About the Issuer Administration Server

The issuer administration server allows multiple issuers and the system operator to share the same infrastructure and application while maintaining a completely separate view of the system. It enables issuers and the system operator to configure the system for their own purposes independently.

Certain options may or may not be displayed depending on the type of license that a client holds. The administration server tailors the interface and available options according to the client's needs. For example an administrator whose issuer only holds a 3-D Secure license will only see and have access to 3-D Secure related functionality. A system administrator that has access to at least one issuer with a 3-D Secure license or a two-factor license is able to access the full administration interface.

Access Levels

User access levels are controlled by assigning, one of six pre-defined, roles to the user. The user role determines which menu items and functions are accessible by the user.

A **read only** option is available, for all user roles, for example, for users in support roles that are not required to add records, edit details or upload files.

The access levels are:

System administrator - the highest level of access in the system with access to system management, issuer management, user management, cardholder management, transactions, reporting and audit logs.

Issuer administrator - provides access to member bank configuration options, cardholder management, transactions, reporting and audit logs for one, or a group of issuers.

IT security - provides dedicated access to audit logs, for one or a group of issuers.

Member administrator - provides dedicated access to the Admins section (administration user management), for one issuer or an issuer group.

Business administrator - business level of access to the system provides access to cardholder management, transactions, reporting and audit logs, for one issuer or an issuer group.

Helpdesk - provides cardholder management and transactions, for one issuer or an issuer group for helpdesk users.

Logging In and Logging Out

Login

To login to the ActiveAccess administration interface you must be previously registered as an administrative user and know your Username and Password. You must also have access to the required one-time passcode, if two-factor authentication is enabled for your user account.

- From your Web Browser make a connection with the Intranet and access the ActiveAccess login page.

  The ActiveAccess administration **Login** screen is displayed.

> ⚠ **Warning**
>
> If you have forgotten your password then contact your system administrator.
>
> If security has been compromised (such as when you suspect another person has logged in using your username and password) you can login and then change your password using the **Edit Profile** link situated on the top banner.

- Enter your **Username** and **Password**.

> ⓘ **Info**
>
> Both **Username** and **Password** are case sensitive.

- Click the **Login** button.
- ActiveAccess supports two-factor authentication for logging into the Administration UI. By default, users are not forced to use two-factor authentication, unless this feature has been enabled during user creation or has been set up by the user in Edit Profile.

Note

To enable this feature, **email notification messages** must be enabled and configured in Settings.

If two-factor authentication login is enabled for your user account, enter your one-time **Passcode**.

Google Authenticator for two-factor authentication login

To use this feature, you must have Google Authenticator installed on a mobile device and have the provided QR code scanned on the app.

If a System Administrator enables this feature for a user, the QR code will be sent to the user's email address. If a user enables this function for their own account, the QR code will be displayed when enabling the feature.

Refer to Install Google Authenticator for setup instructions of Google Authenticator.

- Click the **Login** button.

Upon entering your username and password (and passcode, if required) successfully, you are verified and the first admin page will be displayed. The page that you see will depend on the access rights assigned to your username (**system administration**, **issuer administration**, **business administration**, **IT security**, **member administrator** or **helpdesk**).

Note

If the user logging in does not belong to an Issuer or Issuer Group with a valid license installed, they will not be able to access any administration pages and will be shown the following message:

*The user '**username**' does not belong to an **Issuer** or **Issuer Group** with a valid **3-D Secure enabled** or **Device enabled license** installed.*
Please contact your System Administrator.

Logout

When you have finished using ActiveAccess administration, it is important that you logout from your account, to prevent other users from performing tasks with your username and access level privileges. The Logout function is accessed via the ***Logout*** link displayed on the right of the title bar area.

Warning

It is also important that you logout while leaving your PC unattended.

- Click the *Logout* link.

  The Administration **Login** screen is displayed.

- You may now close your browser window.

Issuer Administration Environment

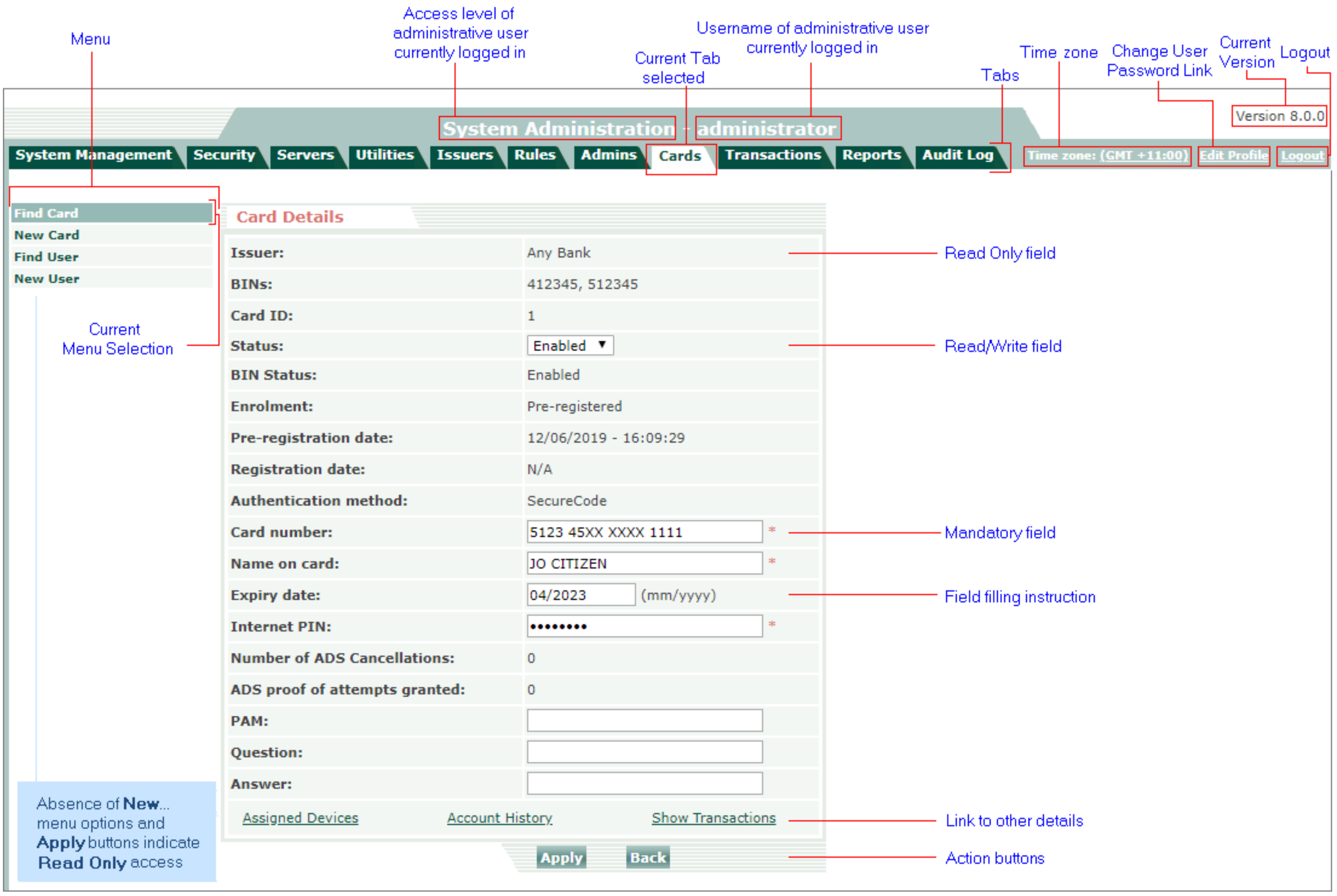
The appearance of the issuer administration pages is consistent throughout, with each being made up of a number of common components.

A banner area at the top of the screen displays the access level and the username of the user currently logged in; the system version; Time zone, Edit Profile and Logout links; and the main menu items as tabs.

Clicking on a menu tab displays the sub menu options on the left side of the page, with the first sub menu item highlighted.

Clicking on the required sub menu option displays the first page for that sub section.

The following example shows the key features of an typical ActiveAccess Administration page.



Card Details

Issuer:	Any Bank
BINs:	412345, 512345
Card ID:	1
Status:	Enabled ▼
BIN Status:	Enabled
Enrolment:	Pre-registered
Pre-registration date:	12/06/2019 - 16:09:29
Registration date:	N/A
Authentication method:	SecureCode
Card number:	5123 45XX XXXX 1111 *
Name on card:	JO CITIZEN *
Expiry date:	04/2023 (mm/yyyy)
Internet PIN:	•••••••• *
Number of ADS Cancellations:	0
ADS proof of attempts granted:	0
PAM:	
Question:	
Answer:	

Issuer Administration Options

Use the menu tabs on the ActiveAccess Issuer Administration title bar to access the administration options. The complete set of options available is:

- **System Management** - set up and maintenance of system settings, issuer administration servers, issuers and issuer groups, issuer certificates, issuer public keys, exchange configuration and archive management.
- **Security** - set up and maintenance of issuer signing certificates, Authentication History Server (AHS) certificates, and trusted Certificate Authorities (CA).
- **Servers** - set up and maintenance of ACS, Administration and Authentication History Servers.
- **Utilities** - upload, manage and run system utilities.
- **Issuers** - set up and maintenance of specific member bank details including card details, rules, custom pages and key management.
- **Rules** - set up and manage business rules and the settings for risk based authentication.

- **Admins** - set up and maintenance of ActiveAccess administrative users.
- **Users**- registration and maintenance of individual cards and users.
- **Transactions** - for accessing transactions, when required for cardholder support purposes, dispute resolution, etc.
- **Reports** - provides reports for cardholder activity, authentication, card enrolment and purchase volume, device authentication, ActiveDevice activity and user enrolment activity and a summary report.
- **Audit Log** - provides a record of administrative user activity. It includes an extensive log of critical actions performed by the administrative staff.

> **Tip**
>
> The audit log section is available to system administrators and issuer administrators only. System administrators have access to an audit log of all events and issuer administrators have access to events relating only to their specific issuer or issuer group.

About System Management

System Administrators only

This section is used for setting up and maintaining system and ACS settings, Issuers and Issuer groups, settings for authentication devices, RBA and OOB, Issuer public keys, exchange configuration and transaction record archiving. It has the following menu options:

- **Settings** - stores general settings for automatic logout idle time; maximum unsuccessful login attempts permitted; automatic unlock lag mktime; maximum number of concurrent logins allowed; and the password policy parameters for admin users.
- **ACS Settings** - Access Control Server and Remote Access Control Server related settings.
- **Issuer Management** - for setting up and maintaining Issuers and Issuer BIN ranges and viewing Issuer groups.
- **Group Management** - for setting up and maintaining Issuers groups and viewing group members
- **Authentication Management** - has settings for:
  - **Device Management** - for finding, setting up and managing devices used for authentication.
  - **Risk Management** - ➕ *new section* for managing risk chains and risk adapters used in 3DS2 risk based authentication.
  - **OOB Management** - ➕ *new section* for registering and managing the OOB adapters used for performing Out of Band (OOB) authentication challenges.
- **Public & Encryption Key Management** - for defining or updating Issuers' public and encryption keys, which are used to validate and decrypt registration API messages signed/encrypted by the Issuer.
- **Exchange Configuration** - for displaying automatically downloaded external currency exchange rates and manually creating currency exchange values for rates not available on the automated list.

- **Archive Management** - for setting up automatic transaction record archiving.

Settings

System Management > Settings

This section is used to specify and maintain general configuration parameters such as automatic logout idle time; maximum unsuccessful logins permitted; automatic unlock lag time; maximum number of concurrent logins allowed; and the password expiry period, etc.

Use the following fields to complete this page:

- **Automatic Logout** time in minutes
  Acceptable range: 0 to 240
  Default: 20 min

  > ⚠ **Warning**
  >
  > Setting this field to 0 disables the automatic logout mechanism and is not recommended.

  If an administrator account remains idle for the specified period of time it will be automatically logged out.

- **Maximum unsuccessful attempts** permitted for user logins.
  A greater number of unsuccessful login attempts will result in the administration account being locked, restricting further access to the account.
  Acceptable range: 0 to 9
  Default: 3

  > ⚠ **Warning**
  >
  > Setting this field to 0 disables the automatic locking mechanism and is not recommended.

- **Automatic unlock** time in minutes.
  The amount of time after which a locked administrator account is automatically unlocked.
  Acceptable range: 0 to 1440
  Default: 0, which disables automatic unlocking such that all locked accounts have to be manually unlocked by another administrator user with the same or higher access level.

- **Maximum concurrent logins** permitted for MIA admin users
  Acceptable range: 0 to 9

> ⚠ **Warning**
>
> Setting the number of concurrent logins to 0 will prevent more than one user logging in at the same time and is not recommended.

- The administration user **Password policy** is set using the following fields:
  - **Password expiry period** determines how often MIA administration users are required to change their MIA login password
    Acceptable range: 0 to 365
  - **Minimum password lifetime** determines the minimum number of days MIA administration users are required to wait before they can change their MIA login password again.
    Acceptable range: 0 to 90
  - **Minimum password length**
    Acceptable range: 0 to 32
    0 indicates no minimum length
  - **Minimum password numeric characters** required
    Acceptable range: 0 to 32
  - **Minimum password uppercase characters** required
    Acceptable range: 0 to 32
  - **Minimum password lowercase characters** required
    Acceptable range: 0 to 32
  - **Minimum password special characters** required
    Acceptable range: 0 to 32.

  > ✎ **Note**
  >
  > The total number of characters entered for **Minimum password numeric characters**, **Minimum password uppercase characters**, **Minimum password lowercase characters** and **minimum password special characters** must be less than or equal to the **Minimum password length**.

- **Registration server URL** is the URL of the registration server used to send final and pre-registration requests to the registration server when issuers upload card data files.
- **Time zone** is is displayed on the system administration menu bar, from where it can be modified at any time, as and when appropriate. The default time zone is set when the application is installed.

All reports and results of searches will be based on the time zone specified on the menu bar at the time of the report or search.

- **Disable admin account if inactive for more than** a specified number of days.
  Acceptable range: 0 to 365.
  The system will disable an admin account if it has not been accessed for more than the specified number of days.
  To disable, set to 0.
- **AHS timeout** in seconds
  Acceptable range: 0 to 3600
  This defines the maximum amount of time the ACS will wait for the Authentication History Server to respond. If a response is not received within the expected time, the ACS will re-schedule the AHS transaction for a later time.
- **Show for the following access levels** checkboxes determine which administrator user roles are able to view **Card Number (plain text)** and **AAV/CAVV/AEVV**.
  By default, card numbers are masked and **AAV/CAVV/AEVV** is hidden.
- **Enable manual ACS restart** checkbox if you want to defer application of changes that require a restart to the next time the server is manually restarted.
  When this option is selected, if changes require the system to be restarted to take effect, you will be prompted that a restart is required. You can choose to defer the restart or select the option to **Restart now**.
- **Enable email notification messages** checkbox if you want the system to send email messages to administrators for two-factor authentication login or notifications such as expiring license keys.
  You will need to configure the mail server settings for this feature to work.
- **Mail server address**, **Mail server port**, **Mail server username**, **Mail server password** and **Mail server protocol** are used to record the address, username and password of an outgoing SMTP mail server.

> **Note**
>
> The sender of the notification messages will be the main administrator user (administrator). Make sure that you have specified a correct email address for this user (use **Edit Profile** link, while logged in as the administrator).

> **Note**
>
> You can test mail server settings by clicking on *Send Test Message* link. The link will appear once you have entered mail server settings and applied the changes.

- **Log level** determines the amount of information generated and routed to console and log file.
  Changes to log level take immediate effect.
  The options are:
  - **All:** includes any information that can be generated by the application.
  - **Debug:** information regarding more frequent and minor operations of the system or further.
  - **Info:** (Default) important information regarding the normal operation of the application or significant events.
  - **Warn:** warnings are minor errors that may not affect the operation of the system at all. For example a missing feature or component that may not affect the system if you are not planning to use its related functionality.
  - **Error:** log errors that may affect performance or operation of the system but do not necessarily prevent the system from operating. Logs incorrect behaviour of external components and systems outside the control of the application.
  - **Fatal:** logs severe problems, imminent system failure, application or component crash.
  - **Off:** Logging is disabled.

  ActiveAccess currently logs information in a subset of the above levels at **Fatal**, **Error**, **Warn**, **Info**, and **Debug** levels. Note that each higher level is inclusive of the messages of lower levels. For example when you set the log level to **Warn,** you will also see **Error** messages.
- ***Apply*** button to save changes.

ACS Settings

➕ *3D Secure 2 settings added*

System Management > ACS Settings

The **ACS Settings** section is used to set local and remote (CAAS) Access Control Server options.

Use the following fields to set ACS settings:

- **ACS reference number**

  Displays a unique reference number provided by EMVCo to ActiveAccess.
- Select **Local** or **Remote (CAAS)** from the **Authentication server** drop down list.

3-D Secure 1 Settings

- **ACS URL** is the fully qualified URL of the Access Control Server's Payer Authentication (PA) processing page, as seen externally.

  The ACS URL specified here is passed to the merchant MPI as part of the ACS response to the Verify Enrolment (VEReq) message and is used by the merchant to transfer the session to the ACS for authentication of the cardholder.

  The default path for the ActiveAccess PA processing page is /acs/pa.

  > **Example**
  >
  > If you have installed ActiveAccess on the web server available on https://www.authenticationserver.com/ you should set the ACS URL to https://www.authenticationserver.com/acs/pa

- **Process timeout** in seconds
  Defines the maximum amount of time a cardholder has to complete their authentication. If the cardholder does not complete the authentication within the prescribed time, ACS returns a session timeout error.
  Acceptable range: 60 to 9000
- **Relative timeout** in seconds

  Determines the amount of time a cardholder has to complete a single page, however, the total time to complete the whole authentication process may not exceed the **Process timeout**.

Acceptable range: 60 to 9000

3-D Secure 2 Settings

- **ACS challenge URL** is the fully qualified URL of the Access Control Server's Challenge (CReq) processing, as seen externally.

  The ACS URL specified here is passed to the 3DS Server as part of the ACS response to the Authentication Request (AReq) message and is used by the 3DS Requestor to transfer the session to the ACS for authentication of the cardholder.

  The default path for the ActiveAccess CReq processing page is /acs/ca.

  > **Example**
  >
  > If you have installed ActiveAccess on the web server available on https://www.authenticationserver.com/ you should set the ACS URL to https://www.authenticationserver.com/acs/ca

- **Initiate CReq timeout** in seconds

  Defines the maximum amount of time between the completion of the TLS handshake and the first CReq message sent to the ACS for processing. If the ACS does not receive any CReq within the prescribed time, it returns a transaction timeout error.

  Acceptable range: 15 to 60

- **Subsequent CReq timeout** in seconds

  Determines the amount of time a cardholder has to complete a single page in App mode. However, the total time to complete the whole authentication process may not exceed the **Process timeout**. If the cardholder does not complete a single page within the prescribed time, ACS returns a transaction timeout error.

  Acceptable range: 300 to 1200

- **RRes timeout** in seconds

  Defines the maximum amount of time the Directory Server has to respond with RRes to the RReq sent by the ACS. If the Directory Server does not respond with RRes within the prescribed time, ACS returns a transaction timeout error.

  Acceptable range: 2 to 10

- **Browser authentication timeout** in seconds

  Determines the amount of time a cardholder has to complete a single page in Browser mode. However, the total time to complete the whole authentication process may not exceed the **Process timeout**. If the cardholder does not complete a single page within the prescribed time, ACS returns a transaction timeout error.

Acceptable range: 300 to 1200

- **RReq retry interval** in seconds

  Failure to complete the initial connection and TLS handshake to the Directory Server for sending RReq results in an immediate retry. Upon second failure, the ACS will wait for the amount of time prescribed in RReq retry interval and retry to connect to the Directory Server.

  Acceptable range: 5 to 20

- **Process timeout** in seconds

  Defines the maximum amount of time a cardholder has to complete their authentication. If the cardholder does not complete the authentication within the prescribed time, ACS returns a transaction timeout error.

  Acceptable range: 315 to 1260

- ***Apply*** button to save changes.

Issuer Management

This section is used to define new issuers and issuer groups, or update existing information.

A group of issuers can be created for administration purposes. Issuer group determines which issuers users have access to; the administration group determines at which level they have access.

Links are provided to **ActiveDevice Settings** for assigning devices, and for creating a **New Issuer Group** or **New Issuer**.

A list of existing issuers and their group memberships is displayed. You can browse to view issuer and issuer group details by clicking on the ***Issuer Name*** and ***Group Membership*** links. The list can be filtered by Issuer Name, Issuer ID, BINs, Status and License Expiry period.

System Management > Issuer Management displays:

- A list of **Issuers**
- ***ActiveDevice Settings*** link to the **ActiveDevice Settings** page.
- ***New Issuer Group*** link to the **New Issuer Group** page.
- ***New Issuer*** link to the **New Issuer** page.

Use the following fields to limit the number of issuers displayed:

- **Issuer Name** (complete or partial) or leave empty to return all matching issuers
- **Issuer ID**, defaults to **All**
- **Issuer BINs** (comma separate multiple BINs)
- **Status** - **All** (default), **Enabled** or **Disabled**
- Select from the **License** key status drop down list:
  - All (default)
  - Valid
  - Expired
  - Expires in less than a month
  - Expires in 1 to 3 months

  - Expires in 3 to 6 months
  - Expires after due to expire in 1 to 6 months
- Click the **Go** button to display the new search results.

The following fields and links are displayed for each issuer:

- *Issuer Name* link to the **Issuer Details** page
- **Issuer ID**
- **BINs** - BIN numbers defined for the issuer
- *Group Membership* indicates the group to which the issuer belongs to. You can click on the group name to display the **Issuer Group Details** page.
- **Status** - Enabled or Disabled
- **License** - Shows the status of the issuer's license key

New Issuer Group

System Management > Issuer Management > New Issuer Group

This page is used to define a new issuer group and to assign issuers to that group.

Use the following fields to add a new issuer group:

- **Name** of the issuer group. It is a good idea to use the word "group" as part of the name for example "ABC Group".

  The system will automatically assign a **Group ID** to the issuer group.
- Optionally specify a parent by selecting from the **Parent group** drop down list.

  This allows you to build a hierarchy of issuers and groups to suit your administration requirements.
- **ACS URL** - the system allows a separate URL to be created for each issuer group. If a separate URL is required, it should be entered here.
- **ACS Challenge URL** - the system allows a separate URL to be created for each issuer group. If a separate URL is required, it should be entered here.
- **Uses confirmation** - Indicates if the Issuer uses the confirmation method. Defaults to **No**.

In the Enrolment component, if **Uses confirmation** is enabled, the cardholder will be taken through the sign up process. If set to disabled, the registration status of the card will be checked and displayed to the cardholder.

When **Activation During Shopping** is enabled, if the cardholder is **pre-registered** and **Uses confirmation** is **No**, the cardholder is required to create a 3-D Secure password (VbV password / Mastercard SecureCode / JSecure password / American Express SafeKey / ProtectBuy password) to use in the authentication process.

If **Uses confirmation** is **Yes**, the cardholder's existing registration data is used in the authentication process, instead of requiring a new 3-D Secure password (VbV password / Mastercard SecureCode / JSecure password / American Express SafeKey / ProtectBuy password) to be created.

Select one or more issuers or groups to add to the group from the **Issuer Members** list or the **Group Members** list. Use the **Add >>** button to add the issuers or child groups to the **Selected** list.

You can use the **<<Remove** button to remove issuers or child groups from the issuer group.

- **MAC Algorithm** used in conjunction with **SecureCode** transactions.
- **Group Members** - Use the **Add >>** and **<< Remove** buttons to add or remove child groups that should belong to the group.
- **Issuer Members** - Use the **Add >>** and **<< Remove** buttons to add or remove issuers that should belong to the group.
- **Use parent certificate, public and encryption keys** option indicates that the group does not have a certificate of its own and will use the parent group's certificate and registration API public key and encryption key. This option is only enabled if you have specified a parent group. Using the parent certificate is only possible if you have also chosen to use the parent keys.
- **Use parent keys** option to indicate that the group does not have any keys of its own and will use the parent group's keys. This option is only enabled if you have specified a parent group.
- ***Apply*** button to save changes.

> **Note**
>
> Once the issuer group has been created, you may optionally specify a separate **ACS URL** for it by editing the Issuer Group Details.

Issuer Group Details

This page is used to view/ edit issuer group details and assign issuers to, or remove issuers from, the issuer group.

System Management > Issuer Management > Issuer Group Details - fields

> **Info**
>
> See the New Issuer Group section of this document for additional information on these fields.

- **Group ID** is a unique identifier, which is used by the system in order to reference the group. Group ID cannot be changed.
- **Name** of the issuer group
- **Parent Group** - you can optionally define a parent group in order to create a hierarchy of groups and issuers to suit your administration requirements.
- **ACS URL** - the system allows a separate URL to be created for each issuer group. If a separate URL is required, it should be entered here.
- **ACS Challenge URL** - the system allows a separate URL to be created for each issuer group. If a separate URL is required, it should be entered here.
- **Uses confirmation** - Indicates if the Issuer uses the confirmation method.

