardholder declined to join the online authentication program during ADS.
CVV2/CVC2_FAILURE	CVV2 or CVC2 verification was unsuccessful.

Table B-4 Cardholder Status Codes *(Continued)*

Code	Meaning
DATA_IN_DATABASE	The card number entered was valid, but the cardholder aborted the enrollment process (not an explicit **Cancel**)
DATA_NOT_IN_DATABASE	The card number was not valid.
DUPLICATE_REGISTER_NO	The cardholder chooses not to re-enroll.
DUPLICATE_REGISTER_REJECT	The Issuer does not allow cardholder re-enrollment
DUPLICATE_REGISTER_YES	The cardholder chose to re-enroll, however, the individual aborted the enrollment process before completing it.
ENROLL_COPY	The cardholder's record is copied to the new card issued to the cardholder. This might be needed in scenarios where one card expires and a new card is issued or the card gets upgraded or side graded. Both the cards might have an overlapping period.
ENROLL_NAME_CHANGE	The cardholder name is changed to a new name. The card number and other details remain the same.
ENROLL_REPLACE	The cardholder's card has been replaced with a new card, for reasons like lost or stolen card.
ENROLLMENT_FAILURE	The cardholder did not successfully complete the enrollment.
ENROLLMENT_SUCCESS	The cardholder successfully enrolled in the 3-D Secure program.
FAILURE_ATTRIBUTES_PAGE	The validation for Attributes Page failed.
GET_QUES_CALLOUT_FAILURE	Pre Verification (Issuer QA) Step callout to get Issuer questions failed.
INVALID_CARD_FOR_RANGE	The card number does not belong to the range in the enrollment website.
ISSUER_QUESTIONS_FAILURE	The cardholder did not answer the Issuer's verification questions correctly.
ISSUER_QUESTIONS_SUCCESS	The cardholder correctly answered the Issuer's verification question, however, the individual aborted the registration process before completing it.
MINI_ENROLLMENT_START	The cardholder started the mini-enrollment.
MINI_ENROLLMENT_SUCCESS	The cardholder successfully enrolled in the 3-D Secure program through mini-enrollment.

Table B-4 Cardholder Status Codes *(Continued)*

Code	Meaning
NO_ISSUER_ANSWERS_IN_DATABASE	Issuer Data policy is >0, but there are no Issuer answers in the Database.
NO_ISSUER_QUESTIONS_IN_DATABA SE	Issuer Data policy is >0, but there are no Issuer questions in the Database.
NOT_ACCEPT_T&C	The cardholder did not accept the Terms & Conditions.
PASSWORD/PAM_FAILURE	Cardholder entered account information, however, the individual aborted the enrollment process before completing it.
POPUP_CLOSED	Cardholder closed the popup during ADS. PARes is sent.
POPUP_TIMEDOUT	The ADS popup is timed out.
POST_FINISH_CALLOUT_FAILURE	After finish callout failed.
POST_MOD1_CALLOUT_FAILURE	Post Identification Step CallOut failed.
PRE_FINISH_CALLOUT_FAILURE	Before Finish callout failed.
QA_CALLOUT_FAILURE	Post Verification (Issuer QA) step callout failed.
QA_CALLOUT_SUCCESS	Post Verification (Issuer QA) step callout success.
SUCCESS_ATTRIBUTES_PAGE	The validation for Attributes Page is successful.
TEMP_PASSWORD_INVALID	Temporary password entered is not correct.
TEMP_RECORD_FOUND	Temporary record for the cardholder found.
TEMP_RECORD_NOT_FOUND	Temporary record for cardholder not found.
AUTO_ENROLLMENT_SUCCESS	The cardholder successfully enrolled into the online authentication program through ADS.
UPLOAD_PREACTIVATED	The cardholder who successfully enrolled into the online authentication program was pre-activated and uploaded using the Data Upload Tool.

PARes Status Code

The possible PARes status codes determined by the ACS are given in the table below:

Table B-5 PARes Status Codes

PARes Status	Description
Y	Authenticated Transaction.
N	Not an authenticated transaction.
U	Unable to authenticate transaction.
A	ACS processing **Purchase Attempts** of ADS.