  The confirmation method is a process allowing cardholders with an enrolment status of "Pre-registered" to utilise their pre-registration account information, instead of creating a new 3-D Secure password, to perform 3-D Secure authentication.
- **MAC Algorithm** to be used in conjunction with **SecureCode** transactions
- **Group Members** - Child groups that belong to the group are listed in the **Selected** list. Other groups (not belonging to any other group) are listed in the **Available** list. Use the **Add >>** and **<< Remove** buttons to change the child groups that belong to the group.
- **Issuer Members** - issuers that belong to the group are listed in the **Selected** list. Other issuers are listed in the **Available** list. Use the **Add >>** and **<< Remove** buttons to change the issuers that belong to the group.
- **Use parent certificate, public and encryption keys** - Selecting this option indicates that the issuer group does not have a certificate of its own and will use the parent group's certificate, registration API public key and encryption key. The option is only enabled if you have

specified a parent group. Using the parent certificate is only possible if you have also chosen to use the parent keys.

> **Note**
>
> Enabling this option will remove the issuer group certificate (if it has one) from the system. You cannot retrieve the certificate once removed.

> **Note**
>
> When you disable this option, the issuer group will no longer use the parent's certificate. You need to create a certificate request for the issuer group and have it signed by the appropriate CAs.

> **Warning**
>
> It is recommended that you make a decision to enable or leave this option disabled at the time of creating the issuer group to avoid the administration overhead of changing this option later.

- **Use parent keys** - Selecting this option indicates that the issuer group does not have any keys of its own and will use the parent group's keys. The option is only enabled if you have specified a parent group.

  Selecting this option indicates that the issuer group does not have any keys of its own and will use the parent group's keys. The option is only enabled if you have specified a parent group.

> **Note**
>
> Changing this option invalidates the issuer group existing certificate. You either need to enable the 'Use parent certificate' option or create a new certificate request, and have it signed by the appropriate CAs.

Note

Enabling this option will delete the issuer group keys from the local HSM. Deleting keys is irreversible unless you have previously backed them up. The following keys will be removed from the local HSM, where < group_id > is the issuer group's unique identifier as shown in the issuer group details:

- SPA< group_id >
- VbVA< group_id >
- VbVB< group_id >
- JCBA< group_id >
- JCBB< group_id >
- MSCA< group_id >
- MSCB< group_id >
- SKA< group_id >
- SKB< group_id >
- DCA< group_id >
- DCB< group_id >
- RSAVbV< group_id >_pub
- RSAVbV< group_id >_pri
- RSAMSC< group_id >_pub
- RSAMSC< group_id >_pri
- RSAJCB< group_id >_pub
- RSAJCB< group_id >_pri
- RSASK< group_id >_pub
- RSASK< group_id >_pri
- RSADC< group_id >_pub
- RSADC< group_id >_pri
- RSADEVICE< group_id >_pub
- RSADEVICE< group_id >_pri

If you are using other HSMs in your system, you also need to remove these keys from those HSMs to keep them synchronised. You also need to update any other party who may use these keys for verification of AAV (UCAF) or CVV (CAVV).

Warning

Disabling this option will create new keys for the issuer group, where < group_id > is the issuer group's unique identifier as shown in the issuer group details. The following keys will be created on the local HSM:

- SPA< group_id >
- VbVA< group_id >
- VbVB< group_id >
- JCBA< group_id >
- JCBB< group_id >
- MSCA< group_id >
- MSCB< group_id >
- SKA< group_id >
- SKB< group_id >
- DCA< group_id >
- DCB< group_id >
- RSAVbV< group_id >_pub
- RSAVbV< group_id >_pri
- RSAMSC< group_id >_pub
- RSAMSC< group_id >_pri
- RSAJCB< group_id >_pub
- RSAJCB< group_id >_pri
- RSASK< group_id >_pub
- RSASK< group_id >_pri
- RSADC< group_id >_pub
- RSADC< group_id >_pri
- RSADEVICE< group_id >_pub
- RSADEVICE< group_id >_pri

If you are using other HSMs in your system, you also need to export these keys to those HSMs to keep them all synchronised. You also need to update any other party who may use these keys for verification of AAV (UCAF) or CVV (CAVV).

Tip

It is recommended that you make a decision to either **enable** or leave this option **disabled** at the time of creating the issuer, to avoid the administration overhead of changing this option later.

> **Info**
>
> Refer to New Issuer Group for additional information on these fields.

- ***Apply*** button to save changes.

> **Note**
>
> A group cannot be removed if it has other groups or Issuers belonging to it.

New Issuer

Use this page to define a new issuer and optionally assign the issuer to an issuer group.

System Management > Issuer Management > New Issuer - fields

- **Status** of **Not Registered** is automatically assigned to new issuers by the system and cannot be changed until you have obtained a license key from GPayments.
- Enter the **Name** of the Issuing bank or financial institution.

  You must enter a name that is unique in the issuer system.
- Enter an optional **Password** for the Issuing bank or financial institution.

  This password is used for authentication of issuer connection to ActiveAccess via UAC. This is in addition to the verification of issuer's client authentication and may be left empty if the extra verification is deemed to be unnecessary.
- **Show extended account information** - Select **Yes** to display all cardholder pre-registration account information, on the card details page, created during the cardholder's Pre-registration with the system. When this option is disabled, only basic cardholder information is displayed on this page.
- **Uses confirmation** - Select **Yes** or **No** to indicate if the Issuer uses the confirmation method.

  The confirmation method is a process allowing cardholders with an enrolment status of "Pre-registered" to utilise their pre-registration account information, instead of creating a new 3-D Secure password, to perform 3-D Secure authentications.
- **Event Logging** - **Disabled** by default. Select **Enabled** to indicate event logging is required or **Enable V+ compatible** to indicate event logging is required, and the maximum number of Activation During Shopping opt-out events reported to the issuer is 9.

This feature allows issuers to download cardholder events through Registration Server Notification messaging. A Notification is a record of a single cardholder event. Each event is stored in ActiveAccess and a record is logged in the event a cardholder completes their registration, opts-out of Activation During Shopping or locks their account.

- If the issuer is to be assigned to an issuer group, select the group from the **Parent group** drop down list.
- If you have specified a parent group:
    - You may select the **Use parent certificate, public and encryption keys** option to indicate that the issuer does not have a certificate of its own and will use the parent group's certificate and registration API public key and encryption key.
    - You may select the **Use parent keys** option to indicate that the issuer does not have any keys of its own and will use the parent group's keys.
- ***Apply*** button to save changes.

Tip

Once you have created the Issuer record a confirmation message will be displayed:

Please note down the **Issuer ID** and **Issuer Name**, and send them to GPayments in order to request a license key for the newly generated issuer.

Note

Once the new issuer has been created, you may optionally specify a separate **ACS URL** for it by editing the Issuer Details.

Info

Refer to Issuer Details for additional information on these fields.

Issuer Details

This page is used to view/ edit issuer details and assign the issuer to, or remove the issuer from an issuer group.

System Management > Issuer Management > Issuer Details (Local and Remote Issuers)

Use the following fields to view / edit issuer details:

> **Note**
>
> Not all fields will be visible to all issuers, depending on issuer or issuer group settings.

- **Issuer ID** is a unique identifier, which is used by the system in order to reference the issuer. Issuer ID cannot be changed. Issuer ID is used in a number of situations such as requesting license key for the issuer, sending pre-registration and final registration messages and also forms part of the unique URL which is used for the issuer enrolment site.
- **Status** - **Enabled** or **Disabled**, if the issuer is registered. Prior to the issuer obtaining a valid license key the Status is displayed as **Not Registered** and cannot be changed.

  > **Note**
  >
  > An issuer account that does not have a valid licence key is practically disabled. This makes most functions unavailable to the issuer including the enrolment, registration and authentication of cardholders.

- **Name** of the issuing bank or financial institution.

  > **Note**
  >
  > This field forms part of the issuer licence key information. You will need to re-apply for a licence key if you change this field.

- **Password** for the Issuing bank or financial institution.

  This password is used for authentication of issuer connection to ActiveAccess via UAC. This is in addition to the verification of issuer's client authentication and may be left empty if the extra verification is deemed to be unnecessary.
- **ACS URL** - the system allows a separate URL to be created for each issuer. If a separate URL is required, it should be entered here.
- **ACS Challenge URL** - the system allows a separate URL to be created for each issuer. If a separate URL is required, it should be entered here.
- **Show extended account information -** Select **Yes** to display all cardholder data as sent by the Registration API messages in the card details page. When this option is disabled, only basic cardholder information is displayed.

- **Allow issuer to access rules -** Select **Yes** or **No** to indicate if the Issuer can access the business rules functionality.

  Business rules are configurable settings which provide issuers control over the customer process during the 3-D Secure transactions. Rules can be configured using a 3-D Secure transaction's parameters such as the Transaction Amount, the Merchant ID, Merchant Name, Acquirer BIN or Merchant Country.

> **Note**
>
> This feature is only available, if the custom pages are rule-compatible.

- If **Allow issuer to access rules** is set to **Yes**, then **Grant Access to Business Admin** and **Grant Access to Helpdesk** checkboxes allow you to grant Business Admin and / or Helpdesk users access to the Rules section. Whether these users have *read only* or *full* access is determined by their Admins settings
- **Authentication Server - Local** or **Remote (CAAS)**
- If **Remote (CAAS)** is selected, **CAAS Server** will be displayed, to allow selection of the already configured remote authentication servers.
- If **Authentication server** is set to **Remote (CAAS)**, optionally select the **Risk engine integration** checkbox if the authentication process is to be integrated with the issuer's risk engine.
- **Risk chain** - Select an already configured Risk Chain from the drop down list to enable Risk-Based authentication for the issuer.
- **ACS interface** - Select **Native** (default) or **HTML** from the drop down list.

  Identifies the ACS interface for presenting the challenge to the cardholder: Native UI or HTML UI. In SDK mode, if the supported interface is not specified in the AReq, the ACS uses the interface that is selected in this field.
- **Uses confirmation** - Indicates if the Issuer uses the confirmation method. Defaults to **No**.

  The confirmation method is a process allowing cardholders with an enrolment status of "Pre-registered" to utilise their pre-registration account information, instead of creating a new 3-D Secure password, to perform 3-D Secure authentications.
- **VISA CEMEA region** - Visa CEMEA require that a CAVV be generated and returned in all PARes messages regardless of the authentication status. Set this field to **Yes**, if this functionality is required.

- **SecureCode MAC Algorithm -** determines the algorithm which is used for calculation of AAV field for SecureCode transactions. By default HMAC algorithm is used. You may change this to CVC2 if required.

> **Note**
>
> The application generates two 3DES keys in the primary HSM, when a CVC2 option is selected for the first time: MSCA< issuer_id > and MSCB< issuer_id >. The system admin must ensure that these keys are copied to all HSM instances.

- **Force cardholders to use device** - if Device Authentication is available, select **Yes** to force cardholders to register their authentication device during the 3-D Secure authentication process. Select **No**, to provide cardholders with a link to allow them to register their authentication device.
- **Event Logging** - **Disabled** (default) or **Enabled** to indicate event logging is required; or **Enable V+ compatible** to indicate event logging is required and the maximum number of Activation During Shopping opt-out events reported to the issuer is 9.
- **Parent group** - select the group to which the Issuer belongs, if any.

> **Note**
>
> The issuer can only be assigned to a single group; however the group itself can belong to another group. This enables you to create a hierarchy of issuers and groups to suit your administration needs.

- **License key** - copy license key provided by GPayments and click ***Apply*** button. The **Status** will then change to **Enabled**.
    - **License status** - once you have entered a valid license key the license status will display the validity period for the key (e.g. **License key is valid until 01/03/2019)** and if it is Device authentication enabled, 3-D Secure authentication enabled or 3-D Secure V2 authentication enabled, if OOB, NPA, and APP features are supported.

      The License status also determines the type of authentication available to the Issuer. When **3-D Secure authentication enabled** is displayed, the issuer can register cardholders and authenticate them using standard 3-D Secure password authentication. When **Device authentication enabled** is displayed, the Issuer can register users and authenticate them using device authentication. This option also allows Issuers to register cardholders for 3-D Secure and authenticate them using device authentication.

Note

If the licence key is not present, invalid or expired, the issuer account is practically disabled. This makes most functions unavailable to the issuer including the enrolment, registration and authentication of cardholders.

- **Issuer BINs** - Use the **BIN Management** link to add, edit, delete, enable and disable one or more BINs for the issuer and specify if device authentication is available for cards that belong to the specified BIN.
- **Use parent certificate, public and encryption keys** - Selecting this option indicates that the issuer does not have a certificate of its own and will use the parent group's certificate, registration API public key and encryption key. The option is only enabled if you have specified a parent group. Using the parent certificate is only possible if you have also chosen to use the parent keys.

Note

Enabling this option will remove the issuer's certificate (if it has one) from the system. You cannot retrieve the certificate once removed.

Note

When you disable this option, the issuer will no longer use the parent's certificate. You need to create a certificate request for the issuer and have it signed by the appropriate CAs.

Tip

It is recommended that you make a decision to enable or leave this option disabled at the time of creating the issuer to avoid the administration overhead of changing this option later.

- **Use parent keys** - Selecting this option indicates that the issuer does not have any keys of its own and will use the parent group's keys. The option is only enabled if you have specified a parent group.

Note

Changing this option invalidates the issuer's existing certificate. You either need to enable the 'Use parent certificate' option or create a new certificate request, and have it signed by the appropriate CAs.

⚠ **Warning**

Enabling this option will delete the issuer's keys from the local HSM. Deleting keys is irreversible unless you have previously backed them up. The following keys will be removed from the local HSM, where < issuer_id > is the issuer's unique identifier as shown in the issuer details:

- SPA< issuer_id >
- VbVA< issuer_id >
- VbVB< issuer_id >
- JCBA< issuer_id >
- JCBB< issuer_id >
- MSCA< issuer_id >
- MSCB< issuer_id >
- SKA< issuer_id >
- SKB< issuer_id >
- DCA< issuer_id >
- DCB< issuer_id >
- RSAVbV< issuer_id >_pub
- RSAVbV< issuer_id >_pri
- RSAMSC< issuer_id >_pub
- RSAMSC< issuer_id >_pri
- RSAJCB< issuer_id >_pub
- RSAJCB< issuer_id >_pri
- RSASK< issuer_id >_pub
- RSASK< issuer_id >_pri
- RSADC< issuer_id >_pub
- RSADC< issuer_id >_pri
- RSADEVICE< issuer_id >_pub
- RSADEVICE< issuer_id >_pri

If you are using other HSMs in your system, you also need to remove these keys from those HSMs to keep them all synchronised. You also need to update any other party who may use these keys for verification of AAV (UCAF) or CVV (CAVV).

Note

Disabling this option will create new keys for the issuer. The following keys, where < issuer_id > is the issuer's unique identifier as shown in the issuer details, will be created on the local HSM:

- SPA< issuer_id >
- VbVA< issuer_id >
- VbVB< issuer_id >
- JCBA< issuer_id >
- JCBB< issuer_id >
- MSCA< issuer_id >
- MSCB< issuer_id >
- SKA< issuer_id >
- SKB< issuer_id >
- DCA< issuer_id >
- DCB< issuer_id >
- RSAVbV< issuer_id >_pub
- RSAVbV< issuer_id >_pri
- RSAMSC< issuer_id >_pub
- RSAMSC< issuer_id >_pri
- RSAJCB< issuer_id >_pub
- RSAJCB< issuer_id >_pri
- RSASK< issuer_id >_pub
- RSASK< issuer_id >_pri
- RSADC< issuer_id >_pub
- RSADC< issuer_id >_pri
- RSADEVICE< issuer_id >_pub
- RSADEVICE< issuer_id >_pri

If you are using other HSMs in your system, you also need to export these keys to those HSMs to keep them all synchronised. You also need to update any other party who may use these keys for verification of AAV (UCAF) or CVV (CAVV).

Tip

It is recommended that you make a decision to enable or leave this option disabled at the time of creating the issuer to avoid the administration overhead of changing this option later.

- **Email Address** - may be used in OTP emails (parameter: $IssuerEmail - max 128 char).
- **Customer service phone number** may be used in OTP emails (parameter: $ServicePhoneNumber - max 32 char).
- ActiveDevice Settings - used to assign one or more device types to a selected issuer and specify device sharing rules.
- ***Apply*** button to save changes.

BIN Management

This section is used to manage BINs of a specified issuer. Each BIN provides a link to allow you to edit the BIN, the status of Device over 3-D Secure or the status of the BIN. BINs can be selected and deleted from the system using the **Delete** button. Only BINs which have no cards assigned to them on the system can be deleted. The **Enable** and **Disable** buttons can be used to change the status of the BIN. New BINs can be added for the issuer through the *Add BIN* link and device authentication can be made available for cards that belong to the specified BIN.

System Management > Issuer Management > Issuer Details > BIN Management > Add BIN

Use the following fields to add a BIN:

- **Issuer** is displayed and cannot be changed.
- **BIN** .
- **Device over 3-D Secure** - **Disabled** or **Enabled** to specify if device authentication is available for cards that belong to this BIN.
- **Status** - **Disabled** or **Enabled** to specify the availability of the 3-D Secure service for cards that belong to this BIN. Cards with a **Disabled** BIN cannot be enrolled, registered or authenticated.
- ***Apply*** button to save changes.

ActiveDevice Settings

This section is used to assign one or more device types to a selected issuer and specify device sharing rules. An issuer may choose to share devices with none, all, or a selected number of issuers and issuer groups.

Note

Device parameters for SMS and email devices are issuer specific and these devices are not shared between issuers and issuer groups. However, the same mobile numbers / email addresses can be registered for different issuers. ActiveAccess treats SMS / email devices that have the same mobile numbers / email addresses as independent devices.

System Management > Issuer Management > Issuer Details > ActiveDevice Settings

Use the following fields to view / edit ActiveDevice settings:

- **Issuer**
- **Supported devices** - authentication devices accepted by the Issuer are listed in the **Selected** list. Other available devices not currently selected by the issuer are listed in the **Available** list. Use the **Add** and **Remove** buttons to change the tokens assigned to the issuer.
- **Allow sharing device with** allows the issuer to share its devices will all, none or a selected list of issuers and groups.
- ***Apply*** button to save changes.

To view device parameter details, click the **Device Parameters** button.

The **Edit Device Parameters** page will be displayed.

Warning

For hardware and software token devices, changing device parameters may adversely affect the authentication of users. Such device parameters must be left as default unless absolutely necessary. You must consult with the device manufacturer before making any changes to these parameters.

Note

For information on default device parameters, go to **Device Management**.

Edit Device Parameters

The first available Device type for the selected Issuer is displayed.

Use the following fields to edit Device Parameters:

- **Device type** This parameter can be left as the default or customised for the selected issuer.

The available device types are:

  - Backup Device
  - CAP (M-Chip 2)
  - CAP (M-Chip 4)
  - Email
  - OOB ➕
  - RSA
  - SMS
  - VASCO

- **Use device's default parameters** - if this option is selected, it indicates that the issuer will use the Default Device Parameters for the selected device.

  Deselect the checkbox to customise the device parameters. If the checkbox is already deselected, you can reset the parameters to the default by selecting it.

> **Note**
>
> For full details of device parameters, refer to Default Device Parameters.

The following fields are additional to the configurable fields in Default Device Parameters:

- **Device type**: SMS
  - **Available SMS Centres** - use the **Add >>** and **<< Remove** buttons to select the appropriate SMS Centres.
- **Device type**: OOB ➕
  - **Available OOB adapters** - use the **Add >>** and **<< Remove** buttons to select the appropriate OOB Adapters.

Group Management

System Management > Group Management

This section is used to set up and maintain issuer groups. It provides access to the same functions as the Issuer Management section, but from an issuer group perspective.

Organising related issuers in a group can greatly reduce the issuer administration overhead. Groups can have their own keys (AAV key[1], CVC2 keys[2], CVV keys[3] and signing key[4]) and certificates. An issuer can be configured to use the parent group's keys to reduce the number of keys generated on the HSM and as a result, also reduce the overhead of key transfer tasks for synchronizing multiple hardware security modules. An issuer may also be configured to use the parent group's certificate in order to reduce the overhead of certificate management and renewal.

A list of issuer groups and their issuer and group members is displayed. You can browse to view issuer group and issuer details by clicking on the **Group Name**,**Issuer Members** and **Group Members** links.

The following fields and links are displayed:

- **Group Name** links to **Group Details** page
- **Group ID**
- **Group Members** links to **Issuer Group Details** page, shows the issuer groups and issuers that belong to this group
- **Issuer Members** links to **Issuer Details** page, shows the license key and certificate details for the selected issuer
- **New Issuer Group**
- **New Issuer**

[1] 192-bit generic key used in AAV HMAC calculation, used in SecureCode transactions

[2] Pair of DES or 3DES keys, used in calculation of AAV CVC2, used in SecureCode transactions

[3] Pair of DES or 3DES keys, used in calculation of CVV, used in VbV transactions

[4] RSA key pair used signing the PARes messages

About Authentication Management

The **Authentication Management** section is used for:

- **Device Management** - for finding, setting up and managing devices used in the authentication process.
- **Risk Management** ➕ *new section* - for managing risk chains and risk adapters used in 3DS2 risk based authentication.
- **OOB Management** ➕ *new section* - for registering and managing the OOB adapters used for performing Out of Band (OOB) authentication challenges.

Device Management

> *The **Device Management** section is grouped with **OOB Management** and **Risk Management** in the **Authentication Management** section.*

This section is used for finding devices, updating device status, uploading hardware token device initialization seed files, and configuring default device parameters.

Note

The term 'devices' is used as a generic term for both devices used for authentication and authentication methods. It includes:

- Hardware and software tokens
- Smart (chip) cards
- Authentication methods such as OTP with SMS or email
- A standalone backup token

Info

Device files for hardware tokens are provided by the device manufacturer and contain information that uniquely identifies each authentication device and can be used to verify the tokens / passwords generated by that device. Each hardware token device is identified by a serial number. The serial number is determined by the device manufacturer and must be unique per device type.

Once a seed file is uploaded into the system, cards/users can be assigned to devices by linking device serial numbers with card/user accounts. Once an account is linked with a device serial number, the card/user enrolment process is complete.

System Management > Authentication Management > Device Management displays

- A list of recently **uploaded device seed files** for hardware tokens. By default the system displays the seed files uploaded in the last 10 days.
- **Edit Default Device Parameters**
- **Upload File** to schedule a new job
- **Find Device** to view or edit the details of each device.

Use the following fields to limit the upload files displayed:

- **Issuer**
- **Device Type**
- **From** and **To Date**
- **Refresh** button to display the new list.

The following fields and links are displayed:

- **Job number** link to the **Job Details** page to view job details including any error message or warnings.
- **Issuer name** (owner of the devices)
- **File Name**
- **Device type**
- When the upload was **Started** and **Finished**
- Number of **Attempts** before the upload was finished
- **Status** of the job: get the current status by pressing the refresh button

Job Details

This page displays details of the seed file upload, including any error messages or warnings, for the job selected on the **Upload File** page.

System Management > Authentication Management > Device Management > Job Details displays

- **Issuer** name
- **Job number**
- **Uploaded** - date and time when the file was first uploaded
- **Device type**
- **File Name**
- **Start** and **Finish** date and time the job
- **Attempts** before the upload was finished
- **Status**

- **Error message**, if any.
- **Error details**
- **Warnings**

Edit Default Device Parameters

System Management > Authentication Management > Device Management > Edit Default Device Parameters

Each device has its own set of device parameters. In the case of hardware tokens, these are manufacturer-defined parameters, such as VASCO or RSA, supported by adding additional libraries and installing vendor specific drivers. Other devices, such as SMS and Email are virtual devices natively supported by ActiveAccess.

Device parameters can be customised per issuer. By default this customisation is disabled, such that all issuers use the default device parameters.

Use the following fields to edit default device parameters:

- **Device type**

  The options are:

  - Backup Device
  - CAP (M-Chip 2)
  - CAP (M-Chip 4)
  - Email
  - RSA
  - SMS
  - VASCO

SMS

System Management > Authentication Management > Device Management > Edit Default Device Parameters - SMS

SMS is a virtual device natively supported by ActiveAccess. This is in contrast to some third party devices such as VASCO or RSA which are supported by adding additional libraries and installation of vendor specific drivers.

The SMS device can be used as a backup device.

The SMS device parameters page is where the administrator can setup the system for sending SMS messages. ActiveAccess supports SMPP-API-0.3.9.1 (Short Message Peer to Peer) protocol for sending SMS messages to an SMS gateway, also known as an SMSC (Short Message Service Centre). The SMS gateway is normally provided by the business section of your preferred telecommunications company.

The connection to the SMSC must be over TCP/IP. The details of connection to the SMSC will be provided by your telecommunications company.

Use the following fields to edit SMS Device Parameters:

- **Device type** - **SMS**
- **SMS token type** - ActiveAccess can generate two types of SMS tokens:
    - **Instant** - the system generates one SMS token per authentication. The token is generated and sent to the user's mobile phone, after the verify enrolment request is received by ActiveAccess. For example the user visits the Internet banking site and enters their user ID and static password. The bank verifies the password and if successful sends a verify enrolment message to ActiveAccess with SMS as device type. ActiveAccess then sends an SMS message which contains the authentication token. The user is then required to enter the token as the second factor of authentication in order to login and access the Internet banking site.
    - **Batch** - the user receives a batch of SMS tokens beforehand. The batch SMS message contains a batch reference number and a list of generated tokens, each identified by a letter of the alphabet. The user is then asked to enter a token that corresponds with a specific letter of the alphabet as shown on the authentication page. With batch SMS, up to 15 tokens can be sent in a single SMS message and hence reduce the cost of sending SMS tokens. The system generates another set of tokens and sends them to the user when the last token for the current batch is used.
- **Batch SMS lifetime** - determines the validity period of batch SMS tokens in days (acceptable range is 0 to 365). Batch tokens will be valid for the period specified by this option. The default is 30 days.

- **Instant SMS lifetime** - determines the validity period of instant SMS tokens in minutes (acceptable range is 0 to 60). Following Instant tokens will be valid for the period specified by this option. The default is 15 minutes. You should consider the mobile network delay for sending SMS messages and provide sufficient time for the user to enter the token.
- **SMS token length** - determines the number of digits in the token generated (acceptable range is 6 to 10). The default is 6 digits.
- **Number of tokens in each batch** - determines the number of tokens included in a batch. The default is 10.

  An SMS message on a GSM network may contain up to 160 characters, while the limit for a CDMA network is between 120 to 153 characters. The system limits the maximum number of tokens based on the CDMA's lower limit of 120 characters.
- **Maximum unsuccessful attempts to send an SMS** - (acceptable range is 0 to 9) if sending an SMS message fails due to network or application errors, such as connection problems to the SMSC or receiving an invalid response from the SMS, the system attempts to resend the SMS message up to the number of times specified by this option. The default value is 5. If all attempts for delivering fail, an error is reported back to the administration user.
- **Maximum number of SMSs sent per authentication session** - (acceptable range is 0 to 99) determines the number of times that a new SMS OTP can be requested by the cardholder during each authentication session. The default value is 3. If the limit is reached, the authentication fails.
- **Accept mobile numbers of** - Select the country name that you would like to accept as SMS mobile number. Select 'All' if you would like to accept all international mobile numbers.
- **Restrict mobile number** - Turn this option on if you want to specify a mobile number format. Enter the required format, eg. ###########, 61#########, 0061#########. Allowed characters are 0-9, '#', '(', ')', '-' and space. Please note that the mobile number, excluding country calling code and trunk code, is checked against the specified patterns. Mobile number patterns should be no longer than 20 characters, including the Country Code.
- **Use as backup device** - Turn this option on if you would like SMS to be used as a backup device. A backup device can be activated once a user reports a device lost or damaged, or requests the helpdesk to disable the device temporarily.
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and one-time password.

- **SMS Centres** - Click on the link to view a list of currently configured SMS gateways. You can click on the SMSC name to edit or view the details or you can add or remove an SMSC entry by selecting the corresponding link.
- **SMS Templates** - Click on the link to Edit Default Templates for Activation During Shopping (ADS), Authentication, Activation via Authentication or Activation/Registration via MIA.
- ***Apply*** button to save changes.

SMS Centre

System Management > Authentication Management > Device Management > Edit Default Device Parameters - SMS > SMS Centres

This section is used to manage and add new SMS Centres. You can select any SMS centre to edit or delete.

- To delete an SMS Centre
  - Choose one or more SMS Centres by clicking the **Select** checkbox adjacent to the **ID**
  - Click the **Delete** button.

  A confirmation message will be displayed.
- To edit an SMS Centre
  - Click the *Name* hyperlink for the SMS Centre you wish to view or edit details.

  The **Edit SMS Centre** page is displayed.
- To add a new SMS Centre
  - Click the *New SMS Centre

  The **New SMS Centre** page is displayed.

EDIT SMS CENTRE

System Management > Authentication Management > Device Management > Edit Default Device Parameters - SMS > SMS Centres > Edit SMS Centre *displays the following fields:*

- **Device ID** is displayed and cannot be changed.
- **Name of Service provider** (mandatory).
- **Domain/IP** and **Port** - If changes are made to Domain name or IP address and Port number, they must correspond to the SMSC provider for connection to SMSC over TCP/IP.

- **System ID, System type and Password** - if changes are made, they must be specific to the parameters that are required for authentication of the client application (in this case ActiveAccess) to the SMS centre and this generally will be provided by the SMSC provider.
- **Sender's mobile number** - maximum length of 20 characters, including the Country Code. Allowed characters are A-Z, a-z, 0-9, '(', ')', '-' and space.
- ***Apply*** button to save changes.

NEW SMS CENTRE

System Management > Authentication Management > Device Management > Edit Default Device Parameters - SMS > SMS Centres > New SMS Centre

Use the following fields to create a new SMS Centre:

- **Name** - Choose a descriptive and unique name.

  If the SMS Centre is actually an MQ Server that consumes SMPP messages, the **Name** should be a unique name which will become the prefix of the required parameters in **AA_HOME/sms-jms-config.properties** for the corresponding SMSviaJMS Client. It is possible to configure as many different SMSviaJMS clients as required for ActiveAccess. For more information regarding the SMSviaJMS configuration parameters, please refer to AA81-GPayments SMS via JMS- Library.pdf.
- **Domain/IP and Port** - Enter the Domain name or IP address and Port number provided by the SMSC provider for connection to SMSC over TCP/IP.

  ActiveAccess currently supports the following types of the SMPP gateways as SMSC and one as SMSviaSMTP:
  - **Real SMPP Compatible SMSC** - This is a real world receiver of the SMPP messages. The IP and Port of the designated SMSC need to be specified for this type. SMS maximum length is 160 ASCII characters (70 Unicode characters).
  - **SMSviaJMS Module** - This acts as an SMSC and receives SMPP messages but relays only the submit_sm messages to the MQ Server, which exclusively consumes submit_sm messages. SMS maximum length is 160 ASCII characters (70 Unicode characters).
  - **SMSviaJMS Library** - This has been embedded into ActiveAccess itself and acts as a real SMPP client but only submits the submit_sm messages to the MQ Server, which exclusively consumes submit_sm messages. **Port** can be set to any number as it does not have any usage here. SMS maximum length is 64k ASCII characters (32k Unicode characters).

  - **SMSviaSMTP Library** - This has been embedded into ActiveAccess itself and acts as an SMTP client, which builds SMS but sends them to the email addresses with a specified template in the **Domain/IP** field. **Port** can be set to any number as it does not have any usage for this type. No limitation is applied for the size of the SMS via SMTP.

Some clients have their own SMS switch, which provides all necessary information regarding SMS delivering and billing. These SMS gateways support only SMTP protocol for the incoming messages. As the ACS provides the ability to send OTP over SMTP, a template has been defined for this purpose, in the form of mailto:$DEVICE_SERIAL_NUMBER\@smtp.com.

The SMS sender module replaces the **$DEVICE_SERIAL_NUMBER** in the Domain/IP field with the registered mobile number of the cardholder and sends the OTP to a generated email account through the SMS switch.

> **For Example**
>
> If a cardholder has been registered with the mobile number of 614501234567, the SMS sender sends the OTP to the 614501234567@smtp.com account and the SMS switch relays it to the cardholder's mobile.

You can also define an email URL instead of an IP address for testing purposes. The email URL must start with **mailto:**, followed by the destination email address (such as **mailto:**myemail@mycompany.com). If you specify an email instead of an IP address, ActiveAccess will send the content of the SMS message to the specified email address. You must also ensure that the mail server settings are properly configured in the **_System Management** > **Settings_** page.

Alternatively, SMPPSim, an open source and free SMPP simulator from http://www.seleniumsoftware.com/, can be used for testing.

Before testing with SMS, make sure that SMS has been selected as the authentication device for the issuer and that the SMS custom pages have been loaded for the issuer.

- **System ID, System type and Password** - These are SMSC specific parameters that are required for authentication of the client application (in this case ActiveAccess) to the SMS centre and should be provided by the SMSC provider. If the SMSC does not require client authentication, leave these fields blank.
- **Sender's mobile number** - Enter the number to be used as the sender's default mobile number, for all messages sent through the selected SMSC. Maximum length is 20

characters, including the Country Code. Allowed characters are A-Z, a-z, 0-9, '(', ')', '-' and space.

- ***Apply*** button to create the new SMS Centre.

SMS Template

Use this section to edit the default SMS templates for:

- Activation During Shopping (ADS)
- Authentication
- Activation via Authentication
- Activation/Registration via MIA.

System Management > Device Management > Edit Default Device Parameters - SMS > SMS Templates > Edit Default Templates

Use the following fields to edit an SMS Template:

- **SMS**
- **Template name** - the options are:
  - Activation During Shopping (ADS)
  - Authentication
  - Activation via Authentication
  - Activation/Registration via MIA
- **Template** - Enter the default system message. This message is sent to the user when an SMS authentication is requested.

Info

Click the adjacent **Help** button for a full list of parameters. The default phrase can incorporate the following details, where appropriate:

SMS Template Parameters	Length (char)
$BatchNumber - serial number of the batch SMS sent when using device authentication of 3-D Secure	max 5

SMS Template Parameters	Length (char)
$CardExpiryDate - expiry date of the credit card	5
$CardHolderName - cardholder name as specified in the system	max 64
$CardProvider - card scheme name for the credit card	max 21
$CurrencySymbol - the currency symbol for the purchase when using device authentication over 3-D Secure	max 3
$IssuerName - Issuer's name as defined in the system	max 256 *
$MerchantCountry - 3 character country code for the Merchant's country	3
$MerchantName - Merchant's name for purchase using device authentication over	max 25 *
3-D Secure	
$MerchantURL - URL of the Merchant's website	max 2048 *
$Pan - credit card number used for device authentication over 3-D Secure	max 19
$LastFourDigitsOfPAN - last 4 digits of credit card number used for device authentication over 3-D Secure	max 4
$PurchaseCurrency - 3 character currency code for the currency of the purchase	max 3
$PurchaseDateTime - date and time of the purchase in the system	22
$PurchaseDescription - description of the purchase when using device authentication over 3-D Secure	max 125 *
$PurchaseDisplayAmount - purchase amount displayed for purchase when using device authentication over 3-D Secure	max 20
$PurchaseXID - merchant's purchase ID when using device authentication over 3-D Secure	28
$RecurringEndDate - end date for a recurring payment	10
$RecurringFrequency - recurring frequency for the purchase in days	max 4

SMS Template Parameters	Length (char)
$TokenA - the one time password. Subsequent tokens for the batch SMS can be displayed as **$TokenB**, **$TokenC**, **$TokenD**,...	max 8

- The parameter can contain Unicode characters, but presenting Unicode characters will reduce the maximum size allowed from 160 to 70 characters.

> **Note**
>
> To be able to send SMS with templates in languages other than English or using symbols in the SMS Template, you must set the following system property in the application server's configuration file: `smpp.default_alphabet` .
>
> > **Example**
> >
> > For Tomcat, set `\-Dsmpp.default_alphabet=ie.omk.smpp.util.UCS2Encoding` in the **TOMCAT_HOME/bin/catalina.bat** or **catalina.sh**.

Email

System Management > Authentication Management > Device Management > Edit Default Device Parameters - Email

Email is a virtual device natively supported by ActiveAccess to provide email OTP authentication.

The Email device can be used as a backup device.

The Email device parameters page is where the administrator can setup the system for sending OTP via email.

Use the following fields to edit email Parameters:

- **Device type** - **Email**
- **Token lifetime** - determines the validity period of email tokens in minutes (acceptable range is 0 to 10). Following the sending of an email, the token will be valid for the period specified by this option. The default lifetime of email tokens is 10 minutes. You should consider the network delay for sending email messages and give enough time for user to enter the token.

- **Token length** - determines the number of digits in the generated token (acceptable range is 6 to 10). The default size is 6 digits.
- **Maximum unsuccessful attempts to send an email** - (acceptable range is 0 to 9) if sending an OTP by email fails due to network or application errors such as connection problems to the mail server or receiving a delivery error, the system attempts to resend the email message up to the number of times specified by this option. The default value is 5. If all attempts for delivering an OTP by email fail, an error is reported back to the administration user.
- **Mail server address, Mail server port, Mail server username, Mail server password**, **Mail server protocol** and **Mail sender** - Enter the address of an outgoing SMTP mail server with a valid username and password

> **Note**
>
> The sender of the notification messages will be the main administrator user (administrator). Make sure that you have specified a correct email address for this user (use **Edit Profile** link, while logged in as the administrator).

- **Minimum wait before the updated email address can be used** (acceptable range is 0 to 9999). 0 to disable this option.
- **Use as backup device** - Turn this option on if you would like **Email** to be used as a backup device. A backup device can be activated once a user reports a device lost or damaged, or requests the helpdesk to disable the device temporarily.
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and one-time password.
- **Email Templates** - Click on the link to **Edit Default Templates** for Activation During Shopping (ADS), Authentication, Activation via Authentication or Activation/Registration via MIA.
- **Send Test Email** - Click on the link to send a test email.

> **Note**
>
> The sender of the test emails will be the main administrator user (administrator). Make sure that you have specified a correct email address for this user (use **Edit Profile** link, while logged in as the administrator).

- ***Apply*** button to save changes.

Email Template

System Management > Authentication Management > Device Management > Edit Default Device Parameters - Email > Email Templates > Edit Default Templates

Use this section to edit the default email templates for:

- Activation During Shopping (ADS)
- Authentication
- Activation via Authentication
- Activation/Registration via MIA
- Subject of Activation During Shopping (ADS)
- Subject of Authentication
- Subject of Activation via Authentication
- Subject of Activation/Registration via MIA.

Use the following fields to edit an Email Template:

- **Type** - **Email** (this cannot be changed)
- **Template name** , the options are:
  - Activation During Shopping (ADS)
  - Authentication
  - Activation via Authentication
  - Activation/Registration via MIA
  - Subject of Activation During Shopping (ADS)
  - Subject of Authentication
  - Subject of Activation via Authentication
  - Subject of Activation/Registration via MIA.
- **Content type** - **Plain** or **HTML** !!! note This field is only available for templates of the email body.
- **Template** - Enter the default content for the email to be sent to the user when email OTP authentication is requested.

Info

Click the adjacent **Help** button for a full list of parameters. The default phrase can incorporate the following details, where appropriate:

Email Template Parameters	Length (char)
$CardExpiryDate - expiry date of the credit card	5
$CardHolderName - cardholder name as specified in the system	max 64
$CardProvider - card scheme name for the credit card	max 21
$CurrencySymbol - the currency symbol for the purchase when using device authentication over 3-D Secure	max 3
$IssuerName - issuer's name as defined in the system	max 256 *
$MerchantCountry - 3 character country code of the Merchant's country	3
$MerchantName - Merchant's name for the purchase when using device authentication over 3-D Secure	max 25 *
$MerchantURL - URL of the Merchant's website	max 2048 *
$Pan - credit card number used for device authentication over 3-D Secure	max 19
$LastFourDigitsOfPAN - last 4 digits of credit card number used for device authentication over 3-D Secure	max 4
$PurchaseCurrency - 3 character currency code for the currency of the purchase	max 3
$PurchaseDateTime - date and time of the purchase in the system	22
$PurchaseDescription - description of the purchase when using device authentication over 3-D Secure	max 125 *
$PurchaseDisplayAmount - purchase amount displayed for purchase when using device authentication over 3-D Secure	max 20

Email Template Parameters	Length (char)
$PurchaseXID - Merchant's purchase ID when using device authentication over 3-D Secure	28
$RecurringEndDate - end date for a recurring payment	max 10
$RecurringFrequency - recurring frequency of the purchase in days	max 4
$TokenA - the one time password.	max 10
$ServicePhoneNumber - customer service phone number of the issuer	max 32
$IssuerEmail - issuer's email address	max 128

* The parameter can contain Unicode characters.

Backup Device

System Management > Authentication Management > Device Management > Edit Default Device Parameters - Backup Device

The backup device is a standalone backup token, which is software generated. It can be used multiple times, as configured in the Backup Device Parameters.

Use the following fields to edit Backup Device Parameters:

- **Device type** - **Backup Device**
- **Backup device lifetime** (acceptable range is 0 to 365 days)

  A value of 0 disables the device.
- **Max usage limit** - the maximum number of times the backup device can be used as (acceptable range is 0 to 9).

  A value of 0 disables the device.
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and a one-time password.
- ***Apply*** button to save changes.

CAP (M-Chip 2) & CAP (M-Chip 4)

System Management > Authentication Management > Device Management > Edit Default Device Parameters - CAP (M-Chip 2) or Edit Default Device Parameters - CAP(M-Chip 4)

Use the following fields to edit CAP (M-Chip 2) Parameters:

- **Device type** - **CAP (M-Chip 2) or CAP (M-Chip 4)**

The following fields are available for configuration by default for CAP (M-Chip 2):

- **IAF, IPB, Terminal verification result, Terminal country code, Transaction type, AIP, Card verification result, Amount other, CID, CVN, KDI, DAC, Maximum PSN size** and **Mode** (Response only or Challenge response) (acceptable range for field values is displayed in field hints, where appropriate).
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and one-time password.
- ***Apply*** button to save changes.

The following fields are available for configuration by default for CAP (M-Chip 4):

- **IAF, IPB, Terminal verification result, Terminal country code, Transaction type, AIP, Card verification result, Amount other, CID, CVN, KDI, DAC, Maximum PSN size, H, b** and **Mode** (Response only or Challenge response) (acceptable range for field values is displayed in field hints, where appropriate).
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and one-time password.
- ***Apply*** button to save changes.

RSA

System Management > Authentication Management > Device Management > Edit Default Device Parameters - RSA

Use the following fields to edit RSA Parameters:

- **Device type** - **RSA**
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and one-time password.

- ***Apply*** button to save changes.

VASCO

System Management > Authentication Management > Device Management > Edit Default Device Parameters - VASCO

VASCO Parameters:

- **Device type** - **VASCO**

The following manufacturer fields are available for configuration by default

- **CHECKCHALLENGE, CHKINACTDAYS, DERIVEVECTOR, DIAGLEVEL, EVENTWINDOW, GMTADJUST, HSMSLOTID, ITHRESHOLD, ITIMEWINDOW, ONLINESG, STHRESHOLD, STIMEWINDOW, STORAGEDERIVEKEY1, STORAGEDERIVEKEY2, STORAGEDERIVEKEY3, STORAGEDERIVEKEY4, STORAGEKEYID, SYNCWINDOW, TRANSPORTKEYID** and **MODE** (Response only or Challenge response) (acceptable range for field values is displayed in field hints, where appropriate).
- **OTP and Password** - Select this option when an authentication requires the user to enter both a static password and one-time password.
- ***Apply*** button to save changes.

Upload File

System Management > Authentication Management > Device Management > Upload File

This page is used to enter the details of the device seed file you wish to upload and to schedule the upload date and time.

The seed file is provided by the device manufacturer.

Use the following fields to upload a file:

- **Issuer**
- **Device type**
- Click the **Choose File** / **Browse...** button, adjacent to **File name**, to locate and select a device seed file to upload.

The **No file chosen** message will then be replaced by the **File name** of the file to be uploaded.

- **Key value** - The device manufacturer may provide a key for decrypting the seed file. Enter the key as provided by the device manufacturer.
- **Schedule Date** and **Time** when you want the uploaded data to be processed.

  Uploaded files scheduled to run in the past are set to run immediately.

  You may also leave these fields blank if you wish to process the uploaded data as soon as possible.

  > **Note**
  >
  > The data upload may take a long time to complete depending on the file size and line speed.

- ***Apply*** button to create the upload job file.

Find Device

System Management > Authentication Management > Device Management > Find Device

Find Device can be used to search for an authentication device based on a number of criteria such as serial number, range of serial numbers, creation data and type of device.

Use the following to find a device:

- **Issuer**
- **Creation date** and **time** (dd/mm/yyyy HH:MM) or specify a date and time range for the search result by entering dates and times in the **From** and **To** fields. The date and time format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.
- **Device type**
- **Device Serial number** or specify a range of numbers to search within:
  - **VASCO** - device serial number, e.g. 123456789000
  - **SMS** - phone number including country code, e.g. +61123456789
  - **RSA** - device serial number, e.g. 11234567890
  - **Email** - email address, e.g. jo.citizen@domain.com
  - **CAP (M-Chip 4)** - device serial number, e.g. 41234500000000005-000

    - **CAP (M-Chip 2)** - device serial number, e.g. 412345000000000005-000

- Click ***Search*** to display device details.

Device Search Result

System Management > Authentication Management > Device Management > Find Device > Search Result

This page displays

- A list of **Devices**
- **Device ID** link to the **Device Details** page
- **Delete**, **Mark as lost**, **Mark as damaged**, **Mark as disabled** and **Back** buttons

The following fields and links are displayed for each device

- **Select** - checkbox for selecting the device to use in conjunction with the **Delete**, **Mark as lost**, **Mark as damaged** and **Mark as disabled** buttons.
- *Device ID* link to the **Device Details** page
- **Serial number** - The unique device / authentication method identifier
- **Issuer** - The issuer name to which this device belongs
- **Device type** - The type/make of the device such as VASCO, RSA, Email, SMS, CHIP, etc
- **Status** - **Active/Lost/Damaged/Disabled**. Only an active device can be used in device authentication. If a device is reported lost, stolen, damaged or disabled, it must be flagged accordingly. A lost or damaged device can no longer be used for authentication and the user must be issued with a new device.

To Delete, Mark as lost, damaged or disabled, devices in the Search Results

- Click the checkbox adjacent to the appropriate device or the checkbox in the **Select** column heading, to select all devices.

> ⚠ **Warning**
>
> **Important:** The display of search results is limited to 400 records, however if you select all records, all records matching the search criteria will be affected by the action you choose to perform.

⚠ **Warning**

Performing the selected action on a large number of records may take a long time to complete and will generate the equivalent number of audit log records. Use this functionality on a large number of records diligently and only where strictly necessary.

- Click the appropriate **Delete**, **Mark as lost**, **Mark as damaged** or **Mark as disabled** button.

Device Details

System Management > Authentication Management > Device Management > Find Device > Device Details

This page is used to view details for the device selected on the **Find Device** page and to change device status if the device has been reported as lost, damaged or temporarily disabled.

The following fields and links are displayed

- **Device ID** - unique device ID
- **Issuer** - The issuer name to which this device belongs
- **Serial number** - The unique device / authentication method identifier
- **Device type** - The type / make of the device, e.g. VASCO, RSA, Email, CAP (M-Chip 4), CAP (M-Chip 2), SMS.
- **Status** - **Active/Lost/Damaged**. Only an active device can be used for authentication. If a device is reported lost, stolen or damaged, it must be flagged accordingly. A lost or damaged device can no longer be used for device authentication and the user must be issued with a new device.
- **Creation date** - The date on which the device was created.
- **Reported lost/damaged on** - displays the last time a token was reported lost or damaged.
- **Device Specific Parameters** - a number of device specific parameters may be displayed for each device. These parameters are determined by the device manufacturer / authentication method and are displayed for completeness.
- **Assigned Users** - link to a list of users assigned to this device.
- **Assigned Cards** - link to a list of cards assigned to this device.
- **Activate Device** - the link appears for devices marked as lost or damaged. This allows the administrator to re-activate the device for example when the user reports that the device has

been found, to save the user from the trouble of having to use a back up device or wait for the replacement to arrive. To activate the device, the administrator needs to enter a valid token generated by the device to confirm that the device is actually in the possession of the user again.

- **Reset device** - this option is currently supported for time-synchronous VASCO tokens. Such devices use an internal clock for generating the tokens which may gradually go out of sync with the authentication server time due to the internal clock's drift. Time synchronous devices automatically adjust this error with each authentication, as long as the time drift is within a reasonable range. The time drift on a device that has not been used for a long period of time may go outside the accepted window for automatic adjustment. In such a case, resetting the device will re-initialise the associated record and allows for a much larger window of synchronization. Before performing this action, the administrator should make sure that the user's account status is enabled and should confirm that the user is entering the token from a linked device by checking the device's serial number against the user account. If this does not resolve the problem, the administrator should reset the token and advice the user to perform another authentication. If resetting the device does not solve the problem, the device should be marked as damaged and a replacement ordered for the user.

Risk Management

> ➕ *Risk Management is a new section.*

This section is used to set up the risk chains, which are used to define the authentication process, and the risk adapters defined in the chain. The sequence in which cardholder credentials are passed to the risk adapters is also defined in the chain. Each risk chain adapter defines a condition, actions to be taken if the condition is met or not met, a match score, together with the number of transactions which must have been performed and on how many days.

For further information about risk-based authentication and risk chains and risk adapters, refer to risk-engine-adapter.

System Management > Authentication Management > Risk Management

This page displays:

- A list of **Risk Chains** and for each Risk Chain:
  - Checkbox to **Select** it
  - **Chain ID** link to Edit Risk Chain
  - A list of **Adapters** that are enabled for the risk chain
  - Link to **Configure risk adapters** for the risk chain
- ***Delete*** button to delete selected risk chains
- Link to Add Risk Chain
- Link to Risk Adapter Management

Add / Edit Risk Chain

System Management > Authentication Management > Risk Management > Add / Edit Risk Chain

Use the following fields to complete this page:

- **Chain ID**

- **Authentication Method Score Range** - Based on the risk score (a value between 0 and 100) returned from the risk evaluation, the ranges defined in the following fields will indicate which authentication method should be used for authenticating the cardholder for each risk score.
    - **Score range for frictionless** - if the risk score falls within this range, the cardholder will be authenticated frictionlessly.
    - **Score range for static password** - if the risk score falls within this range, the cardholder will be required to authenticate using static authentication data that has previously been assigned to them, e.g. static password.
    - **Score range for device** - if the risk score falls within this range, the cardholder will be required to authenticate using an authentication device that has previously been assigned to them, e.g. SMS OTP, Email OTP, Vasco, etc.
    - **Score range for OOB** - if the risk score falls within this range, the cardholder will be required to authenticate using the authentication method utilised by the OOB service, e.g. biometrics, push notifications, etc.
    - **Score range for decline** - if the risk score falls within this range, the authentication will be rejected.