ECI Values

The Electronic Commerce Values which will be included in the PARes if the PARes status is “Y” or “A” is given in the table below:

Table B-6 ECI Values in PARes

PARes Status	Visa ECI value	MasterCard ECI value
Y	05	02
A	06	01

Invalid Request Codes

The IReq code is an error code indicating the particular data which invalidates the VEReq. This field is included when the VEReq is syntactically correct, but business processing cannot be performed for some reason identified by the code. The following table lists and describes the Ireq codes you may see in the "Verify Enrollment," report:

Table B-7 Invalid Request Codes

Code	Description
50	Acquirer not participating in 3-D Secure.
51	Merchant not participating in 3-D Secure.
52	Password required, but no password was supplied.
53	Supplied password is not valid for combination of Acquirer BIN and Merchant ID.
54	ISO code not valid per ISO tables (for either country or currency).
55	Transaction data not valid. For example: • purchase amount is not the same as display amount • PAReq.acctid is not the same as VERes.acctid
56	PAReq was incorrectly routed; either: • the PAReq was received by the wrong ACS, or • the PAReq should never have been sent, based on the values in the VERes.
57	Serial number cannot be located
98	Transient system failure
99	Permanent system failure

Reason Column Codes for Failed Transactions Report

The Reason column in the Failed Transactions report summarizes the reason for the failure. The table below lists and describes the reasons:

Table B-8 Reason for Failed Transactions

Reason	Description
AAV_HMAC_ERROR	AAV generation failed.
AAV_HMACKEY_ERROR	HMAC key not found or key is invalid.
ARQC_ERROR	Chip card error.
ATTEMPTS	Attempts Transaction
AUTH_FAILED	Cardholder failed authentication.
CALLOUT_ABORT	The callout invoked was aborted.
CANCEL	Cardholder cancelled the transaction.
CARD_EXPDATE_DECRYPT_ERROR	Error while decrypting card expiry date.
CAVV_GEN_ERROR	CAVV generation failed.
CAVV_KEY_ERROR	CVV key pairs not found or key pair is invalid.
CH_DATA_ERROR	Cardholder data exceeding in memory buffer.
CH_LOCKED	The cardholder was locked during the transaction.
CH_NAME_DECRYPT_ERROR	Error while decrypting cardholder name.
CH_NAME_ENCRYPT_ERROR	Error while encrypting cardholder name.
CH_NAME_UPDATE_FAILED	Cardholder name could not be updated due to Update Cardholder Profile callout error.
CH_NOTFOUND	Mismatched account.
CH_REENROLL	The cardholder wants to add a secondary cardholder through the Welcome page and there is no Verify Issuer Answers Callout configured.
CH_STATUS_INVALID	Cardholder's status not valid for transaction.
CVV_KEYIND_INVALID	Invalid CVV Key indicator value

Table B-8 Reason for Failed Transactions

Reason	Description
DATABASE_FAILURE	Could not connect to database.
HINT_FAILED	Cardholder failed authentication during Hint/Response.
INVALID_PROXYPAN	Cardholder proxy pan not valid.
NO_VIA_CALLOUT	VIA CallOut is required but is not configured.For example, If you want to enroll secondary cardholder, the VIA callout is mandatory.
OPTIN_DECLINE	Cardholder declined to join the online authentication program during ADS.
OPTIN_POPUP_CLOSED	Cardholder closed the popup during ADS.
OPTIN_POPUP_TIMEDOUT	The popup during ADS was timed out due to cardholder inactivity.
PAN_DECRYPT_ERROR	Error while decrypting cardholder PAN.
PAREQ_CALLOUT	The status of the transaction as decided by the PAReq callout. This is used to implement Advanced ADS.
PAREQ_MATCH_FAILED	PAReq did not match/have corresponding VEReq. Can be a case of a replay attack.
PAREQ_VALIDATION_FAILED	PAReq does not conform to the 3-D Secure specifications.
PARES_GEN_FAILED	Error in generating PARes XML message.
POPUP_CLOSED	Cardholder closed the popup during transaction. PARes was sent.
POPUP_TIMEDOUT	Cardholder’s popup is timed-out due to inactivity.
PRE_PARES_CALLOUT	The status of the transaction as decided by the Pre PARes callout. This is used to implement Advanced ADS.
RCPT_FAILED	Receipt failed.
SEC_CH_INSERT_FAILED	Secondary cardholder could not be inserted.
SET_PWD_FAILED	Cardholder could not set the secret password.
SIGNPARES_FAILED	Invalid signing certificate for range.
TX_DBINSERT_FAILED	Database flush failed.

Index