Info

- The ranges defined must fully cover the range between 0 and 100
- Each range must have a begin and end value
- It is not required to have a score range for every authentication method. The score range for some authentication methods can be left blank if these authentication methods are not used by the issuer.
- The ranges can be defined in your preferred order, e.g. OOB can have a lower score range than device.
- Ranges can not overlap.

Example 1

Score range for frictionless: 0..40

Score range for static password: 41..50

Score range for device: 51..60

Score range for OOB: 61..80

Score range for decline: 81..100

Example 2

Score range for frictionless: 0..40

Score range for static password:

Score range for device: 61..100

Score range for OOB: 41..60

Score range for decline:

- ***Apply*** button to save changes
- ***Back*** button to return to the **Risk Chains** page.

Configure Risk Chain

System Management > Authentication Management > Risk Management > Configure Risk Chain

In this section, available Risk Adapters can be enabled/disabled, configured and prioritized for the corresponding risk chain.

This page displays:

- Chain ID
- A list of available **Risk Adapters** that can be configured for this Risk Chain, and for each Risk Adapter:
  - Checkbox to **Select** it. Risk Adapters can only be selected if they have been configured.
  - **Adapter ID** link to Configure Risk Adapter
  - **Move Up** and **Move Down** arrows to change the **Priority** of the risk adapter, i.e. the order in which the risk adapter is used in the risk chain
  - **Status**
    - Not configured
    - Configured
- ***Enable*** button to enable selected risk adapters
- ***Disable*** button to disable selected risk adapters
- ***Back*** button to return to the **Risk Management** page.

Configure Risk Adapter

System Management > Authentication Management > Risk Management > Configure Risk Chain > Configure Risk Adapter

This page displays:

- **Adapter ID**
- **Adapter name**

Use the following fields to complete this page:

- **Condition** which has been defined in the adapter and for each Condition:
  - **Matched behaviour** for when the Condition is matched
    - Continue
    - Finish
  - **Mismatched behaviour** for when the Condition is not matched
    - Continue
    - Finish
  - **Matched score** - the score produced when the condition is matched
  - **Condition value** - the transaction data is compared with this value to determine if it matches the condition or not.
- ***Apply*** button to save changes
- ***Back*** button to return to the **Config Risk Chain** page.

Risk Adapter Management

System Management > Authentication Management > Risk Management > Risk Adapter Management

The Risk Adapter Management page displays:

- A list of **Risk Adapters** and for each Risk Adapter:
  - Checkbox to **Select** it
  - **Adapter ID** - links to Edit Risk Adapter ID

  - **Adapter name**
  - **Risk adapter connector**
- **Delete** button to delete selected risk adapters
- Link to Register Risk Adapter
- Link to Risk Adapter Connector Management.

Register Risk Adapter

System Management > Authentication Management > Risk Management > Risk Adapter Management > Register Risk Adapter

Use the following fields to complete this page:

- **Adapter name**
- Select **Risk adapter connector** from the drop down list
- ***Apply*** button to save changes
- ***Back*** button to return to the **Risk Adapter Management** page.

Edit Risk Adapter

System Management > Authentication Management > Risk Management > Risk Adapter Management > Edit Risk Adapter

Use the following fields to complete this page:

- **Adapter ID**
- **Adapter name**
- Select **Risk adapter connector** from the drop down list
- ***Apply*** button to save changes
- ***Back*** button to return to the **Risk Adapter Management** page.

Risk Adapter Connector Management

System Management > Authentication Management > Risk Management > Risk Adapter Management > Risk Adapter Connector Management

This section is used to define one or more connectors for communicating with remote risk adapters, which are called by ActiveAccess for risk-based authentication.

> **Note**
>
> To establish a secure connection with Risk Adapters, you may need CA Certificates and a keystore.

The Risk Adapter Connector Management page displays:

- A list of **Risk Adapter Connectors** and for each Risk Adapter Connector:
  - Checkbox to **Select** it
  - **Name** - links to Edit Risk Adapter Connector
  - **URL**
- **Delete** button to delete selected risk adapters
- ***Back*** button to return to the **Risk Adapter Management** page
- Link to Add Risk Adapter Connector.

Add / Edit Risk Adapter Connector

System Management > Authentication Management > Risk Management > Risk Adapter Management > Add / Edit Risk Adapter Connector

Use the following fields to complete this page:

- **Name** of the Risk Adapter Connector
- **URL** of the Risk Adapter Connector
- **Connection timeout**
- **Read timeout**
- ***Apply*** button to save changes
- ***Back*** button to return to the **Risk Adapter Connector Management** page.

OOB Management

> ➕ *OOB Management is a new section.*

This section is used to register and manage the OOB adapters that are used for performing Out of Band (OOB) authentication challenges. For more information about OOB adapters, refer to OOB Adapter Specification.

OOB Management

System Management > Authentication Management > OOB Management

This page displays:

- A list of **OOB Adapters** and for each adapter:
  - Checkbox to **Select** it
  - **Adapter ID** link to Edit OOB Adapter
  - **Adapter name**
  - **OOB adapter connector**
- Link to Register OOB Adapter
- Link to OOB Adapter Connector Management
- ***Delete*** button to remove selected OOB adapters.

Register / Edit OOB Adapter

System Management > Authentication Management > OOB Management > Register / Edit OOB Adapter

Use the following fields to complete this page:

- **Adapter name**
- **OOB adapter connector**
- Select an **OOB server** from the drop down list.
- ***Apply*** button to save changes

- ***Back*** button to return to the **OOB Management** page.

OOB Adapter Connector Management

System Management > Authentication Management > OOB Management > OOB Adapter Connector Management

This section is used to define one or more Out of Band authentication connectors, which allow ActiveAccess to trigger the external OOB process and perform interactions with the cardholder for authentication.

This page displays:

- A list of **OOB Adapter Connectors** and for each connector:
    - Checkbox to **Select** it
    - **Name** link to Edit OOB Adapter Connector
    - **URL**
- Link to Add OOB Adapter Connector
- ***Delete*** button to remove selected OOB adapters.
- ***Back*** button to return to the **OOB Management** page.

Add / Edit OOB Adapter Connector

System Management > Authentication Management > OOB Management > OOB Adapter Connector Management > Add OOB Adapter Connector

Use the following fields to complete this page:

- **Name** of the OOB Adapter Connector
- **URL** of the OOB Adapter Connector
- **Connection timeout**
- **Read timeout**
- ***Apply*** button to save changes
- ***Back*** button to return to the **OOB Adapter Connector Management** page.

Public & Encryption Key Management

System Management > Public & Encryption Key Management

This section is used to provide or update the issuer's public and encryption keys. A valid public key must be defined for each issuer. The issuer system uses the issuer's public key to validate an issuer's signature. Issuers are required to sign their registration messages with a valid private key that corresponds to the public key as provided to the issuer system.

ActiveAccess uses encryption keys to encrypt cardholder data during communication between ActiveAccess and other hosts in the environment.

A KeyStore with the following details should be prepared for the encryption key that is to be uploaded, through Upload encryption key:

- **KeyStore type/format:** JCEKS
- **KeyStore provider:** SunJCE
- **Key algorithm:** DESede
- **Key size:** 112 or 168 bit
- **Key name:** can be any
- **No of keys in the KeyStore:** Only one key must be populated in the KeyStore

Such KeyStores can be easily created by the Java Keytool utility using the following command:

```
keytool -genseckey -alias enckey168 -keypass 123456 -keyalg DESede -keysize 168
-keystore enc-key.JKS -storepass 123456 -storetype JCEKS
```

This page displays for each key:

- **Owner**-
- **Owner Type** - type of the owner of the key, Issuer or Group
- **Certificate Information** -
- **Validity** - validity of the certificate
- **Issuer** - issuer of the certificate
- **Delete encryption key** link

- **Download public key** link
- **Download encryption key** link

Export Encryption Key

System Management > Export Encryption Key

Use the following fields to export the encryption key:

- **Encryption KeyStore** - Enter the File password.
- Click **Export**.

Upload Public Key

System Management > Upload Public Key

Use the following fields to view/ update public key details:

- **Issuer** or an **Issuer group**.A message is shown to indicate whether a public key is currently available for this item or not.
- Enter the path and filename for the **XML signing certificate**; you can use the **Choose File** / **Browse...** button.

  The system uses the public key contained in the certificate in order to validate the issuer signature when it receives messages through the registration server. Issuers must ensure that this certificate corresponds to the RSA private key, which is used in signing the registration messages.
- **Certificate information** - Displays the certificate information if one is already loaded for the selected issuer or the issuer group
- **Public Key** - Displays the public key in hexadecimal format if one is already loaded for the selected issuer or the issuer group
- ***Apply*** button to update public key information.
- ***Download*** button to save a previously uploaded certificate as a PEM encoded certificate.

Upload Encryption Key

System Management > Upload Encryption Key

Use the following fields to view / update encryption key details:

- **Issuer** or an **Issuer group**. A message is shown to indicate whether an encryption key is currently available for this item or not.
- **Choose File** button, adjacent to **Encryption KeyStore** to locate and select an encryption key file to upload.

  The **No file chosen** message or current file name will be replaced with the name of the file to be uploaded.

  The system uses the AES (128 Bits) key contained in the JKS KeyStore in order to encrypt/ decrypt cardholder data that is being transferred between ActiveAccess modules and other external hosts. Issuers must ensure that this AES key is used in encrypting and decrypting cardholder data at other external hosts.
- **KeyStore password** - File password for the Encryption KeyStore.
- **Encryption key** - Displays the key information if one is already loaded for the selected issuer or the issuer group
- ***Apply*** button to update public key information.

Exchange Configuration

System Management > Exchange Configuration

Business rules are configurable settings which provide issuers control over the customer process during the 3-D Secure transactions. The Amount Threshold rule is used to determine whether authentication can be bypassed based on an amount threshold. To cater for this requirement, it is necessary to set a threshold amount in a default currency. Where the default currency is the same as the transaction currency, this calculation is straightforward. However, where these currencies differ, it is necessary to first convert the transaction currency to an equivalent value in the default currency before calculating whether the threshold has been exceeded. In order to compare the default currency and transaction currency values where they differ, it is necessary to maintain a list of currency exchange rates.

To automate the maintenance of currency exchange values, the ACS system has been configured to automatically download an external currency exchange rate resource file. Where this list of rates is not comprehensive, and a transaction is received which is in a currency not found on the automated list, this section provides the necessary functionality to manually create currency exchange values.

The Exchange Configuration page shows a list of manually configured currency rates. The Base Currency signifies the transaction currency whilst the Target Currency signifies the currency of the issuer threshold as configured in the currency value on the Amount Threshold rule page. The Rate value is used as a multiplier, to convert an amount in the Base Currency to an equivalent amount in the Target Currency. Manual exchange rates can be edited by clicking on the *Base Currency* link.

Links are provided to *View automatic exchange rates* and *View effective exchange rates* and *Add* for adding a manual exchange rate.

This page displays:

- **Manual Exchange Rates** list
- *View automatic exchange rates* link to the **Automatic Exchange Rates** page
- *View effective exchange rates* link to the **Effective Exchange Rates** page
- *Add* link to the **Add Exchange Rate** page
- **Delete** button to allow selected exchange rates to be deleted

The following fields and links are displayed for each exchange rate:

- **Base Currency** link to the **Edit Exchange Currency** page
- **Target Currency**
- **Rate**
- **Last Update** - Shows the date and time the exchange rate was last updated.

Add Exchange Configuration

System Management > Exchange Configuration > Add > Add Exchange Rate

Use this page to add an exchange rate that is not supported by the automated currency exchange file.

Use the following fields to add a currency exchange rate:

- **Base Currency**
- **Target Currency** for the currency of the issuer threshold as configured in the currency value on the Amount Threshold rule page.
- **Rate** which should be multiplied by the Base Currency to equal the amount in the Target Currency.

> ⚠ **Warning**
>
> Note that values entered here take precedence over those rates obtained by the automatic exchange rates feed when they have been updated more recently than the automatic updates.

- ***Apply*** button to save the currency exchange rate.

Edit Exchange Configuration

System Management > Exchange Configuration > Add > Edit Exchange Rate

Use this section to edit currency rates that have been manually created through the Exchange Rate section.

- On the **Exchange Configuration** page, select the *Base Currency* link.

  The **Edit Exchange Rate** page is displayed.

- The **Base Currency** and the **Target Currency** are displayed and cannot be changed.
- Enter a value for the **Rate** which should be multiplied by the Base Currency to equal the amount in the Target Currency.

> ⚠ **Warning**
>
> Note that values entered here take precedence over those rates obtained by the automatic exchange rates feed when they have been updated more recently than the automatic updates.

- ***Apply*** button to save the currency exchange rate.

View Automatic Exchange Rates

Use this page to view the automatic exchange rates held in the system.

This page displays:

- **Automatic Exchange Rates** list
- **View manual exchange rates**
- **View effective exchange rates**
- **Refresh list** to update the list with the most recent exchange rates.

The following fields and links are displayed for each exchange rate:

- **Base Currency**
- **Target Currency**
- **Rate**
- **Last Update** - Shows the date and time the exchange rate was last updated.

CurrencyConvertor.properties file

You can specify the currency exchange settings by editing the **CurrencyConvertor.properties** file located in ActiveAccess' **AA_HOME** directory on the server. The following parameters are configurable in this file:

AUD_URL: Specifies the URL of the feed that provides Australian Dollar exchange rates. The default is http://www.rba.gov.au/rss/rss-cb-exchange-rates.xml.

MAX_UNSUCCESSFUL_TRY: Specifies the number of times an attempt can be made to connect to try to the exchange feed URL before giving up in the case of an error is displayed.

AUD_FILE_TYPE: Specifies the format of the currency feed for the Australian Dollar. Default is XML.

RETRY_INTERVAL: Specifies the time in seconds that the system waits before sending another request in the case of error. Default is 30.

AUD_DATE_PATTERN: Specifies the format for date and time.

UPDATE_PERIOD: Specifies how often exchange rates are updated (hours). Default is 24.

PROXY_HOST: If required specifies the proxy address to be used for connecting to the exchange feed. Default is blank.

PROXY_PORT: If required specifies the proxy port to be used for connecting to the exchange feed. Default is blank.

PROXY_USER: If required, specifies the user name to be used to connect via the proxy. Default is blank.

PROXY_PASSWORD: If required, specifies the password to be used for connecting via the proxy. Default is blank.

ActiveAccess server should be restarted for changes to take effect.

Note

Automatic Exchange Rates rely on access to the Internet or an external resource configured to retrieve these details. If no access is available, the following message is displayed "Loading effective exchange rates, please wait..."

View Effective Exchange Rate

Use this page to view the effective exchange rates.

This page displays:

- **Effective Exchange Rates** list
- **View manual exchange rates** link to the **Manual Exchange Rates** page
- **View automatic exchange rates** link to the **Automatic Exchange Rates** page

- **Refresh list** to update the list with the most recent exchange rates.

The following fields and links are displayed for each exchange rate:

- **Base Currency**
- **Target Currency**
- **Rate**
- **Last Update** - Shows the date and time the exchange rate was last updated.

> **Note**
>
> Effective Exchange Rates rely on access to the Internet or an external resource configured to retrieve these details. If no access is available, the following message is displayed "Loading effective exchange rates, please wait..."

Archive Management

System Management > Archive Management

The **Archive Management** section is used to define automatic archive settings and review the history of previous archives.

An automatic archive process can be scheduled to run at a specified time to collect records that are older than a specified date. Several archive databases can be introduced to the archive procedure but only ones which are not closed can be used for the scheduled archive procedure.

Archived databases can be chosen as the default for transaction and audit log search purposes.

Links are provided to Archive Databases, Edit Archive Settings, Archive Database Details and Archive history details pages.

This page displays:

- **Archive Settings**
- **Archive Databases** link to the **Archive Databases** page
- **Edit** link to the **Archive Settings** page

Edit Archive Settings

Use the following fields and links to edit the archive settings:

- **Automatic archive** checkbox to enable / disable automatic archiving
- **Start date** for archiving in dd/mm/yyyy format
- **Start time** for archiving in hh:mm format
- **Archive old records every**, and select **Days** or **Months** from the drop down list to specify how often records should be archived.
- **Collect records which are older than**, and select **Days** or **Months** from the drop down list to specify the age of records to archive.
- **Automatic archive purge** checkbox to enable / disable automatic archive purging
- **Purge start date** for purging archived records in dd/mm/yyyy format

- **Purge start time** for purging archived records in hh:mm format
- **Purge old archived records every**, and select **Days** or **Months** from the drop down list to specify how often records should be archived.
- **Purge archived records which are older than**, and select **Days** or **Months** from the drop down list to specify the age of records to archive.
- ***Apply*** button to save the settings

Archive Databases

This page displays:

- **Archive Databases** list
- **New Archive Database**

The following fields and links are displayed for each archive database:

- **Select** radio button to indicate which archive database to delete
- **Archive database (Archive user)**
- **Creation date** - the date that the archive database was created.
- **End date** - the date that the archive database was closed. A database is closed once a new archive database is added. Closed archive databases are not used for archiving but can still be used for Transaction/Audit Log Searches.
- **Archive user status** - indicates which archive database is the default for Transaction and Audit Log searches
- **Set as default for Search** link for selecting a different archive database to use for Transaction and Audit Log searches

New Archive Database

Use the following fields to add a new Archive Database:

- Select either **Database Link** or **Database user**
- If the **Database link** radio button is selected, enter the **Database Link**.

This must be a valid database link to an ActiveAccess archive database with the schema that has already been defined in Archive/archive_schema.sql under the ActiveAccess package.

- If the **Database user** radio button is selected, enter a valid ActiveAccess archive database, with a schema that has already been defined in Archive/archive_schema.sql under the ActiveAccess package.

> **Note**
>
> The current ActiveAccess database user should have the appropriate access rights to the archive database user objects.

- ***Apply*** button to save the new Archive Database.

> **Note**
>
> Creating a new archive database closes the current archive database and all subsequently archived records are recorded in the new archive database.
> A closed archive database can still be accessed by selecting it as the default for Transaction/Audit Log searches.

Archive Database details

This page displays:

- Links to the **Archive history details** pages

The following fields and links are displayed in Archive Database Details page

- **Archive Database** is displayed and cannot be changed
- **Creation date** is displayed and cannot be changed
- **End date -** the date that the archive database was closed. A database is closed once a new archive database is added. Closed archive databases are not used for archiving but can still be used for Transaction/Audit Log Searches.
- **Archive History** tab - lists previous archive activities with a *link* to the **Archive history details** of each archive run.
- **Purge History** tab - lists previously purged archive activities with a link to the **Purge history details** of each purge archive run.

Archive History Details

The following fields and links are displayed:

- **Archive history details** for a specified archive date and time and record age
- **Table** - name of the database table archived
- **Number of Records Archived**

Purge History Details

The following fields and links are displayed

- **Purge history details** for a specified purge date and time and record age
- **Table** - name of the database table purged
- **Number of Records Purged**

Security

System Administrators only

The **Security** section is used for setting up and maintaining digital certificates that are used for verification of connections with external parties and signing messages.

⚠ **Warning**

Note that server certificate related tasks that allow authentication of ActiveAccess server to external clients such as browsers and directory servers have been delegated to the ActiveAccess container. This is the application/web server which is used to run ActiveAccess server. Please consult with your application server documentation for setting up and installing SSL server certificates.

***Security** has the following sub menu options:*

- **Issuer Certificate** - for setting up and maintaining the issuers' signing certificates that are used to sign PARes messages.
- **AHS Certificate** - for setting up and maintaining client certificates used for connections to the authentication history server.
- **CAAS Certificate** - for setting up and maintaining CAAS certificates used for connections to the remote CAAS server.
- **Directory Server Certificate** - + *new section* for setting up and maintaining client certificates used for connections to the Directory Server to send RReq.
- **OOB Certificate** - + *new section* for setting up and maintaining client certificates used for connections to the RESTful OOB adapters.
- **Risk Certificate** - + *new section* for setting up and maintaining client certificates used for connections to the RESTful RBA adapters.
- **CA Certificate** - for setting up and maintaining trusted certificates. ActiveAccess uses CA certificates to validate server certificates in outbound connections to external servers such as authentication history server.

Issuer Certificate

Security > Issuer Certificate

This section is used to setup and maintain issuers' signing certificates. Issuer certificates are used to sign PARes messages. The issuer certificates must be issued by the certificate authority designated by the 3-D Secure provider for this purpose.

The following fields and links are displayed:

- **Currently installed certificates** list
- **Create Certificate Request** for creating new certificate requests for issuers or groups
- **Install Certificate** for installation of signed certificates
- **Delete Selected Certificates** remove selected certificates.

The following fields and links are displayed for each issuer:

- **Owner**, either a group or an issuer, and links to the **Group Details** page or the **Issuer Details** page
- **Owner Type** - Shows whether the owner is a group or an issuer
- **Provider** - 3-D Secure provider of the certificate. The certificate is only used for 3-D Secure transactions, which belong to the same provider. Provider link enables certificate to be downloaded for viewing.
- **Certificate Information** - Certificate details such as Common Name (CN), Organization (O), Organization Unit (OU), Location (L), State (ST) and Country (C)
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.
- **Issuer** - The certificate authority (CA) who issued the certificate
- **Signature Algorithm** – The hash algorithm used to sign the certificate.

Create Certificate Request

Security > Issuer Certificate > Certificate Request

Use this section to create a certificate signing request (CSR) that can be sent to a designated certificate authority (CA) to obtain a signed certificate. The certificate used in signing PARes message must be signed by an appropriate CA which is designated by the scheme. You need a separately signed certificate for each supported scheme. The CSR is created in standard PKCS#10 format.

Use the following fields to create a CSR:

- Each scheme may have certain requirements regarding the format and content of CSR fields that need to be entered here. Please contact the scheme for information regarding creating a CSR. Please note that some fields may not be required by a scheme and that the following explanations are generic.
    - Select whether the CSR is for an **Issuer** or an **Issuer Group** and select the organization from the list
    - Select an authentication **Provider** (scheme) from the list
    - ➕ Select a **Key type** from the list. The options are **RSA (3DS1)**, used for signing 3D Secure 1 transactions, and **RSA (3DS2)**, used for signing 3D Secure 2 transactions.
    - If the RSA Signing key is inactive, the **Alias** list is displayed and you will be required to select an **Alias**. The RSA Signing key that is created with the PCIDSS Key Retiring Utility or through **Issuers** > **Key Management** will remain inactive until a certificate request is created and signed by card schemes, then installed for the specified Alias
    - The **Key size** will be displayed once a provider and a key type (and alias, if available) have been selected. The key size is based on the size of the RSA Signing Key of the provider for each issuer.
    - Select the **Hash Algorithm** to be used to create the certificate request from the list. Defaults to **SHA1**.
    - **Common Name** - a descriptive name for the certificate, for example 'Any Bank Signing Certificate'
    - **Organization** name - for example 'Any Bank'
    - **Organizational Unit** - the name of the department within the organization to which this certificate belongs, for example 'Card Services'
    - **City** - for example 'Sydney'
    - **Province** full name - for example 'New South Wales'
    - **Two-letter country code** - for example AU for 'Australia.'

Install Certificate

Security > Issuer Certificate > Install Certificate

Use this section to install a certificate which is signed by the CA. The signed certificate must correspond to a previously created CSR for the same issuer and must be in standard PKCS#7 format.

Use the following fields to install a signed certificate:

- Select the appropriate radio button to indicate whether the **Issuer** or the **Issuer Group** was previously used for creating the CSR.
- Select an authentication **Provider** (scheme) from the drop sdown list. Select the provider whose CA has signed the certificate.
- If the RSA Signing key is inactive, the **Alias** list is displayed and you will be required to select an **Alias**. The RSA Signing key that is created with the PCIDSS Key Retiring Utility or through **Issuers** > **Key Management** will remain inactive until a certificate request is created and signed by card schemes, then installed for the specified Alias.
- Use the **Certificate content (file)** field to locate the PKCS#7 file that contains the signed certificate or copy and paste the signed CSR (if in base64 text format) in the **Certificate content** field.

AHS Certificate

Security > AHS Certificate

This section is used to set up and maintain SSL client certificates which are used to authenticate ActiveAccess to the authentication history server. Note that not all 3-D Secure providers may require an authentication history server. Check with the 3-D Secure provider regarding creating AHS client certificates and the designated CA for signing the certificates.

The following fields and links are displayed:

- **Currently installed certificates** list
- *Create Certificate Request* links to the **AHS Certificate Request** page for creating a new AHS client certificate requests.

- *Install Certificate* links to the **Install AHS Certificate** page for installation of the signed AHS client certificate
- *Delete Selected Certificates* link used with the **Select** checkbox to remove selected certificates and associated private keys.
- *Import Certificate* links to the **Import AHS Certificate** page for direct installation of a signed AHS client certificate which contains a private key as well as a public key.

The following fields and links are displayed for each provider:

- **Owner** - the 3-D Secure provider and links to the **Export AHS Certificate** page. The certificate is only used for 3-D Secure transactions which belong to the same provider.
- **Certificate Information** - Certificate details such as Common Name (CN), Organization (O), Organization Unit (OU), Location (L), State (ST) and Country (C)
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.
- **Issuer** - The certificate authority (CA) that issued the certificate
- **Signature Algorithm** - The hash algorithm used to sign the certificate.

Create Certificate Request

Security > AHS Certificate > AHS Certificate Request

Use this section to create a certificate signing request (CSR) that can be sent to a designated certificate authority (CA) to obtain a signed certificate. The certificate is used in connection to the authentication history server designated by the 3-D Secure provided and must be signed by a CA approved by the respective 3-D Secure provider. The CSR is created in standard PKCS#10 format.

Use the following fields to create a CSR:

- Each scheme may have certain requirements regarding the format and content of CSR fields that need to be entered here. Please contact the scheme for information regarding creating a CSR. Please note that some fields may not be required by a scheme and that the following explanations are generic.
    - **Provider** (scheme)

  - **Common Name** - a descriptive name for the certificate for example 'Any Bank AHS Client Certificate'.
  - **Organization** - the name of your organization for example 'Any Bank'.
  - **Organization Unit** - the name of the department within the organization to which this certificate belong for example 'Card Services'.
  - **City** - for example 'Sydney'.
  - **Province** - enter the state or province full name for example 'New South Wales'.
  - **Two-letter country code** for example AU for 'Australia'.
  - **Key size** ,defaults to **1024**.
  - **Hash Algorithm** used to create the certificate request, defaults to **SHA1**.

Install AHS Certificate

Security > AHS Certificate > Install AHS Certificate

Use this section to install a certificate which is signed by the CA. The signed certificate must correspond to a previously created CSR for the same provider and must be in standard PKCS#7 format.

Use the following fields to install a signed certificate:

- **Provider** (scheme) - Select the provider whose CA has signed the certificate.
- Click the **Choose File** / **Browse...** button adjacent to **Certificate content (file)**, to locate and select the PKCS#7 file that contains the signed certificate *or* copy and paste the signed CSR (base64 text format) into the **Certificate content** text box.

Export AHS Certificate

Security > AHS Certificate > Export AHS Certificate

Use this section to export the SSL client certificate in a number of formats including PKCS#12 which allows you to export both private and public keys.

Use the following fields to export a certificate:

- **Provider** (scheme).

- **Type**, the options are:
  - **KeyStore** - to export both private and public keys
  - **Certificate** - to export the public key in DER binary encoded X509 format
  - **Certificate path** - to export the entire certificate chain in P7B format.
- If the export type selected is KeyStore, select from the **Format** list:
  - **PFX** to export in standard PKCS#12 format
  - **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications.
- If the export type selected is KeyStore, enter a **File password** to protect the private key.

Import AHS Certificate

Security > AHS Certificate > Import AHS Certificate

The 3-D Secure provider may issue an SSL certificate which contains both the public and private key and is already signed. You may install this type of certificate using the import functionality provided in this section.

Use the following fields to import a certificate:

- **Provider** (scheme) .
- Select the certificate **Format.** Supported formats are **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications or **PFX** to export in standard PKCS#12 format.
- Click the **Choose File** / **Browse...** button to locate and select the **File**
- Enter the **File password** which is used to protect the private key.

CAAS Certificate

Security > CAAS Certificate

This section is used to set up and maintain SSL client certificates which are used to authenticate ActiveAccess to the CAAS server. Note that the CAAS server may use mutual SSL authentication to verify the client, which in this case is ActiveAccess. Check with the CAAS server provider for more details.

The following fields and links are displayed:

- **Currently installed certificates** list
- **Create Certificate Request** for creating a new CAAS client certificate requests.
- **Install Certificate** for installation of the signed CAAS client certificate
- **Delete Selected Certificates** link used with the **Select** checkbox to remove selected certificates and associated private keys.
- **Import Certificate** for direct installation of a signed CAAS client certificate that contains a private key as well as a public key.

The following fields and links are displayed for each provider:

- **Certificate Information** links to the **Export CAAS Certificate** page. The **Certificate Information** contains certificate details such as Common Name (CN), Organization (O), Organization Unit (OU), Location (L), State (ST) and Country (C)
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.
- **Issuer** - The certificate authority (CA) that issued the certificate
- **Signature Algorithm** - The hash algorithm used to sign the certificate.

Create Certificate Request

Security > CAAS Certificate > CAAS Certificate Request

Use this section to create a certificate signing request (CSR) that can be sent to a designated certificate authority (CA) to obtain a signed certificate. The certificate is used in connection to the authentication history server designated by the 3-D Secure provided and must be signed by a CA approved by the respective 3-D Secure provider. The CSR is created in standard PKCS#10 format.

Use the following fields to create a CSR:

- Each scheme may have certain requirements regarding the format and content of CSR fields that need to be entered here. Please contact the scheme for information regarding creating a

CSR. Please note that some fields may not be required by a scheme and that the following explanations are generic.

- **Common Name** - a descriptive name for the certificate for example 'caas-client'.
- **Organization** - the name of your organization for example 'Internet Widgits Pty Ltd'.
- **Organization Unit** - the name of the department within the organization to which this certificate belong for example 'Caas Services'.
- **City** for example 'Sydney'.
- **Province** - enter the full name of the state or province, for example 'New South Wales'.
- **Two-letter country code**, for example AU for 'Australia'.
- Select a **Key size** from the list. Defaults to **1024**.
- Select the **Hash Algorithm** to be used to create the certificate request from the list. Defaults to **SHA1**.

Install CAAS Certificate

Security > CAAS Certificate > Install CAAS Certificate

Use this section to install a certificate which is signed by the CA. The signed certificate must correspond to a previously created CSR for the same provider and must be in standard PKCS#7 format.

Use the following fields to install a signed certificate:

- Click the **Choose File** / **Browse...** button adjacent to **Certificate content (file)**, to locate and select the PKCS#7 file that contains the signed certificate *or* copy and paste the signed CSR (base64 text format) into the **Certificate content** text box.

Export CAAS Certificate

Security > CAAS Certificate > Export CAAS Certificate

Use this section to export the SSL client certificate in a number of formats including PKCS#12 which allows you to export both private and public keys.

Use the following fields to export a certificate:

- Select the export **Type** from the list. The options are:
    - **KeyStore** - to export both private and public keys
    - **Certificate** - to export the public key in DER binary encoded X509 format
    - **Certificate path** - to export the entire certificate chain in P7B format.
- If the export type selected is KeyStore, select from the **Format** drop down list:
    - **PFX** to export in standard PKCS#12 format
    - **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications.
- If the export type selected is KeyStore, enter a **File password** to protect the private key.

Import CAAS Certificate

Security > CAAS Certificate > Import CAAS Certificate

The CAAS server operator may issue an SSL certificate which contains both the public and private key and is already signed. You may install this type of certificate using the import functionality provided in this section.

Use the following fields to import a certificate:

- Select the certificate **Format.** Supported formats are **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications or **PFX** to export in standard PKCS#12 format.
- Click the **Choose File** / **Browse...** button to locate and select the **File**
- Enter the **File password** which is used to protect the private key.

Directory Server Certificate

Security > Directory Server Certificate

➕ *New section.*

This section is used to set up and maintain client certificates used for connections to the Directory Server to send RReq.

The following fields and links are displayed:

- **Currently installed certificates** list
- *Create Certificate Request* links to the **Directory Server Certificate Request** page for creating a new AHS client certificate requests.
- *Install Certificate* links to the **Install Directory Server Certificate** page for installation of the signed Directory Server certificate
- *Delete Selected Certificates* link used with the **Select** checkbox to remove selected certificates and associated private keys.
- *Import Certificate* links to the **Import Directory Server Certificate** page for direct installation of a signed Directory Server certificate which contains a private key as well as a public key.

The following fields and links are displayed for each provider:

- **Owner** - the 3-D Secure provider and links to the **Export Directory Server Certificate** page. The certificate is only used for 3-D Secure transactions which belong to the same provider.
- **Certificate Information** - Certificate details such as Common Name (CN), Organization (O), Organizational Unit (OU), Location (L), State (ST) and Country (C), Key size, Hash algorithm.
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.
- **Issuer** - The certificate authority (CA) that issued the certificate
- **Signature Algorithm** - The hash algorithm used to sign the certificate.

Create Certificate Request

Security > Directory Server Certificate > Directory Server Certificate Request

Use this section to create a certificate signing request (CSR) that can be sent to a designated certificate authority (CA) to obtain a signed certificate. The certificate is used in connection to the authentication history server designated by the 3-D Secure provided and must be signed by a CA approved by the respective 3-D Secure provider. The CSR is created in standard PKCS#10 format.

Use the following fields to create a CSR:

- Each scheme may have certain requirements regarding the format and content of CSR fields that need to be entered here. Please contact the scheme for information regarding creating a CSR. Please note that some fields may not be required by a scheme and that the following explanations are generic.
    - **Provider** (scheme)
    - **Common Name** - a descriptive name for the certificate for example 'Any Bank Directory Server Certificate'.
    - **Organization** - the name of your organization for example 'Any Bank'.
    - **Organizational Unit** - the name of the department within the organization to which this certificate belong for example 'Card Services'.
    - **City** - for example 'Sydney'.
    - **Province** - enter the state or province full name for example 'New South Wales'.
    - **Two-letter country code** for example AU for 'Australia'.
    - **Key size** ,defaults to **1024**.
    - **Hash Algorithm** used to create the certificate request, defaults to **SHA1**.

Install Directory Server Certificate

Security > Directory Server Certificate > Install Directory Server Certificate

Use this section to install a certificate which is signed by the CA. The signed certificate must correspond to a previously created CSR for the same provider and must be in standard PKCS#7 format.

Use the following fields to install a signed certificate:

- **Provider** (scheme) - Select the provider whose CA has signed the certificate.
- Click the **Choose File** / **Browse...** button adjacent to **Certificate content (file)**, to locate and select the PKCS#7 file that contains the signed certificate *or* copy and paste the signed CSR (base64 text format) into the **Certificate content** text box.

Export Directory Server Certificate

Security > Directory Server Certificate > Export Directory Server Certificate

Use this section to export the SSL client certificate in a number of formats including PKCS#12 which allows you to export both private and public keys.

Use the following fields to export a certificate:

- **Provider** (scheme).
- **Type**, the options are:
    - **KeyStore** - to export both private and public keys
    - **Certificate** - to export the public key in DER binary encoded X509 format
    - **Certificate path** - to export the entire certificate chain in P7B format.
- If the export type selected is KeyStore, select from the **Format** list:
    - **PFX** to export in standard PKCS#12 format
    - **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications.
- If the export type selected is KeyStore, enter a **File password** to protect the private key.

Import Directory Server Certificate

Security > Directory Server Certificate > Import Directory Server Certificate

The 3-D Secure provider may issue an SSL certificate which contains both the public and private key and is already signed. You may install this type of certificate using the import functionality provided in this section.

Use the following fields to import a certificate:

- **Provider** (scheme) .
- Select the certificate **Type** Supported formats are **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications or **PFX** to export in standard PKCS#12 format.
- Click the **Choose File** / **Browse...** button to locate and select the **File**
- Enter the **File password** which is used to protect the private key.

OOB Certificate

➕ *New section.*

Security > OOB Certificate

This section is used to set up and maintain client certificates used for connections to the RESTful OOB adapters.

The following fields and links are displayed:

- **Currently installed certificates** list
- *Create Certificate Request* links to the **OOB Server Certificate Request** page for creating a new AHS client certificate requests.
- *Install Certificate* links to the **Install OOB Server Certificate** page for installation of the signed OOB Server certificate
- *Delete Selected Certificates* link used with the **Select** checkbox to remove selected certificates and associated private keys.
- *Import Certificate* links to the **Import OOB Server Certificate** page for direct installation of a signed OOB Server certificate which contains a private key as well as a public key.

The following fields and links are displayed for each provider:

- **OOB Server** name - links to the **Export OOB Server Certificate** page.
- **Certificate Information** - Certificate details such as Common Name (CN), Organization (O), Organizational Unit (OU), Location (L), State (ST) and Country (C).
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.
- **Issuer** - The certificate authority (CA) that issued the certificate
- **Signature Algorithm** - The hash algorithm used to sign the certificate.

Create Certificate Request

Security > OOB Server Certificate > OOB Server Certificate Request

Use this section to create a certificate signing request (CSR) that can be sent to a designated certificate authority (CA) to obtain a signed certificate. The certificate is used in connection to the authentication history server designated by the 3-D Secure provided and must be signed by a CA approved by the respective 3-D Secure provider. The CSR is created in standard PKCS#10 format.

Use the following fields to create a CSR:

- Each scheme may have certain requirements regarding the format and content of CSR fields that need to be entered here. Please contact the scheme for information regarding creating a CSR. Please note that some fields may not be required by a scheme and that the following explanations are generic.
    - **OOB Server** - select from the list.
    - **Common Name** - a descriptive name for the certificate for example 'Any Bank OOB Server Certificate'.
    - **Organization** - the name of your organization for example 'Any Bank'.
    - **Organizational Unit** - the name of the department within the organization to which this certificate belong for example 'Card Services'.
    - **City** - for example 'Sydney'.
    - **Province** - enter the state or province full name for example 'New South Wales'.
    - **Two-letter country code** for example AU for 'Australia'.
    - **Key size** ,defaults to **1024**.
    - **Hash Algorithm** used to create the certificate request, defaults to **SHA1**.

Install OOB Server Certificate

Security > OOB Server Certificate > Install OOB Server Certificate

Use this section to install a certificate which is signed by the CA. The signed certificate must correspond to a previously created CSR for the same provider and must be in standard PKCS#7 format.

Use the following fields to install a signed certificate:

- **OOB Server** - select from the list.

- Click the **Choose File** / **Browse…** button adjacent to **Certificate content (file)**, to locate and select the PKCS#7 file that contains the signed certificate *or* copy and paste the signed CSR (base64 text format) into the **Certificate content** text box.

Export OOB Server Certificate

Security > OOB Server Certificate > Export OOB Server Certificate

Use this section to export the SSL client certificate in a number of formats including PKCS#12 which allows you to export both private and public keys.

Use the following fields to export a certificate:

- **OOB Server** - select from the list.
- **Type**, the options are:
    - **KeyStore** - to export both private and public keys
    - **Certificate** - to export the public key in DER binary encoded X509 format
    - **Certificate path** - to export the entire certificate chain in P7B format.
- If the export type selected is KeyStore, select from the **Format** list:
    - **PFX** to export in standard PKCS#12 format
    - **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications.
- If the export type selected is KeyStore, enter a **File password** to protect the private key.

Import OOB Server Certificate

Security > OOB Server Certificate > Import OOB Server Certificate

The 3-D Secure provider may issue an SSL certificate which contains both the public and private key and is already signed. You may install this type of certificate using the import functionality provided in this section.

Use the following fields to import a certificate:

- **OOB Server** - select from the list.

- Select the certificate **Type** Supported formats are **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications or **PFX** to export in standard PKCS#12 format.
- Click the **Choose File** / **Browse...** button to locate and select the **File**
- Enter the **File password** which is used to protect the private key.

Risk Certificate

➕ *New section*.

Security > Risk Certificate

This section is used to set up and maintain client certificates used for connections to the RESTful RBA adapters.

The following fields and links are displayed:

- **Currently installed certificates** list
- *Create Certificate Request* links to the **Risk Server Certificate Request** page for creating a new AHS client certificate requests.
- *Install Certificate* links to the **Install Risk Server Certificate** page for installation of the signed Risk Server certificate
- *Delete Selected Certificates* link used with the **Select** checkbox to remove selected certificates and associated private keys.
- *Import Certificate* links to the **Import Risk Server Certificate** page for direct installation of a signed Risk Server certificate which contains a private key as well as a public key.

The following fields and links are displayed for each provider:

- **Risk Server** name - links to the **Export Risk Server Certificate** page.
- **Certificate Information** - Certificate details such as Common Name (CN), Organization (O), Organizational Unit (OU), Location (L), State (ST) and Country (C).
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.

- **Issuer** - The certificate authority (CA) that issued the certificate
- **Signature Algorithm** - The hash algorithm used to sign the certificate.

Create Risk Server Certificate Request

Security > Risk Certificate > Risk Server Certificate Request

Use this section to create a certificate signing request (CSR) that can be sent to a designated certificate authority (CA) to obtain a signed certificate. The certificate is used in connection to the authentication history server designated by the 3-D Secure provided and must be signed by a CA approved by the respective 3-D Secure provider. The CSR is created in standard PKCS#10 format.

Use the following fields to create a CSR:

- Each scheme may have certain requirements regarding the format and content of CSR fields that need to be entered here. Please contact the scheme for information regarding creating a CSR. Please note that some fields may not be required by a scheme and that the following explanations are generic.
    - **Risk Server** - select from the list.
    - **Common Name** - a descriptive name for the certificate for example 'Any Bank Risk Server Certificate'.
    - **Organization** - the name of your organization for example 'Any Bank'.
    - **Organizational Unit** - the name of the department within the organization to which this certificate belong for example 'Card Services'.
    - **City** - for example 'Sydney'.
    - **Province** - enter the state or province full name for example 'New South Wales'.
    - **Two-letter country code** for example AU for 'Australia'.
    - **Key size** ,defaults to **1024**.
    - **Hash Algorithm** used to create the certificate request, defaults to **SHA1**.

Install Risk Server Certificate

Security > Risk Certificate > Install Risk Server Certificate

Use this section to install a certificate which is signed by the CA. The signed certificate must correspond to a previously created CSR for the same provider and must be in standard PKCS#7 format.

Use the following fields to install a signed certificate:

- **Risk Server** - select from the list.
- Click the **Choose File** / **Browse…** button adjacent to **Certificate content (file)**, to locate and select the PKCS#7 file that contains the signed certificate *or* copy and paste the signed CSR (base64 text format) into the **Certificate content** text box.

Export Risk Server Certificate

Security > Risk Certificate > Export Risk Server Certificate

Use this section to export the SSL client certificate in a number of formats including PKCS#12 which allows you to export both private and public keys.

Use the following fields to export a certificate:

- **Risk Server** - select from the list.
- **Type**, the options are:
    - **KeyStore** - to export both private and public keys
    - **Certificate** - to export the public key in DER binary encoded X509 format
    - **Certificate path** - to export the entire certificate chain in P7B format.
- If the export type selected is KeyStore, select from the **Format** list:
    - **PFX** to export in standard PKCS#12 format
    - **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications.
- If the export type selected is KeyStore, enter a **File password** to protect the private key.

Import Risk Server Certificate

Security > Risk Server Certificate > Import Risk Server Certificate

The 3-D Secure provider may issue an SSL certificate which contains both the public and private key and is already signed. You may install this type of certificate using the import functionality provided in this section.

Use the following fields to import a certificate:

- **Risk Server** - select from the list.
- Select the certificate **Type** Supported formats are **JKS** to export in the Java KeyStore format used by the Java Keytool and most Java-based applications or **PFX** to export in standard PKCS#12 format.
- Click the **Choose File** / **Browse...** button to locate and select the **File**
- Enter the **File password** which is used to protect the private key.

CA Certificate

Security > CA Certificate

This section is used to set up and maintain trusted certificate authority certificates. ActiveAccess uses this list in order to validate the certificate chain of installed certificates and to authenticate remote connections to external SSL enable servers such as the authentication history server.

ActiveAccess is installed with the most recent CA certificates from 3-D Secure providers. However, you may need to maintain and add new certificates they may be introduced at a later time by the 3-D Secure provider or in order to test with non-production 3-D Secure systems that use a different CA.

The following fields and links are displayed:

- **Currently installed certificates** list
- *Import CA Certificate* links to the **Import CA Certificate** page for installation of trusted root certificates.
- *Delete Selected Certificates* link used with the **Select** checkbox to remove selected certificates.

The following fields and links are displayed for each provider:

- **Owner** - the 3-D Secure provider. Clicking on the link allows you to save the certificate in DER binary encoded X509 certificate format.
- **Type** - displays the key type
- **Certificate Information** - Certificate details such as Common Name (CN), Organization (O), Organizational Unit (OU), Location (L), State (ST) and Country (C)
- **Validity** - Shows the validity period of the certificate
- **Status** - The status of a certificate can either be **Valid**, **Expired** or **Not signed**. You need to reapply for certificates before they expire. A certificate status is shown as not signed if the certificate is not signed by a trusted certificate authority.
- **Issuer** - The certificate authority (CA) that issued the certificate.
- **Signature Algorithm** - The hash algorithm used to sign the certificate.

Import Certificate

Security > CA Certificate > Import CA Certificate

This section allows you to install additional trusted root certificates.

ActiveAccess is installed with the most recent CA certificates from 3-D Secure providers. However, you may need to maintain and add new certificates they may be introduced at a later time by the 3-D Secure provider or in order to test with non-production 3-D Secure systems that use a different CA.

Use the following fields to import a certificate:

- **Provider** - select the scheme from the list
- **Key type** - select the key type from the list
- Click the **Choose File** / **Browse...** button to locate and select the **File**. ActiveAccess supports X509 certificates in DER encoded binary or based64 encoded formats.

Servers

System Administrators only

This section is used to manage administration and access control server nodes when ActiveAccess is running in a load-balanced configuration. It is also used for setting up and maintaining authentication history servers.

When ActiveAccess is installed, the first instance of administration server and access control server are automatically recognised. However, as you expand the system by adding more administration or access control servers, for load-balancing or fail-over, you are required to introduce newly added nodes using the facility provided in this section. ActiveAccess uses these lists in order to communicate changes in the administration and options to all administration and access control server nodes.

Warning

If you do not properly introduce these servers here, the additional servers will continue to function, however they will not receive notifications when changes occur to options throughout the admin interface, which will result in system instability.

Warning

Registration and enrolment server nodes do not need to be introduced as they each run independently.

Servers has the following menu options:

- **MIA Servers** - for managing MIA Servers
- **Access Control Servers** - for managing Access Control Servers
- **Authentication History Servers** - for managing Authentication History Servers
- **Centralised Authentication and Authorisation Server** - for managing Centralised Authentication and Authorisation Servers.

- **Out of Bank Authentication Server** - ➕ *new section* for managing OOB Authentication Servers
- **Risk Server** - ➕ *new section* for managing Risk Servers

MIA Servers

Servers > MIA Servers

A server entry is automatically created for the first instance of administration that you install. If you wish to install more than one server, you should first create an entry for the new server here and specify the IP address of the new instance and an arbitrary but descriptive name for the server.

This page displays:

- **MIA servers** list
- **Add Server** link
- **Delete Selected Servers** link used with the **Select** checkbox to remove selected servers.

The following fields and links are displayed for each administration server:

- **IP** link to the **Edit Server** page
- **Server Name**

Access Control Servers (ACS)

Servers > ACS Server Management

A server entry is automatically created for the first instance of ACS that you install. If you wish to install more than one server, you should first create an entry for the new server here and specify the IP address of the new instance and an arbitrary but descriptive name for the server.

This page displays:

- **Access control servers** list
- **Delete Selected ACS Servers** link used with the **Select** checkbox to remove selected servers.

The following fields and links are displayed for each administration server:

- **Server name** link to the **Edit Server** page
- **Domain name**
- **Binding IP**
- The **AHS Client** column shows whether the AHS client functionality is turned on for the ACS. If enabled the ACS will send PATransReq messages to the authentication history server.

Authentication History Servers (AHS)

Servers > AHS Server Management

This section is used to define one or more authentication history servers. The authentication history server is a repository of authentication activity maintained by the 3-D Secure provider, which can be used for dispute resolution by Issuers and Acquirers. ActiveAccess sends a copy of each 3-D Secure authentication attempt to the appropriate authentication history server. Not all 3-D Secure providers support and require the transactions to be sent to an authentication history server (e.g. Visa and Mastercard require AHS but other providers do not).

This page displays:

- **Authentication history servers** list
- **Add AHS Server**
- **Delete Selected AHS Servers** link used with the **Select** checkbox to remove selected servers.

The following fields and links are displayed for each administration server:

- *URL* of the authentication history server, as provided by the 3-D Secure provider, links to the **Edit AHS Server** page.
- **ACS ID** provided by the AHS administrator for the authentication history server.
- **Login ID** provided by the AHS administrator for the authentication history server.
- **Provider**, which is the entity (e.g. Mastercard or Visa) that manages the authentication history server.

Edit AHS Server

Servers > AHS Servers> Edit AHS Server

The **Edit AHS Server** page is used to change AHS details

Fields displayed on this page:

- **Provider**

  This is the entity (e.g. Mastercard or Visa) that manages the authentication history server.

- **URL**

  This the fully qualified URL of the authentication history server as provided by the 3-D Secure provider.

- Authentication history server **ACS ID, Login ID** and **Password**

  These are provided by the AHS administrator. You will need to contact the 3-D Secure provider to obtain this information. This information is required in order to establish a successful connection to the authentication history server.

Add AHS Server

Servers > AHS Servers > AHS Server Management > Add AHS Server

The **Add AHS Server** page is used to define new AHS servers

Fields displayed on this page:

- **Provider**
- **URL**
- **ACS ID**
- **Login ID**
- **Password**

> ⓘ **Info**
>
> For full information on individual fields please refer to the Edit AHS Server section of this document.

Centralised Authentication and Authorisation Servers (CAAS)

Servers > CAAS Server Management

This section is used to define one or more centralised authentication and authorisation servers. Centralised authentication and authorisation servers are remote authentication servers, which allow issuer banks to connect ActiveAccess with previously implemented remote servers that support authentication with the cardholder's existing database.

This page displays:

- **Centralised authentication and authorisation servers** list
- **Add CAAS Server**
- **Delete Selected CAAS Servers** link used with the **Select** checkbox to remove selected servers.

The following fields and links are displayed for each administration server:

- **CAAS URL**, which is the fully qualified URL of the remote authentication server (CAAS). Refer to CAAS document for further details of the URL. It links to the **Edit CAAS Server** page.
- **CAAS username**, which determines the username to access the CAAS server.

Edit CAAS Server

Servers > CAAS Servers> Edit CAAS Server

The **Edit CAAS Server** page is used to change CAAS details

Fields displayed on this page:

- **CAAS URL**

  This is the fully qualified URL of the remote authentication server (CAAS). Refer to CAAS document for further details of the URL.

- **CAAS username**

  This is the username used for accessing the CAAS server. Leave it blank if there is no username required by the CAAS authentication server.

- **CAAS password**

  This is the password associated with the CAAS username. Leave it blank if no password is required.

- **CAAS Connection timeout** in seconds (acceptable range is 60 to 9000)

This determines the maximum amount of time the ACS, as a CAAS client, can take to complete a connection with the CAAS authentication server.

- **Maximum SMS Request** (acceptable range is 0 to 99) (0 to disable)

  This determines the maximum number of SMS requests that the ACS will attempt to initiate with the remote CAAS server. Enter 0 to disable sending SMS initialisation requests to the remote server.

- **SMS Template**

  This template is used by the remote CAAS server to send the SMS OTP via a text message.

  Use **{0}** within the template to indicate the Token/OTP.

The following flags are available to use within the template:

- **$LastFourDigitsOfPAN** - to indicate the last four digits of the card
- **$MerchantName** - to indicate the merchant name for the current transaction
- **$PurchaseRealAmount** - to indicate the transaction amount.

> **Note**
>
> See SMS Template Parameters for a full list of available parameters.

- **Email Template**

  This template is used by the remote CAAS server to send the OTP via an email message.

  Use **{0}** within the template to indicate the Token/OTP.

The following flags are available to use within the template:

- **$LastFourDigitsOfPAN** - to indicate the last four digits of the card number
- **$MerchantName** - to indicate the merchant name for the current transaction
- **$PurchaseRealAmount** - to indicate the transaction amount
- **$ServicePhoneNumber** - to indicate the issuer's customer service phone number
- **$IssuerEmail** - to indicate the issuer's email address

Note

See Email Template Parameters for a full list of available parameters.

- **Email Subject Template**

  This template is used by the remote CAAS server for the Subject to be used for the OTP via email message.

  The flags described in Email Template above can be used for the Subject template.

- Select the **Use Proxy** checkbox if the ACS is to connect to the remote CAAS server via a proxy and complete the following:
  - **Proxy host**, which determines the proxy's IP address or domain name.
  - **Proxy port**, which determines the proxy's port.
  - **Proxy username**, which determines the proxy's username, if required.
  - **Proxy password** associated with the Proxy username, if required.
  - ***Apply*** button to save updated settings.
  - Click the **Check CAAS Status** link to verify that the CAAS server can be reached by the current remote authentication settings.

    The **Check CAAS Status** will be displayed, which shows the current status of the remote authentication server and is used to indicate the remote authentication server is running or not. * Click the **Retry** button to re-test the remote authentication server status.
  - Click the **Close** button to close this page.

Add CAAS Server

Servers > CAAS Servers > CAAS Server Management > Add CAAS Server

The **Add CAAS Server** page is used to define new CAAS servers

Fields displayed on this page:

- **CAAS URL**
- **CAAS username**
- **CAAS password**
- **CAAS Connection timeout**

- **Maximum SMS request**
- **SMS template**
- **Email template**
- **Email subject template**
- **Use proxy**
- **Proxy host**
- **Proxy port**
- **Proxy username**
- **Proxy password**

> ℹ **Info**
>
> For full information on individual fields, please refer to the Edit CAAS Server section.

Utilities

System Administrators only

This section is used to load, run and manage add-ins from within the ActiveAccess administration. Utilities can be assigned to, and run on behalf of, an Issuer or Issuer Group.

Utilities include:

- **PCIDSS Key Retiring Utility**

  This PCIDSS Key Retiring utility retires specified encryption keys and re-generates new encryption keys. Related table columns are then re-encrypted by new keys. The utility allows for the automatic retiring of old keys and re-generation of new ones, while keys manually created by HSM administrators can also be introduced as new keys.

  In the case of automatic key retiring, the utility can be run for selected general MIA / ACS settings encryption keys or issuer / groups based on key type and provider. Replacement with manually created keys can be done for general MIA / ACS settings encryption keys or issuer by entering the new key alias of keys created by the HSM administrator.

  For further information, refer to Key Retiring Utility.

***Utilities** has the following sub menu options:*

- **Utilities** - used for managing add-in utilities
- **Upload Utility** - used to upload add-in utilities on behalf of one or a number of Issuer or Issuer Groups.

The first **Utilities** page is **Utilities Search Result**.

Note

Utilities shown may vary.

Utilities

Utilities > Utilities Search Results

The Utilities section is used for viewing the details and availability of utilities in the system, and for managing and running selected utilities.

> **Note**
>
> Utilities shown may vary.

This page displays:

- Utilities List
- **Delete** button to allow selected utilities to be deleted

The following fields and links are displayed for each utility:

- **Select** checkbox
- **Name**
- **File Name**
- **Version**
- **Issuer**
- **Group**
- **Creation time**
- **Run** link - links to the **first** page of the selected Utility.

Upload Utility

Utilities > Upload Utility

Use this page to upload utilities to the system or on behalf of one or a number of Issuers or Issuer Groups.

Use the following fields to upload a utility:

- **Select the appropriate Issuer** or **Group** to upload the utility for.

- **File name** - click the Choose File button to locate and select the utility file to upload.
- ***Apply*** to upload the selected utility.

Key Retiring Utility

> *Previously AA85 - PCIDSS Key Retiring Utility.pdf*

This PCIDSS Key Retiring utility retires specified encryption keys and regenerates new encryption keys. Related table columns are then re-encrypted by new keys. The utility allows for the automatic retiring of old keys and regeneration of new ones, while keys manually created by HSM administrators can also be introduced as new keys.

In the case of automatic key retiring, the utility can be run for selected general MIA / ACS settings encryption keys or issuer / groups based on key type and provider. Replacement with manually created keys can be carried out for general MIA / ACS settings encryption keys or issuers by entering the new key alias of keys created by the HSM administrator.

Uploading the Utility

A System Administrator will be responsible for uploading the utility through the MIA (**Utilities > Upload Utility**).

To upload the utility

- There is no need to select an Issuer or Group to upload this utility.
- Browse to locate and select the **File name** (PCIDSSKeyRetiringUtility.war).
- Click the **Apply** button to upload the utility.

  The utility will be listed in the MIA utilities section (**Utilities > Utilities**) **PCIDSS Key Retiring Utility**.

Running the Utility

This utility makes changes in the HSM keystore and re-encrypts cardholder data and configuration settings in the database. Therefore, a full backup of the HSM keystore and ActiveAccess database should be taken before running this utility. If any archive database has been configured for automatic archiving, a backup of its database should be taken as well.

Note

Automatic archiving and purging in **System Management > Archive Management** must be disabled before running the utility. During the utility run, all ActiveAccess modules must stop receiving requests from the outside world.

Utility List

To run the utility

- Go to the MIA utilities section (**Utilities > Utilities**)
- Click the *Run* link adjacent to the **PCIDSS Key Retiring Utility**.

  The **PCIDSS Key Retiring Utility** screen is displayed prompting users to select which issuer, group or general encryption keys to run the utility for.

Retiring keys automatically

To customise the key retiring process

- Select **Retire old keys and generate new ones automatically**

To retire keys automatically

- Select the **General encryption keys** radio button
  - Select the **MIA settings encryption key** checkbox
  - Select the **ACS settings encryption key** checkbox
- Select the **Issuer** radio button
  - Select the **Issuer** from the drop down list
  - Select the key type from the **Type** drop down list
  - Select the provider from the **Provider** drop down list
  - If the **Type** selected is **RSA Signing**, select the key size from the **Key size** drop down list.
- Select the **Group** radio button
  - Select the issuer group from the **Group** drop down list
  - Select the key type from the **Type** drop down list
  - Select the provider from the **Provider** drop down list

  - If the key type selected for **Type** is **RSA Signing**, select the **Key size** from the drop down list.
- Click the **Prepare** / **Run** button

> **Note**
>
> The key retiring process for SecureCode HMAC, CAVV, and RSA Signing Keys is a one-stage process and once one of these key type options is selected, the Run button will be available. The process for retiring General/Data Encryption Keys occurs in two stages: Preparation and Finalization. For stage one of the process, the **Prepare** button will be available.

Retiring keys using manually created keys

Select the following field to customise the key retiring process

- Select **Retire old encryption keys and use the keys which have been created by HSM administrator**

Use the following fields for retiring keys using manually created keys

- Select the **General encryption keys** radio button
  - Select the **MIA settings encryption key** checkbox and enter the created key in the **New key alias** field
  - Select the **ACS settings encryption key** checkbox and enter the created key in the **New key alias** field
- Select the **Issuer** radio button
  - Select the **Issuer** from the drop down list
  - Enter the created key in the **New key alias** field
- Click the **Prepare** button

Results

When the process is complete, the Results will be available for immediate display. For more details of the utility process you can check **AA_HOME/mia_log.log**.

Encryption Key - Preparation Failure

If there is a failure within any of the steps of the preparation process, the utility stops and logs the details of the issue for the administrator's reference.

Encryption Key - Failed Resume/Rollback

If the encryption key retiring fails in the preparation stage, the process can be resumed from the latest status once the issue is resolved or all the changes can be undone using the Rollback option. When a process has a failed status, new processes cannot be started until the current process is successfully resumed or rolled back.

Encryption Key - Preparation Success

During the encryption key retiring process, a new encryption key is generated and a temporary column is added to the specified table for every column that keeps encrypted data. The data from the main column is decrypted using the old key, then encrypted using the new key and stored in a temp column.

Encryption Key - Finalization Re-encrypt/Finalize/Rollback

Once the preparation stage of the encryption key retiring process is completed successfully, the process can be finalized.

If any new data has been created after the completion of the preparation stage, the encryption process can be redone using the **Re-encrypt** option.

Alternatively, all the changes made during the preparation stage can be undone using the **Rollback** option.

The **Finalize** option completes the encryption key retiring process. In the Finalization process, once all the required columns are re-encrypted, the main column is dropped and the **temp** column is renamed to the name of the main column. In the final step, all the required constraints and indexes are created for the main column.

When the MIA settings encryption key is automatically or manually retired and replaced with a new one

If there are any other instances of MIA, Registration or Enrolment servers, rather than the current server, in the environment, replace the **DBOWNERPASSWORD** and **DBPASSWORD** values with their plain values in the **TOMCAT_HOME/bin/config/miaconfig.properties**, **regconfig.properties** or **eb_config.properties** file, then add the following properties to it and restart:

HSMENCALIAS=MIA_DB_DESEDE_NEW (where MIA_DB_DESEDE_NEW is the new MIA settings encryption key alias in HSM)

PLAIN_TEXT=

When the ACS settings encryption key is automatically or manually retired and replaced with a new one

If there is any other instance of ACS, rather than the current server, in the environment, replace the **DBOWNERPASSWORD** and **DBPASSWORD** values with their plain values in the **TOMCAT_HOME/bin/config/acsconfig.properties** file, then add the following properties to it and restart:

HSMENCALIAS=AA_Administration_NEW (where AA_Administration_NEW is the new ACS settings encryption key alias in HSM)

PLAIN_TEXT=

When the Issuer's data encryption key is automatically or manually retired and replaced with a new one

The current notification report files of the selected issuer are no longer valid and will be re-collected in the next run of the specified job in the Registration server.

If there is any other instance of Registration server, rather than the current instance, in the environment, add the following property into the **TOMCAT_HOME/bin/config/regconfig.properties** file:

NOTIFICATION_REPORT_REGEN_ISSUERIDS=1234567890 (where 1234567890 is the Issuer ID)

If property **NOTIFICATION_REPORT_REGEN_ISSUERIDS** already exists, modify its value by appending the Issuer ID to the end and restart.

Encryption Key - Archive

Following the successful finalization of the encryption key retiring process, if archiving is configured on the system, the encryption key of the archive database must also be retired and replaced using the **Re-encrypt Archive** option.

Issuers

System Administrators and **Issuer Administrators** only

This section is used to set issuer specific settings; maintain and upload card details; create and maintain custom pages and manage keys.
When a new issuer is created all issuer settings are set to default.
Issuers has the following menu options:

***Issuers** has the following sub menu options:*

- Settings
- Upload Registration Files
- Registration Requests
- Custom Pages
- Key Management

The first **Issuers** page is **Settings**.

Settings

This section is used to set up and maintain issuer system settings for displaying PARes, providing proof of authentication attempts to merchants, maximum unsuccessful authentication/ enrolment attempts permitted for cardholders and the automatic unlock lag time.

Note

Settings are different for **Local** and **Remote** Issuers.

Local Settings

Issuer > Settings

Use the following fields to manage Local Settings:

- Select an **Issuer** from the drop down list, to display its settings.
  This field is not displayed if the user is assigned to a single issuer.
- **Issuer ID** cannot be changed.
- **BINs** - displays a list of BINs currently assigned to the selected issuer. The BIN list can only be changed by a user with System Admin access level from **System Management > Issuer Management** section.
- **Maximum authentication attempts** allows the administrator to setup an upper limit for the number of successful authentications that can be performed by each user (acceptable range is 0 to 999) in a specified period of time (acceptable range is 0 to 24 hours). This is particularly useful when the issuer is being charged per transaction for each authentication and it makes sense to set an upper limit for the financial liability.

  This option is disabled by default which means the number of successful authentications that can be performed by the user is not limited.

  Once a set limit is reached, further authentication attempts fail at the UEReq/UERes level with status code 'U' and reason code '5' (maximum number of transactions exceeded).
- **Maximum unsuccessful attempts** that will be permitted for unsuccessful authentication or enrolment attempts by cardholders (acceptable range is 0 to 9).

  The default value is **3**, which means that 4 unsuccessful authentication or registration attempts with a card will result in the card being locked to avoid further access for security reasons. An issuer may change to any other value to comply with their internal policy.

  > ⚠ **Warning**
  >
  > Setting this field to 0 disables the automatic locking mechanism and is not recommended.
- **Maximum interaction** is used to set a maximum number of cardholder interactions as determined by the selected Challenge Flows and security requirements to allow an appropriate number of cardholder retries without going beyond the pre-set maximum (acceptable range is 0 to 10). When the limit is reached, the transaction fails but the card will not be locked.

- **Automatic unlock** time in minutes (acceptable range is 0 to 1440). A currently locked card can be automatically unlocked after the amount of time specified here has passed.

  This may help to reduce helpdesk calls if set properly.

  The default value is **0**, which implies that this field is disabled and as such all locked accounts have to be manually unlocked by helpdesk staff.

- Specify the cardholder **Password policy** using the following:
  - **Minimum password length** between 1 and 128 chars (typically 6)
  - **Maximum password length** between 1 and 128 chars (typically 16)
  - **Minimum password digit**, the minimum number of numerical characters the password must contain. The default value is 0, which disables this field.
  - **Minimum password capital letter**, the minimum number of capital letters the password must contain (typically 1). The default value is 0, which disables this field.

> **Note**
>
> The sum total of the numbers entered for **Minimum password digit** and **Minimum password capital letter** must be less than or equal to the **Minimum password length**.

- **Time zone**

  This allows administrators to set an individual time zone for the specified issuer.

  The default time zone is set when the application is installed and is displayed for reference, on the menu bar, from where it can be modified at any time, as and when appropriate. Modification of the Time zone on the menu bar *does not* change the Time zone for the Issuer in the Issuer Settings.

> **Note**
>
> If you modify the Time zone in the menu bar it will persist for the current session only. It will revert to the Time zone entered in the Issuer settings, the next time you login.
>
> All search parameters for transactions, audit logs and reports (daily, monthly and annual) will be based on the Time zone specified on the menu bar at the time of the search.

⚠ **Warning**

IMPORTANT: If the time zone in **Issuers > Settings** is changed, it will impact the data displayed for issuer reports (daily, monthly and annual). When attempting to change the time zone, a warning message is displayed with the following options:

- **Continue and delete report data** - reports will not be available for the selected issuer until the next overnight report run, which will use the new time zone.

NOTE :If auto archive is enabled, archived data will no longer be collected and previous report data will be lost.

- **Continue and keep report data** - existing report data will be inaccurate due to the time change. Accurate reports will not be available until the next overnight report run, which will use the new time zone.
- **Cancel** - time zone will not be changed.

- **Language selection during authentication**

  This allows administrators to enable or disable the language selection page displayed to cardholders during the challenge process of 3-D Secure 2 authentications.

- A link is provided to Provider Settings.

Provider Settings

There are a number of settings that can be specified per authentication scheme. You should set these parameters in accordance with the recommendation of the 3-D Secure authority of each scheme.

Issuer > Settings > Provider Settings

Use the following fields to view / edit Providers settings:

- Select an **Issuer** from the drop down list
- Select a **Provider ID** from the drop down list
- Select **Enabled** or **Disabled** from the **Activation during shopping** drop down list to enable or disable the cardholder registration during the shopping process.

  Enabling this option allows an issuer to dynamically enrol the cardholders while they are shopping at a 3-D Secure enabled merchant site. The activation during shopping process only applies to those cardholders who have been pre-registered by their issuer in the system.

- Select **Enabled** or **Disabled** from the **Proof of authentication attempt** drop down list to enable to disable providing authentication attempt guarantee to merchants.

This option applies to SafeKey, SecureCode, ProtectBuy, J/Secure and Verified by Visa in 3-D Secure version 1.0.2 and later. An issuer may choose to provide proof of authentication attempts for non-enrolled cardholders, when an authentication is requested by the merchant. Proof of attempt processing provides guarantee of funds transfer to the merchant. This may shift the liability to the issuer despite the fact the cardholder was not enrolled and could not be authenticated. Proof of attempt is an incentive for the merchants to implement 3-D Secure.

- Specify the value for **Maximum ADS proof of attempts** (acceptable range is 0 to 9). The option limits the number of times a user is allowed to opt-out of ADS processes and still receive proof of authentication attempt status code. Once the limit is reached, cancelling ADS will result in PARes status='N' to be returned to the merchant and it is likely that cardholder transaction will not be authorised by the merchant. Set this option to 0, if you wish to grant unlimited authentication attempts to cardholders.
- Specify the value for **PAReq freshness period** in minutes (acceptable range is 0 to 60). The default value 0, which effectively disables this option.

  An ACS may receive duplicate PAReq messages due to cardholder actions (for example, if the cardholder clicks the **Back** or **Refresh** buttons during the authentication process). In order to provide good customer service, and minimise cardholder confusion, the 3-D Secure protocol recommends that receipt of a duplicate PAReq within a reasonable time should not be treated as an error. This is called the **PAReq freshness period**. According to the 3-D Secure bulletin of July 12, 2004, the recommended period should be between 10 and 15 minutes.

> ⚠ **Warning**
>
> ActiveAccess sends a PARes with status code 'U' and iReqCode 56, if a duplicate PAReq is received outside the period specified by this parameter.

> ⚠ **Warning**
>
> The ADS and attempt process for Visa, American Express, Diners Club International and JCB is the same but different for Mastercard. Mastercard does not currently recognise attempt processing in the sense defined by Visa specification and does not provide authentication guarantee and liability shift if the cardholder is not enrolled. However, Mastercard still requires a PARes with status 'A' to be sent when the cardholder cancels ADS up to the limit defined by the issuer. For more information refer to Visa 3-D Secure standard and Mastercard SecureCode specification.

- *Mastercard SecureCode only*: Select **Mastercard SecureCode** or **Mastercard Identity Check** from the **Authentication type** drop down list.

- *American Express SafeKey only*: Specify the value for **Maximum forgot password attempts** (acceptable range is 0 to 9, default is 2 as specified in the SafeKey Issuer Implementation Guide). The option limits the number of times a user is allowed to enter an incorrect SafeKey before the card is locked. Once the limit is reached, it will result in PARes status='N' to be returned to the merchant and the cardholder transaction may not be authorised by the merchant.
- Select **A (Attempted)** or **N (Not approved)** from the **Unsupported device PARes status** drop down list.

  This option specifies the PARes to be used for unsupported devices.
- Specify any **Browser Unsupported devices** in the text box

  This is for specifying browsers / devices for which authentication is not supported in browser mode. It can also be used to quickly remove support if, for example, a security issue has been reported for a particular browser.

  Separate multiple browsers / devices using commas (,). This setting is not case sensitive.
- Specify any **App Unsupported devices** in the text box

  This is for specifying browsers / devices for which authentication is not supported in app mode. It can also be used to quickly remove support if, for example, a security issue has been reported for a particular browser.

  Separate multiple browsers / devices using commas (,). This setting is not case sensitive.
- Set the **Challenge Mandated Indicator**

  The ACS decides based on the ACS Challenge Mandated Indicator, the 3DS Requestor Challenge Indicator, and the ACS Rendering Type whether to perform the requested challenge.
- **Cardholder info for non-exempt authentication** - Text provided by the ACS to the cardholder during a frictionless transaction that was not authenticated by the ACS.

  It is optional for issuers to provide information to the cardholder.

  > **Example**
  >
  > “Additional authentication is needed for this transaction, please contact (Issuer Name) at xxx-xxx-xxxx.”
- **ACS Operator ID** - An ACS identifier assigned by the Directory Server. Each Directory Server can provide a unique ID to each ACS on an individual basis.

- **Broad Info** - Unstructured information sent between the 3DS Server, the Directory Server and the ACS.

> **Example**
>
> "TLS 1.x will be turned off starting summer 2019"

- **Display attempt time** - The duration of displaying an attempt page for JCB cards only in case of attempt returning status. A value of **0** indicates that no attempt page should be shown.

Remote Settings

Issuers > Settings

Use the following fields to view/ edit Remote Settings:

- **Issuer** This field is not displayed if the user is assigned to a single issuer.
- **Issuer ID** cannot be changed
- **Time zone**

  This allows administrators to set an individual time zone for the specified issuer.

  The default time zone is set when the application is installed and is displayed for reference, on the menu bar, from where it can be modified at any time, as and when appropriate. Modification of the Time zone on the menu bar *does not* change the Time zone for the Issuer in the Issuer Settings.

> **Note**
>
> If you modify the Time zone in the menu bar it will persist for the current session only. It will revert to the Time zone entered in the Issuer settings, the next time you login. All search parameters for transactions, audit logs and reports (daily, monthly and annual) will be based on the Time zone specified on the menu bar at the time of the search.

⚠ **Warning**

IMPORTANT: If the time zone in **Issuers > Settings** is changed, it will impact the data displayed for issuer reports (daily, monthly and annual). When attempting to change the time zone, a warning message is displayed with the following options:

- **Continue and delete report** data - reports will not be available for the selected issuer until the next overnight report run, which will use the new time zone.

NOTE- If auto archive is enabled, archived data will no longer be collected and previous report data will be lost.

- **Continue and keep report data** - existing report data will be inaccurate due to the time change. Accurate reports will not be available until the next overnight report run, which will use the new time zone.
- **Cancel** - time zone will not be changed.

Authentication Scheme Settings

There are a number of settings that can be specified per authentication scheme including activation during shopping, attempt processing and PAReq freshness period. You should set these parameters in accordance with the recommendation of the 3-D Secure authority of each scheme.

- Select **Enabled** or **Disabled** from the **Use ACS local settings** drop down list.

  Enabling this option allows issuer settings to be set locally in the ACS instead of remotely on the CAAS side.

  ✎ **Note**

  If **Disabled**, refer to Remote Messaging Specification for further information on setting these parameters.

*If **Enabled**:*

- Select **Enabled** or **Disabled** from the **Activation during shopping** drop down list to enable or disable the cardholder registration during the shopping process.

  Enabling this option allows an issuer to dynamically enrol the cardholders while they are shopping at a 3-D Secure enabled merchant site. The activation during shopping process only applies to those cardholders who have been pre-registered by their issuer in the system.

- Select **Enabled** or **Disabled** from the **Proof of authentication attempt** drop down list to enable to disable providing authentication attempt guarantee to merchants.

  This option applies to SafeKey, SecureCode, ProtectBuy, J/Secure and Verified by Visa in 3-D Secure version 1.0.2 and later. An issuer may choose to provide proof of authentication attempts for non-enrolled cardholders, when an authentication is requested by the merchant. Proof of attempt processing provides guarantee of funds transfer to the merchant. This may shift the liability to the issuer despite the fact the cardholder was not enrolled and could not be authenticated. Proof of attempt is an incentive for the merchants to implement 3-D Secure.

- Specify the value for **Maximum ADS proof of attempts** (acceptable range is 0 to 9). The option limits the number of times a user is allowed to opt-out of ADS processes and still receive proof of authentication attempt status code. Once the limit is reached, cancelling ADS will result in PARes status='N' to be returned to the merchant and it is likely that cardholder transaction will not be authorised by the merchant. Set this option to 0, if you wish to grant unlimited authentication attempts to cardholders.
- Specify the value for **PAReq freshness period** in minutes (acceptable range is 0 to 60). The default value 0, which effectively disables this option.

  An ACS may receive duplicate PAReq messages due to cardholder actions (for example, if the cardholder clicks the **Back** or **Refresh** buttons during the authentication process). In order to provide good customer service, and minimise cardholder confusion, the 3-D Secure protocol recommends that receipt of a duplicate PAReq within a reasonable time should not be treated as an error. This is called the **PAReq freshness period**. According to the 3-D Secure bulletin of July 12, 2004, the recommended period should be between 10 and 15 minutes.

  > ⚠ **Warning**
  >
  > ActiveAccess sends a PARes with status code 'U' and iReqCode 56, if a duplicate PAReq is received outside the period specified by this parameter.

  > ⚠ **Warning**
  >
  > The ADS and attempt process for Visa, American Express, Diners Club International and JCB is the same but different for Mastercard. Mastercard does not currently recognise attempt processing in the sense defined by Visa specification and does not provide authentication guarantee and liability shift if the cardholder is not enrolled. However, Mastercard still requires a PARes with status 'A' to be sent when the cardholder cancels ADS up to the limit defined by the issuer. For more information refer to Visa 3-D Secure standard and Mastercard SecureCode specification.

- **Mastercard SecureCode only**: Select **Mastercard SecureCode** or **Mastercard Identity Check** from the **Authentication type** drop down list.

- **American Express SafeKey only**: Specify the value for **Maximum forgot password attempts** (acceptable range is 0 to 9, default is 2 as specified in the SafeKey Issuer Implementation Guide). The option limits the number of times a user is allowed to enter an incorrect SafeKey before the card is locked. Once the limit is reached, it will result in PARes status='N' to be returned to the merchant and the cardholder transaction may not be authorised by the merchant.
- Select **A (Attempted)** or **N (Not approved)** from the **Unsupported device PARes status** drop down list.

  This option specifies the PARes to be used for unsupported devices.
- Specify any **Unsupported devices** in the text box

  This is for specifying browsers / devices for which authentication is not supported. It can also be used to quickly remove support if, for example, a security issue has been reported for a particular browser.

  Separate multiple browsers / devices using commas (,). This setting is not case sensitive.

Upload Registration Files

Issuers > Upload Registration Files

The **Upload Registration Files** section is used to upload user registration or card registration messages for bulk registration or pre-registration of cardholders and users. Files can be uploaded for an individual Issuer or for an Issuer Group.

> **Info**
>
> Please see the **Users** section for information on registering and managing individual card and user accounts.

The main page shows a report on recently performed file uploads and their status.

You can schedule uploading a user or card registration file using the *Upload File* link and, view details using the *Job* number link, and schedule or cancel scheduled uploads using the *Edit* or *Cancel* links.

> **Note**
>
> This page will not be available for remote issuers.

Use the following fields and links for managing card uploads:

- The first available **Issuer** is displayed by default. If you are assigned to an issuer group, select All or an **Issuer** from the drop down list and click the adjacent **Refresh** button.

  A list of the selected issuer's card files and their status is displayed.
- Select **All** or the type of registration message from the **Message Type** drop down list.

  A list of the selected issuer's card files and their status is displayed.
- The default report is for the last 10 days, but you can specify an upload **Date** range for the search result by entering dates in the **From** and **To** fields using dd/mm/yyyy format and clicking the **Refresh** button.
- Click the *Upload File* link (which is only displayed when an Issuer is selected) to schedule a file upload job for the selected issuer.

  The **Upload File** page is displayed.

The following details are displayed for each uploaded file for the selected issuer:

- **Job Number** - this number is defined by the system and links to the **Job Details** page, which provides full details for the job and details of any error messages or warning conditions
- **Issuer**- name of the issuer that owns the card upload job
- **Group** - name of the issuer group that owns the card upload job
- **Message Type**- the type of registration message either card registration or user registration
- **File Name** - the name of the file uploaded
- **Started** - the date and time the file upload started
- **Finished** - the date and time the file upload finished
- **Attempts** - the number of times the file upload was attempted
- **Status** - the upload status shows the current status for data upload, which can be one of the following:
  - Completed
  - Completed with warnings
  - Processing
  - Failed
  - Scheduled

  - Cancelled

- **Edit** link - displayed for **Scheduled** uploads.

  This links to the **Edit Upload Details** page for updating the scheduled date and time.

- **Cancel** link - displayed for **Scheduled** uploads.

  The administrator may cancel a scheduled upload, by clicking the *Cancel* link, but cannot cancel one which is in progress.

Upload File

Issuers > Upload Registration Files > Upload File

This page is used to enter the details of the card file you wish to upload and to schedule the upload date and time.

Use the following fields to upload a file:

- Choose the appropriate radio button and select an **Issuer** or an **Issuer group** from the drop down list.
- Select the type of registration message either **Card Registration** Or **User Registration** from the **Message Type** drop down list
- Click the **Choose File** / **Browse...** button adjacent to **File name**, to locate and select a registration file to upload.

  The **No file chosen** message will then be replaced by the File name of the file to be uploaded.

- Enter **Schedule Date** and **Time** when you want the uploaded data to be processed.

  Uploaded files scheduled to run in the past are set to run immediately.

  You may also leave these fields blank if you wish to process the uploaded data as soon as possible.

Note

The data upload may take a long time to complete depending on the file size and line speed.

Job Details

Issuers > Upload Registration Files > Job Details

This page provides job details and a link to the registration request details via the Message ID link. It also provides information on any error conditions that prevented the upload from being processed successfully.

The fields displayed are:

- **Issuer** name
- **Job number**
- **Message ID** link to **Request details**
- **Message type** - Card Registration or User Registration
- **Uploaded** date and time
- **File name**
- When the upload was **Started** and **Finished**
- Number of **Attempts** before the upload was finished
- **Status** of the job
- **Error message**
- **Error Details**
- **Warnings**

Edit Uploaded File

Issuers > Upload Registration Files > Edit Uploaded File

This page is used to update the scheduled processing time by specifying a new **Date** and **Time**.

Use the following fields to edit the file's scheduled upload:

- **Issuer** - cannot be changed
- **Message type** - cannot be changed
- **File name** - cannot be changed.

To upload a different file you must first cancel this upload using the **Cancel** link on the **Upload Registration File** page and then select the **Upload File** link.

- **Date** using dd/mm/yyyy format
- **Time** using hh:mm format
- **Apply** button to save.

Registration Requests

Issuers > Registration Requests Search

The **Registration Requests** section is used to view requests for user registration or card registration messages

You can view registration request details using the **REG ID** link.

> **Note**
>
> This page will not be available for remote issuers.

Use the following fields to find a registration request:

- Select from the **Issuer** drop down list to limit the results to the specified issuer **OR**
- Select from the **Group** drop down list to limit the results to the specified issuer group.
- The **Request ID** is the identifier entered in the registration message by the issuer. Enter all of the **Request ID** to search.
- The default **Creation date** range is for the last 10 days, but you can specify a date and time range (inclusive) in the **From** and **To** fields. The date and time format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.
- The default **Completion date** range is for the last 10 days, but you can specify a date and time range (inclusive) in the **From** and **To** fields. The date and time format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.
- Select the **Status** of the registration requests from the drop down list. The options are:
    - All (default)
    - Completed

- Completed with warnings
- Failed
- Processing

- Click **Search** to display registration request details

A list of the selected issuer or issuer group's registered requests and their progress is displayed.

Issuers > Registration Requests displays:

The following details are displayed for each registration request

- **REG ID** - this number is defined by the system and links to the **Request Details** page, which provides full details for the request job and details of any error messages or warning conditions
- **Issuer** - name of the issuer who owns the registration request
- **Group** - name of the issuer group who owns the registration request
- **Creation date** - the date the request was created
- **Completion date** - the date the request was completed
- **Request ID** - the Request ID associated with the request message
- **Progress** - the status of the request; Completed, Completed with warnings, Failed or Processing.

Custom Pages

Issuers > Custom Pages

This section is used to upload, store and manage issuer branded pages. Branded pages are displayed during user enrolment and authentication processes.

Each issuer is assigned a separate space and a separate URL for their enrolment and authentication pages. This ensures that users will always be presented with their own issuer branded pages during the enrolment and authentication process.

> **Note**
>
> For ease of upload, you can zip the files first and upload them all at once.

Note

A set of sample custom pages, with *Any Bank* branding, is available in the ActiveAccess installation package: ActiveAccess/data/custompage/issuer

The naming convention for enrolment and authentication pages is as follows:

Page	Filename
J/Secure authentication	auth_jcb_index.xsl
SecureCode authentication	auth_spa_index.xsl
VbV authentication	auth_vbv_index.xsl
SafeKey authentication	auth_sk_index.xsl
ProtectBuy authentication	auth_dc_index.xsl
Cardholder enrolment home page	reg_index.xsl
Two-factor device authentication	dev_index.xsl

Other resources can be uploaded to the issuer space such as help files and graphics, etc.

To avoid any run time problems or security risk, only trained personnel can upload branded pages. As such, the option to upload custom pages is available at the **system administration** level only.

Issuer administrators have read-only access to this function, which can be used to download custom pages and branded material.

Note

The issuer system limits issuer space to a flat file structure (i.e. all files are created at the same directory level.

You can upload new pages using the **Upload File** link and **Delete** or **Download** pages.

Use the following fields and links for managing the custom pages:

- Select an **Issuer** from the drop down list of available issuers and click the **Refresh** button.

  A list of the issuer's custom pages is displayed.

  Or

- Select a **Group** from the drop down list of available groups and click the **Refresh** button.

  A list of the group's custom pages is displayed.

- **Upload File** link to upload a new file for the selected issuer or issuer group.

  The **Upload File** page is displayed.

- **Download Selected** link, used in conjunction with the **Select** checkbox to download one or multiple custom pages, for the selected issuer or issuer group.
- **Delete Selected** link, used in conjunction with the **Select** checkbox to delete one or multiple custom pages, for the selected issuer or issuer group

The following custom page details are displayed for the selected issuer:

- **File Name**
- **Size** - size of file in bytes
- **Date** - date and time of upload
- **Delete** link to delete the page
- **Download** link to download the page

Upload File

Issuers > Custom Pages > Upload File

This page is used to enter the name and location of the custom page you wish to upload

Use the following fields to upload a file:

- Select the **Issuer** for which you are uploading the custom pages from the drop down list
- Alternatively a **Group** can be selected from the drop down list. Selecting a group allows the administrator to roll out an update to all the issuers that are a direct member of the group or a member of a group owned by the selected group.

> **Note**
>
> **Important:** Care should be taken when rolling out an update to a group as it will overwrite the corresponding files on all the member issuers. Issuers may have configuration, graphics or text files specific to their own brand. You should not upload a generic package that overwrites these issuer branded pages through this facility without carefully checking first.

- Click the **Choose File** / **Browse…** button, adjacent to **File name**, to locate and select a custom page file to upload.

  The **No file chosen** message will then be replaced with the name of the file to be uploaded

- Click the **Apply** button to upload the file.

  File upload confirmation is displayed and if uploaded pages support rules, a link is provided to allow issuer to use rules.

Key Management

The system creates a number of cryptographic keys for each issuer in order to protect sensitive and confidential information. These keys are securely stored on a hardware security module (HSM).

This section lists keys used by the issuer and the history of any changes. The list of keys is retrieved from the local HSM accessible by the MIA instance, which is currently being accessed by the user. It is the responsibility of the system administrator to keep all HSM instances synchronised at all times.

This section also allows the administrator to retire the current Signing RSA or CAVV validation keys and replace them with the ones that have been created by the HSM administrator using vendor or third party utilities. Card and general encryption keys cannot be retired and replaced using this interface as a process to decrypt previously encrypted fields with an old key and re-encrypt them using a new key is required. GPayments has developed a PCIDSS Key Retiring Utility for this purpose.

Use the following fields and links for viewing keys:

- The first available **Issuer** is displayed by default. You can select a different **Issuer** from the drop down list of available issuers and click the adjacent **Refresh** button.

  A list of the selected issuer's current keys is displayed.

- If the required **Issuer** or an **Issuer Group** is not displayed, select it from the appropriate drop down list.
- You can select the **General keys** radio button to view the list of the general encryption keys that are used to encrypt general critical settings and configuration parameters.

This page displays for each key;

- *Alias* link to the **Key Details** page
- *Delete*. link to allow unused keys to be deleted

The following key details are displayed for the selected issuer or issuer group:

- **Provider**
- **Algorithm**
- **Type**
- **Alias**
- **Creation time** - date and time of upload
- **Status**

New Key

Issuers > Key Management > New Key

The **New Key** section is used to retire the current Signing RSA or CAVV validation keys and replace them with the ones that have already been created by the HSM administrator, using vendor or third party utilities.

Alternatively, the **PCIDSS Key Retiring Utility** provided in the ActiveAccess installation package allows for the automatic retiring of old keys and re-generation of new ones. Refer to the document *AA85 – PCIDSS Key Retiring Utility* for further details.

Use the following fields and links for generation of new keys:

- **Issuer** or **Group**
- **Type**
- **Provider**

> **Note**
>
> SecureCode HMAC generation key is only available for the Mastercard provider.

- **Algorithm** is displayed and cannot be changed.
- **Old alias** is displayed and cannot be changed.
- **Old key size** is displayed and cannot be changed.
- **New alias status** is displayed and cannot be changed.
- **New alias**.
- If the key **Type** is **Signing RSA Key**, select a **Key size** from the drop down list. Defaults to **1024**.

Key Details

Issuers > Key Management > Key Details

The **Key Details** section is used to list the history of the changes for the specified key.

The following key details are displayed for the selected alias:

- **Alias**
- **Algorithm**
- **Creation time** - date and time of upload
- **Expiration time** - date and time the key will expire
- **Status**
- **Active** - the key is being used by the system
- **Inactive** - the key needs to be activated through a pre-defined process
- **Expired** - the key has been retired and will no longer be used by the system.
    - **Delete** link to allow unused keys to be deleted.

Use the following for generating new keys:

- New Key link

Rules

System Administrators and **Issuer Addministrators**
Access can also be granted to **Business Admin** and **Helpdesk** users at System Admin level.
Whether these users have *read only* or *full* access is determined by their Admins settings.

This section is used to set up and manage business rules and the sequence in which they are applied for Issuers that have rules functionality enabled.

The rules that can be applied are determined by whether the authentication server is remote or local. Authentication exemption rules and settings can be applied for local and remote authentication servers and registration enforcement rules can be applied for local authentication servers.

You can set up and maintain Issuer authentication exemption business rule settings for the local or remote ACS (CAAS). These business rules are configurable settings, which provide Issuers with control over the customer process during 3-D Secure transactions as described in the table below. Rules can be configured using 3-D Secure transaction parameters such as Transaction Amount, Merchant ID, Merchant Name, Acquirer BIN or Merchant Country. The sequence in which the rules are applied can be defined by setting Priority values for each rule.

Rule Management has the following tabs:

- **Registration** - allows two pre-defined rules to be used for checking authentication requests processed or transparently authenticated by a local authentication server. The Rules are:
  - **Amount Threshold**
  - **Merchant Blacklist**

  These rules can be enabled, disabled and have their order of priority changed.
- **Authentication**
  - **Soft Launch List**
  - **Merchant Whitelist**
  - **Merchant Watchlist**

    - **Location Watchlist**
    - **Domestic & International Transaction Amount Threshold**

  These rules can be enabled, disabled and have their order of priority changed.

- **Settings** - used to set up transaction number and / or amount thresholds to be used for determining if authentication is to be initiated or bypassed. Also used to define the authentication response (PARes) to be sent for any transactions where authentication is bypassed.

Rules can be set to apply by default and not just for exceptions.

Registration

Rules > Rule Management > Registration

This section is used to set up and maintain settings for business rules that force customer registration. These business rules are configurable settings which provide issuers control over the customer process during 3-D Secure transactions.

These rules can be configured using 3-D Secure transaction parameters such as the Transaction Amount, Merchant ID, Merchant Name, Acquirer BIN or Merchant Country.

The sequence in which the rules are applied can be changed by setting a Priority for each rule.

Rule	Description	Parameters	Behaviour	
Amount Threshold	A threshold that determines if pre-registered cardholders are to be forced to opt-in to Activation During Shopping.	**Transaction amount** (AUD or converted to AUD)	*Greater than or equal to threshold:* No Opt-Out option available on the ADS page, only cancel	*Less than threshold:* Opt-Out option will be available on the ADS page *Opt-Out* - sets transaction status to 'A'

Rule	Description	Parameters	Behaviour	
Merchant Blacklist	Merchant criteria that initiate the authentication.	**Merchant** Merchant ID Merchant name Acquirer BIN Merchant country	*On list:* No Opt-Out option available on the ADS page, only cancel *Cancel* - sets Transaction Status to 'N'.	*Not on list:* Opt-Out option will be available on the ADS page *Opt-Out* - sets transaction status to 'A'

Use the following fields to view / edit the Rules:

- If the required **Issuer** or an **Issuer Group** is not displayed, select it from the appropriate drop down list.
- Click the **Refresh** button.

Note

These fields are not displayed if the user is assigned to a single issuer.

The following fields and links are displayed for each rule:

- **Select** checkbox to be used in conjunction with the **Enable** and **Disable** buttons.
- *Rule Name* link to the **Rule Details** page
- **Priority** sequence in which the rules are applied, can be changed by clicking **Move Up** or **Move Down**
- **Status** - Enabled, Disabled or Not Configured

Use the following steps to enable or disable a rule:

- Choose one or more rules by clicking the **Select** checkbox adjacent to the **Rule Name**
- Click the **Enable** or **Disable** button as appropriate.

  A confirmation message will be displayed.

Amount Threshold

Rules > Rule Management > Registration > Amount Threshold

The Amount Threshold rule allows an issuer to encourage pre-registered cardholders to register for 3-D Secure based on the value of the transaction.

When this rule is enabled, the cardholder is pre-registered and when they purchase from a 3-D Secure enabled merchant, if the value of the transaction is equal to or exceeds the threshold amount, the cardholder will be presented with the standard ADS page but will not be given the opportunity to Opt-Out. Instead, the cardholder will only be able to Cancel the transaction and the authentication result that will be returned to the merchant will be, **N**.

If the transaction is in a currency other than the one selected for the rule, a conversion will be made to convert the value of the transaction into the currency of the rule, so that the converted value can be compared with the threshold to determine the appropriate action.

> **Note**
>
> If currency conversion is not available, the default will be for registration to be enforced.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more sets of rules.
- **BIN** links to the **Edit Amount Threshold** page.
- **Delete** button used in conjunction with selected rules.
- Links for **Manage Exchange Rates** and **Add**.

To manually create currency exchange values:

- Click the **Manage Exchange Rates** link.

  The **Manage Exchange Rate** page is displayed.

To add Amount Threshold rules:

Rules > Force Registration > Amount Threshold > Add

- Click the **Add** link.

  The **Add Amount Threshold** page is displayed.

> **Note**
>
> The *Add* link is disabled when a rule has been set for All BINs of the selected issuer.

To delete a rule:

- Select the checkbox adjacent to the BIN and click the **Delete** button.

  Confirmation of the deletion is displayed.

To set transaction amount thresholds:

- **Issuer** name is displayed and cannot be changed.
- Select the **BIN** to be used for the threshold from the drop down list.
- Enter an **Amount** for the threshold.
- Select the default currency to be used for the domestic threshold from the **Currency** drop down list.
- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

Merchant Blacklist

The Merchant Blacklist rule allows an issuer to encourage pre-registered cardholders to register for 3-D Secure based on merchant related transaction parameters. If the attributes of the business rule match the merchant related transaction parameters, the cardholder will not be allowed to Opt-Out of the Activation During Shopping process and will only be able to cancel the transaction. Issuers can use any combination of Merchant ID, Merchant Name, Acquirer BIN and Merchant Country to create a rule to encourage cardholders to register.

If the cardholder cancels the transaction, the authentication result returned to the merchant will be an **N**.

When checking the Merchant details from a transaction against the Merchant Blacklist, the Merchant is considered to be a match if any of the Merchant details (Merchant ID, Merchant name, Acquirer BIN or Merchant country) from the PAReq match the corresponding details on the Blacklist.

You can set a maximum number of rules for the Merchant Blacklist, import a file of Merchant details or add individual Merchant details to the list, delete Merchant details and edit Merchant details.

Merchant Blacklist Details

Rules > Rule Management > Registration > Merchant Blacklist > Merchant Blacklist Search Results

You can add individual Merchant details or import a file of Merchant details to the list or select any Merchant details to delete or edit.

The following fields and links are displayed:

- **Maximum no of rules in blacklist** (default is 50)
- **Select** checkbox for selecting one or more sets of Merchant details
- **Delete** button used in conjunction with selected Merchant details
- **Merchant ID**, **Merchant Name**, **Acquirer BIN** and **Merchant Country** links to the **Edit Merchant Blacklist** page
- Links for **Add** and **Import**

To change the number of rules permitted in the blacklist:

- Enter the **Maximum no of rules in blacklist**.
- Click the **Apply** button.

To add individual Merchant details:

- Click the **Add** link.

  The **Add Merchant Blacklist** page is displayed.

To import a file of Merchant details:

- Click the **Import** link.

  The **Import Merchant Blacklist** page is displayed.

> **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml. The following is an example of a sample .xml file:

```
<MerchantBlacklist>
    <Merchant>
```

```
        <Id>1</Id>
        <Name>hi</Name>
        <AcquirerBIN>412345</AcquirerBIN>
        <CountryCode>024</CountryCode>
    </Merchant>
    <Merchant>
        <Id>12134567890</Id>
        <Name>hi</Name>
        <AcquirerBIN>412345</AcquirerBIN>
    </Merchant>
</MerchantBlacklist>
```

To delete Merchant details:

- Select the checkbox adjacent to the Merchant ID and click the **Delete** button.

  Confirmation of the deletion is displayed.

Edit Merchant Blacklist

Rules > Rule Management > Registration > Merchant Blacklist > Edit Merchant Blacklist

To edit the Merchant Blacklist:

- **Issuer** name is displayed and cannot be changed.
- Edit any of the Merchant fields:
  - **Merchant ID**
  - **Merchant Name**
  - **Acquirer BIN**
  - **Merchant Country**.
- Click the **Apply** button. A confirmation message will be displayed.

When checking whether a transaction matches the Merchant Blacklist, the system will compare the Merchant ID, Merchant Name, Acquirer BIN and Merchant Country from the PAReq, with the values entered.

- Click the **Back** button to return to the Merchant Blacklist.

Import Merchant Blacklist

Rules > Rule Management > Registration > Merchant Blacklist > Import Merchant Blacklist

This page is used to import a file of merchant Blacklist rules to add to the Merchant Blacklist. The format of the file should be CSV, with each record incorporating values for any of the required Merchant ID, Merchant Name, Acquirer BIN and Merchant Country fields necessary to define the rule.

> **Note**
>
> Merchant country is defined by a country code and name and uses the format:
> < ISO 3166-1 numeric code>/< ISO 3166-1 country name>
>
> For example:
>
> 008/Albania
>
> 024/Angola
>
> 036/Australia

To import a file of merchant watchlist rules:

- **Issuer** name is displayed and cannot be changed.
- Click the **Choose File** / **Browse** button adjacent to **File name**, to locate and select a file to import.

  The **No file chosen** message will be replaced with the name of the file to be imported.

  > **Note**
  >
  > A maximum of 1000 records can be imported at one time.

- Click the **Apply** button.

  A confirmation message will be displayed.

Authentication

Rules > Rule Management > Authentication

Rule	Description	Parameters	*If on list*	*If not on list*
Soft Launch List	Primary Account Numbers that will not be allowed to bypass the authentication procedure.	**Cardholder:** Primary Account Number	Other business rules applied in the specified sequence.	Cardholder transparently authenticated. Transaction Status set to 'Y' or 'A', as configured under the Settings tab.
Merchant Whitelist	Merchant criteria that allow the authentication procedure to be bypassed.	**Merchant:** Merchant ID Merchant name Acquirer BIN Merchant country	Cardholder transparently authenticated. Transaction Status set to 'Y' or 'A', as configured under the Settings tab.	Other business rules applied in the specified sequence.
Merchant Watchlist	Merchant criteria that initiate the authentication procedure.	**Merchant:** Merchant ID Merchant name Acquirer BIN Merchant country	Initiates authentication procedure.	Other business rules applied in the specified sequence.
Location Watchlist	Merchant countries that initiate the authentication procedure	**Merchant country:** Country / Currency code	Initiates authentication procedure.	Other business rules applied in the specified sequence.
Domestic & International Transaction Amount Threshold	A threshold that determines if the authentication procedure is to be initiated or bypassed. Domestic threshold used for the set default transaction purchase currency, otherwise, International threshold used.	**Transaction amount**	*Greater than or equal to threshold:* Initiates authentication procedure.	*Less than threshold or currency not in file:* Cardholder transparently authenticated. Transaction Status set to ‘Y’ or 'A', as configured under the Settings tab.

Rule	Description	Parameters	*If on list*	*If not on list*
Stand-In Transaction	A threshold that determines if the authentication procedure is to be bypassed when the remote authentication server (CAAS) cannot be contacted or is not responding at the Verify Registration (first message to CAAS) stage.	**Transaction amount** (AUD or converted to AUD)	*Greater than or equal to Stand-in threshold:* Unable to authenticate Transaction Status set to 'U'	*Less than Stand-In threshold:* Cardholder transparently authenticated. Transaction Status set to 'Y' or 'A', as configured under the Settings tab.

- Click the **Rules** tab, if it is not already selected.

Use the following fields to view / edit the Rules:

- If the required **Issuer** or an **Issuer Group** is not displayed, select it from the appropriate drop down list.
- Click the **Refresh** button.

> **Note**
>
> These fields are not displayed if the user is assigned to a single issuer.

The following fields and links are displayed for each rule:

- **Select** checkbox to be used in conjunction with the **Enable** and **Disable** buttons.
- **Rule Name** link to the **Rule Details** page
- Once two or more rules are enabled, the **Priority** sequence in which the rules are applied can be changed by clicking **Move Up** or **Move Down**. Once Priority is customised, click **Reset to Default**, to reset the sequence in which the rules are applied back to the system default.
- **Status** - Enabled, Disabled or Not Configured

To enable or disable a rule:

- Choose one or more rules by clicking the **Select** checkbox adjacent to the **Rule Name**

- Click the ***Enable*** or ***Disable*** button as appropriate.
  A confirmation message will be displayed.

Soft Launch List Rule

If the cardholder's Primary Account Number is on the Soft Launch List, the authentication procedure will not be bypassed, and the other business rules will be applied in the specified sequence.

> ⚠ **Warning**
>
> If the cardholder is not on the list, the cardholder will be considered to be transparently authenticated and transaction status will be set to **Y** or **A**, as configured under the **Settings** tab.

You can search for PANs in the Soft Launch List, import a file of PANs or add an individual PAN to the list and edit a PAN.

The first page in this section is **Search Soft Launch List**.

Search Soft Launch List

Rules > Rule Management > Soft Launch List > Search Soft Launch List

This page displays:

- **Issuer** name = cannot be changed.
- **Search** button to search for cardholder PANs already in the Soft Launch List.
- **Import** button to import a list of PANs to add to the list
- **Add** button to add an individual PAN to the list

> **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml.

To search for a cardholder PAN:

- Enter a **Primary Account Number** and click the **Search** button. Leave the field blank to search for all PANs.

The **Soft Launch List** page is displayed.

Soft Launch List

Rules > Rule Management > Authentication > Soft Launch List > Soft Launch List Search Results

PANs are listed according to the search criteria you entered on the **Search Soft Launch List** page. You can add an individual PAN or import a list of PANs to the list or select any PAN to delete or edit it.

The following fields and links are displayed:

- **Select** checkbox - for selecting the Primary Account Number in conjunction with the **Delete** button
- **Primary Account Number** link to the **Edit Soft Launch List** page
- Links for **Add** and **Import**

To edit a PAN:

- Click the **Primary Account Number** link.

  The **Edit Soft Launch List** page is displayed.

To add an individual PAN:

- Click the **Add** link.

  The **Add Soft Launch List** page is displayed.

To import a file of PANs:

- Click the **Import** link.

  The **Import Soft Launch List** page is displayed.

To delete a PAN:

- Select the checkbox adjacent to the Primary Account Number and click the **Delete** button.

Edit Soft Launch List

Rules > Rule Management > Authentication > Soft Launch List > Search Soft Launch List > Edit Soft Launch List

To edit the Soft Launch List:

- **Issuer** name is displayed and cannot be changed.
- Edit the **Primary Account Number**.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Soft Launch List Search Results.

Add to Soft Launch List

Rules > Rule Management > Authentication > Soft Launch List > Add Soft Launch List

This page is used to add individual PANs to the Soft Launch List.

To add to the Soft Launch List:

- **Issuer** name is displayed and cannot be changed.
- Enter a **Primary Account Number**.
- Click the **Apply** button.

  A confirmation message will be displayed.

Import Soft Launch List

Rules > Rule Management > Authentication > Soft Launch List > Import Soft Launch List

This page is used to import a file of cardholder PANs to add to the Soft Launch List. The format of the file should be CSV, with each record incorporating a PAN value.

To import a file of PANs:

- **Issuer** name is displayed and cannot be changed.
- Click the **Choose File** / **Browse...** button adjacent to **File name**, to locate and select a file to import.

  The **No file chosen** message will be replaced with the name of the file to be imported.

  > **Note**
  >
  > A maximum of 1000 records can be imported at one time.

- Click the **Apply** button.

A confirmation message will be displayed.

Merchant Whitelist Rule

If any of the Merchant details are on the Merchant Whitelist, the authentication procedure will be bypassed and the other business rules will be applied in the specified sequence.

> **Note**
>
> If any of the merchant's details are on the list, the cardholder will be considered to be transparently authenticated and transaction status will set to **Y** or **A**, as configured under the **Settings** tab.

When checking the Merchant details from a transaction against the Merchant Whitelist, the Merchant is considered to be a match if any of the Merchant details (Merchant ID, Merchant name, Acquirer BIN or Merchant country) from the PAReq match the corresponding details on the Whitelist.

You can search for Merchant details in the Merchant Whitelist, import a file of merchant details or add Merchant details to the list and edit Merchant details.

The first page in this section is **Search Merchant Whitelist**.

Search Merchant Whitelist

Rules > Rule Management > Merchant Whitelist > Search Merchant Whitelist

This page displays:

- **Search** button to search for Merchant details already in the Merchant Whitelist.
- **Import** button to import a file of Merchant details to add to the list

> **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml. The following is an example of a sample .xml file:

```
<MerchantWhitelist>
      < Merchant>
          <Id>1</Id>
          <Name>hi</Name>
          <AcquirerBIN>412345</AcquirerBIN>
```

```
            <CountryCode>024</CountryCode>
        </Merchant>
        <Merchant>
            <Id>12134567890</Id>
            <Name>hi</Name>
            <AcquirerBIN>412345</AcquirerBIN>
        </Merchant>
    </MerchantWhitelist>
```

- **Add** button to add individual Merchant details to the list

To search for a Merchant:

- **Issuer** name is displayed and cannot be changed.
- Enter Merchant details as follows, or leave them blank to display all Merchants on the Whitelist:
    - Enter a **Merchant ID**
    - Enter a **Merchant name**
    - Enter an **Acquirer BIN**
    - Select a **Merchant country** from the drop down list. Default is All.
- Click the **Search** button.

The **Merchant Whitelist** page is displayed.

Merchant Whitelist

Rules > Rule Management > Authentication > Merchant Whitelist > Merchant Whitelist Search Results

Merchant details are listed according to the search criteria you entered on the **Search Merchant Whitelist** page. You can add an individual Merchant or import a file of Merchants to the list or select any Merchant to delete or edit it.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more sets of Merchant details
- **Delete** button used in conjunction with selected Merchant details
- *Merchant Id*, *Merchant Name*, *Acquirer BIN* and *Merchant Country* links to the **Edit Merchant Whitelist** page
- Links for *Add* and *Import*

To add individual Merchant details:

- Click the *Add* link.

  The **Add Merchant Whitelist** page is displayed.

To import a file of Merchant details:

- Click the *Import* link.

  The **Import Merchant Whitelist** page is displayed.

To delete Merchant details:

- Select the checkbox adjacent to the Merchant ID and click the **Delete** button.

  Confirmation of the deletion is displayed.

Edit Merchant Whitelist

Rules > Rule Management > Authentication > Merchant Whitelist > Edit Merchant Whitelist

To edit the Merchant Whitelist:

- **Issuer** name is displayed and cannot be changed.
- Edit any of the Merchant fields:
  - **Merchant ID**
  - **Merchant Name**
  - **Acquirer BIN**
  - **Merchant Country**.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Merchant Whitelist Search Results.

Add to Merchant Whitelist

Rules > Rule Management > Authentication > Merchant Whitelist > Add to Merchant Whitelist

This page is used to add Merchant details to the Merchant Whitelist.

When checking whether a transaction matches the Merchant Whitelist, the system will compare the Merchant Id, Merchant Name, Acquirer BIN and Merchant Country from the PAReq, with the values entered.

To add to the Merchant Whitelist:

- **Issuer** name is displayed and cannot be changed.
- Enter a value into any of the Merchant fields:
  - **Merchant Id**
  - **Merchant Name**
  - **Acquirer BIN**
  - **Merchant Country** select from the drop down list.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Merchant Whitelist Search Results.

Import Merchant Whitelist

Rules > Rule Management > Authentication > Merchant Whitelist > Import Merchant Whitelist

This page is used to import a file of merchant whitelist rules to add to the Merchant Whitelist. The format of the file should be CSV, with each record incorporating values for any of the required Merchant Id, Merchant Name, Acquirer BIN and Merchant Country fields necessary to define the rule.

Note

Merchant country is defined by a country code and name and uses the format:
< ISO 3166-1 numeric code > / < ISO 3166-1 country name>

For example:

008/Albania

024/Angola

036/Australia

To import a file of merchant whitelist rules:

- **Issuer** name is displayed and cannot be changed.
- Click the **Choose File** / **Browse...** button adjacent to **File name**, to locate and select a file to import.

  The **No file chosen** message will be replaced with the name of the file to be imported.

  > **Note**
  >
  > A maximum of 1000 records can be imported at one time.

- Click the **Apply** button.

A confirmation message will be displayed.

Merchant Watchlist

If any of the Merchant's details are on the Merchant Watchlist, the authentication procedure will be initiated. If the Merchant's details are not on the list, the other business rules will be applied in the specified sequence.

> **Note**
>
> If any of the merchant details are on the list, the authentication procedure will be initiated.

When checking the Merchant details from a transaction against the Merchant Watchlist, the Merchant is considered to be a match if any of the Merchant details (Merchant ID, Merchant name, Acquirer BIN or Merchant country) from the PAReq match the corresponding details on the Watchlist.

You can search for Merchant details in the Merchant Watchlist, import a file of Merchant details or add individual Merchant details to the list and edit Merchant details.

The first page in this section is **Search Merchant Watchlist**.

Search Merchant Watchlist

Rules > Rule Management > Authentication > Merchant Watchlist > Search Merchant Watchlist

This page displays:

- **Search** button to search for Merchant details already in the Merchant Watchlist.
- **Import** button to import a file of Merchant details to add to the list

> **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml

- **Add** button to add individual Merchant details to the list

To search for a Merchant:

- **Issuer** name is displayed and cannot be changed.
- Enter Merchant details as follows, or leave them blank to display all Merchants on the Watchlist:
  - Enter a **Merchant ID**
  - Enter a **Merchant name**
  - Enter an **Acquirer BIN**
  - Select a **Merchant country** from the drop down list. Default is All.
- Click the **Search** button.

The **Merchant Watchlist** page is displayed.

Merchant Watchlist Search Results

Rules > Rule Management > Authentication > Merchant Watchlist > Merchant Watchlist Search Results

Merchant details are listed according to the search criteria you entered on the **Search Merchant Watchlist** page. You can add an individual Merchant or import a file of Merchants to the list or select any Merchant to delete or edit it.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more sets of Merchant details
- **Delete** button used in conjunction with selected Merchant details
- **Merchant Id**, **Merchant Name**, **Acquirer BIN** and **Merchant Country** links to the **Edit Merchant Watchlist** page

- Links for **Add** and **Import**

To add individual Merchant details:

- Click the **Add** link.

  The **Add Merchant Watchlist** page is displayed.

To import a file of Merchant details:

- Click the **Import** link.

  The **Import Merchant Watchlist** page is displayed.

> **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml

To delete Merchant details:

- Select the checkbox adjacent to the Merchant ID and click the **Delete** button.

  Confirmation of the deletion is displayed.

Edit Merchant Watchlist

Rules > Rule Management > Authentication > Merchant Watchlist > Edit Merchant Watchlist

To edit the Merchant Watchlist:

- **Issuer** name is displayed and cannot be changed.
- Edit any of the Merchant fields:
  - **Merchant Id**
  - **Merchant Name**
  - **Acquirer BIN**
  - **Merchant Country**.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Merchant Watchlist Search Results.

Add to Merchant Watchlist

Rules > Rule Management > Authentication > Merchant Watchlist > Add to Merchant Watchlist

This page is used to add Merchant details to the Merchant Watchlist.

A new Merchant Watchlist rule can be created by entering a value in at least one of the fields on the page:

When checking whether a transaction matches the Merchant Watchlist, the system will compare the Merchant Id, Merchant Name, Acquirer BIN and Merchant Country from the PAReq, with the values entered.

To add to the Merchant Watchlist:

- **Issuer** name is displayed and cannot be changed.
- Enter a value into any of the Merchant fields:
  - **Merchant ID**
  - **Merchant Name**
  - **Acquirer BIN**
  - **Merchant Country** select from the drop down list.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Merchant Watchlist Search Results.

Import Merchant Watchlist

Rules > Rule Management > Authentication > Merchant Watchlist > Import Merchant Watchlist

This page is used to import a file of merchant watchlist rules to add to the Merchant Watchlist. The format of the file should be CSV, with each record incorporating values for any of the required Merchant Id, Merchant Name, Acquirer BIN and Merchant Country fields necessary to define the rule.

> **Note**
>
> Merchant country is defined by a country code and name and uses the format:
>
> < ISO 3166-1 numeric code> < ISO 3166-1 country name>
>
> For example:
>
> 008/Albania
>
> 024/Angola
>
> 036/Australia

To import a file of merchant watchlist rules:

- **Issuer** name is displayed and cannot be changed.
- Click the **Choose File** / **Browse** button to locate and select the **File name**.

  The **No file chosen** message will be replaced with the name of the file to be imported.

  > **Note**
  >
  > A maximum of 1000 records can be imported at one time.

- Click the **Apply** button.

  A confirmation message will be displayed.

Location Watchlist

If the merchant's country is on the Location Watchlist, the authentication procedure will be initiated. If the merchant's country is not on the list, the remaining business rules will be applied.

> **Note**
>
> If the merchant's country is not on the list, the cardholder will be considered to be transparently authenticated and transaction status will set to **Y** or **A**, as configured under the **Settings** tab.

You can search for Locations, import a file of Locations or add an individual Location to the list.

The first page in this section is **Search Location Watchlist**.

Search Location Watchlist

Rules > Rule Management > Authentication > Location Watchlist > Search Location Watchlist

This page displays:

- **Search** button to search for countries already in the Location Watchlist.
- **Import** button to import a file of countries to add to the list

> **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml.

- **Add** button to add individual countries to the list

To search for a Location:

- **Issuer** name is displayed and cannot be changed.
- Select a **Merchant country** from the drop down list. Default is All.
- Click the **Search** button.

  The **Location Watchlist** page is displayed.

Location Watchlist Search Results

Rules > Rule Management > Authentication > Location Watchlist > Location Watchlist Search Results

Merchant countries are listed according to the search criteria you entered on the **Search Location Watchlist** page. You can add an individual Merchant country or import a file of Merchant countries to the list or select any Merchant country to delete or edit it.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more Merchant Countries
- **Delete** button used in conjunction with selected Merchant Countries
- **Merchant Country** link to the **Edit Location Watchlist** page
- Links for **Add** and **Import**

To add individual Merchant countries:

- Click the **Add** link.

  The **Add Location Watchlist** page is displayed.

To import a file of Merchant countries:

- Click the **Import** link.

  The **Import Location Watchlist** page is displayed.

> ✎ **Note**
>
> The supported file formats for uploading rule configurations are .csv and .xml.

To delete Merchant countries:

- Select the checkbox adjacent to the Merchant Country and click the **Delete** button.

  Confirmation of the deletion is displayed.

Edit Location Watchlist

Rules > Rule Management > Authentication > Location Watchlist > Edit Location Watchlist

Editing a Merchant country replaces the selected country with the new country selected.

To edit the Location Watchlist:

- **Issuer** name is displayed and cannot be changed.
- Edit **Merchant country** by selecting a different country from the drop down list.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Location Watchlist Search Results.

Add to Location Watchlist

Rules > Rule Management > Authentication > Location Watchlist > Add to Location Watchlist

This page is used to add individual Merchant countries to the Location Watchlist.

When checking whether a transaction matches the Merchant Watchlist, the system will compare the Merchant Country from the PAReq, with the Merchant countries entered on the watchlist.

To add to the Location Watchlist:

- **Issuer** name is displayed and cannot be changed.
- Select a **Merchant Country** from the drop down list.
- Click the **Apply** button.

  A confirmation message will be displayed.
- Click the **Back** button to return to the Merchant Watchlist Search Results.

Import Location Watchlist

Rules > Rule Management > Authentication > Location Watchlist > Import Location Watchlist

This page is used to import a file of merchant countries to add to the Location Watchlist. The format of the file should be CSV, with each record incorporating a Merchant country value.

> **Note**
>
> Merchant country is defined by a country code and name and uses the format:
> < ISO 3166-1 numeric code>/< ISO 3166-1 country name>
>
> For example:
>
> 008/Albania
>
> 024/Angola
>
> 036/Australia

To import a file of Location watchlist rules:

- **Issuer** name is displayed and cannot be changed.
- Click the **Choose File** / **Browse** button to locate and select the **File name**.

  > **Note**
  >
  > A maximum of 1000 records can be imported at one time.
- Click the **Apply** button.

A confirmation message will be displayed.

Domestic & International Transaction Amount Threshold

Rules > Rule Management > Authentication > Domestic & International Transaction Amount Threshold

The domestic and international transaction thresholds determine if the authentication procedure is to be initiated or bypassed.

The Domestic threshold is used when the transaction purchase currency is the selected Default Currency; otherwise, the International threshold is used.

If the transaction amount is less than the defined transaction amount threshold, the cardholder will be transparently authenticated.

If the transaction amount is greater than or equal to the threshold, the authentication procedure will be initiated.

> **Note**
>
> If the transaction currency is not in the currency file, the default will be for the Issuer ACS to pass the PARes back to the merchant indicating Cardholder Transparently Authenticated.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more sets of rules.
- **BIN** links to the **Edit Domestic & International Transaction Amount Threshold** page.
- **Delete** button used in conjunction with selected rules.
- Links for **Manage Exchange Rates** and **Add**.

To manually create currency exchange values:

- Click the **Manage Exchange Rates** link.

  The **Manage Exchange Rate** page is displayed.

To add Domestic & International Transaction Amount Threshold rules:

Rules > Rule Management > Authentication > Authentication > Domestic & International Transaction Amount Threshold > Add

- Click the **Add** link.

The **Add Domestic & International Transaction Amount Threshold** page is displayed.

> **Note**
>
> The *Add* link is disabled when a rule has been set for All BINs of the selected issuer.

To delete a rule:

- Select the checkbox adjacent to the BIN and click the **Delete** button.

  Confirmation of the deletion is displayed.

To set Domestic & International transaction amount thresholds:

- **Issuer** name is displayed and cannot be changed.
- Select the **BIN** to be used for the threshold from the drop down list.
- Enter a **Domestic amount** for the threshold.
- Enter an **International amount** for the threshold.
- Select the currency to be used for the domestic threshold from the **Default currency** drop down list.
- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

Manage Exchange Rates

Rules > Rule Management > Authentication > Domestic & International Transaction Amount Threshold > Manage Exchange Rates

Currency exchange values can be manually defined for each issuer to set customised exchange rates or for rates not available on the automated list. These rates take precedence over the general rates that are downloaded from external resources or manually defined by the system administrator in System Management > Exchange Configuration.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more defined exchange rates.
- *Base Currency* links to the **Edit Exchange Rate** page.
- **Delete** button used in conjunction with selected exchange rates.
- **Add** link to add an exchange rate.

To manually create currency exchange values:

Rules > Rule Management > Authentication > Domestic & International Transaction Amount Threshold > Manage Exchange Rates > Add

- Click the *Add* link.

  The **Add Exchange Rate** page is displayed.

To delete a defined exchange rate:

- Select the checkbox adjacent to the Base Currency and click the **Delete** button.

  Confirmation of the deletion is displayed.

To manually create currency exchange values:

- **Issuer** name is displayed and cannot be changed.
- Select the **Base currency** and **Target currency** to be used for the currency exchange rate from the drop down list.
- Enter a **Rate** for the currency exchange.
- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

Stand-In Transaction Threshold

Rules > Authentication Exemption > Stand-In Transaction Threshold

The Stand-In Transaction Threshold rule is applied if the remote authentication server (CAAS) cannot be contacted or is not responding at the Verify Registration (first message to CAAS) stage.

However, if the cardholder is in the middle of the authentication process and has commenced selection and the CAAS cannot be contacted or is not responding then the Issuer ACS will be unable to authenticate the transaction and Transaction Status will be set to 'U' (Unable to authenticate).

> **Note**
>
> If the transaction amount (AUD or converted to AUD) is less than the Stand-In threshold, the Issuer ACS will pass the PARes back to the merchant indicating Cardholder Transparently Authenticated.

The following fields and links are displayed:

- **Select** checkbox for selecting one or more sets of rules.
- *BIN* links to the **Edit Stand-In Transaction Threshold** page.
- **Delete** button used in conjunction with selected rules.
- Links for **Manage Exchange Rates** and **Add**.

To manually create currency exchange values:

- Click the **Manage Exchange Rates** link.

  The **Manage Exchange Rate** page is displayed.

To add Stand-In Transaction Threshold rules:

Rules > Authentication Exemption > Stand-In Transaction Threshold > Add

- Click the **Add** link.

  The **Add Stand-In Transaction Threshold** page is displayed.

> **Note**
>
> The *Add* link is disabled when a rule has been set for All BINs of the selected

issuer.

To delete a rule:

- Select the checkbox adjacent to the BIN and click the **Delete** button.

  Confirmation of the deletion is displayed.

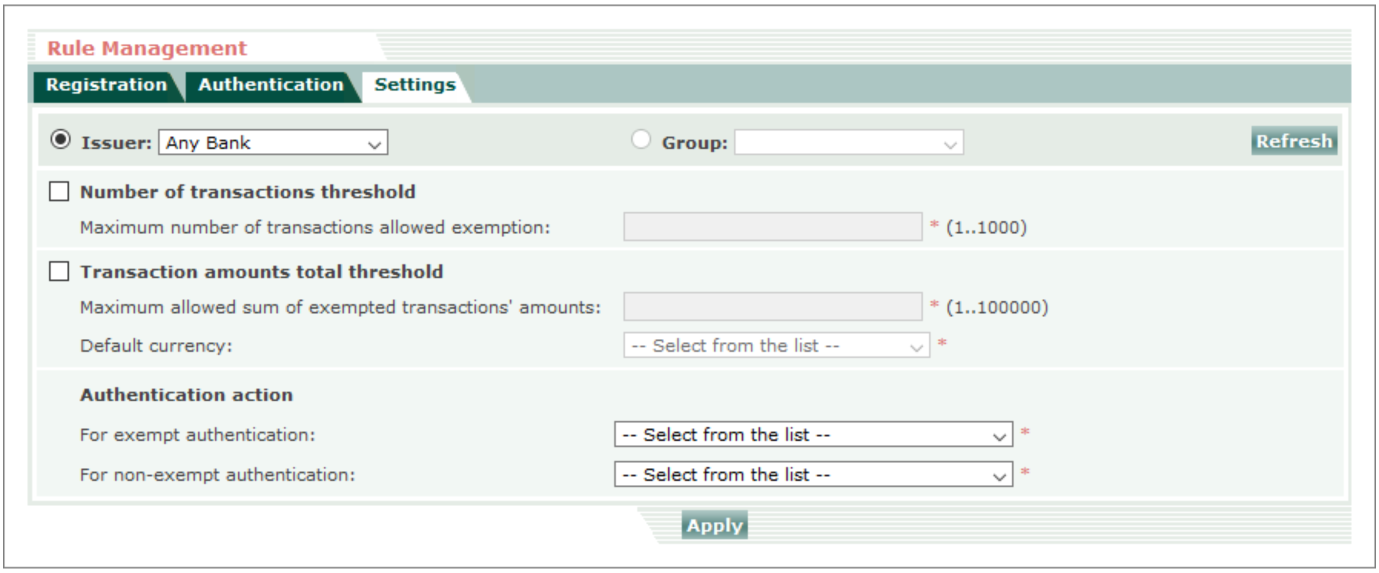
To set Stand-In Transaction thresholds:

- **Issuer** name is displayed and cannot be changed.
- Select the **BIN** to be used for the threshold from the drop down list.
- Enter an **Amount** for the threshold.
- Select the default currency to be used for the threshold from the **Currency** drop down list.
- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

Settings

Rules > Rule Management > Settings



Rule Management

● Issuer: Any Bank ○ Group: Refresh

□ Number of transactions threshold

Maximum number of transactions allowed exemption: * (1..1000)

□ Transaction amounts total threshold

Maximum allowed sum of exempted transactions' amounts: * (1..100000)

Default currency: -- Select from the list -- *

Authentication action

For exempt authentication: -- Select from the list -- *

For non-exempt authentication: -- Select from the list -- *

This section is used to set thresholds, by issuer or issuer group, for the number of transactions and the transaction amounts total (which determine if the authentication procedure is to be initiated or bypassed). It is also used to define the authentication response (PARes) and transaction status for cardholders when authentication is bypassed.

If one threshold is specified - if the **number of transactions or** the **transaction amounts total** is less than the specified threshold, the cardholder will be transparently authenticated.

If both thresholds are specified, if the **number of transactions and** the **transaction amounts total** are less than the specified thresholds, the cardholder will be transparently authenticated.

If the **number of transactions or** the **transaction amounts** total is greater than or equal to the specified thresholds, the authentication procedure will be initiated.

Use the following fields to view / edit the Settings:

- If the required **Issuer** or an **Issuer Group** is not displayed, select it from the appropriate drop down list.
- Click the **Refresh** button.

Note

These fields are not displayed if the user is assigned to a single issuer.

- To set a **Number of transactions threshold**, select the checkbox and enter a number from **1** to **1000** (inclusive) in **Maximum number of transactions allowed exemption**. This is the number of times a cardholder can be exempt, after which time they will be required to be authenticated. Once authenticated successfully, the transaction count is reset to 0.
- To set a **Transaction amounts total threshold**, select the checkbox and enter an amount from **1** to **100000** (inclusive) in **Maximum allowed sum of exempted transactions amounts**. Once the cardholder is authenticated successfully, the transaction amounts total is reset to 0.
- Select the **Default** currency, which will apply to the transaction amounts total, from the drop down list.
- To select an **Authentication action** for exempt and non-exempt authentication, select from the appropriate drop down lists for the selected issuer or issuer group:
- **For exempt authentication** - the options are:

  Set PARes='A' (Attempted)

  Set PARes='Y' (Approved)
- **For non-exempt authentication** - the options are:

  Set PARes='N' (Not approved)

  Show authentication page
- Click the **Apply** button to save changes.

Admin Users

System Administrators and **Member Administrators**

This section is used to set up and manage administrative users. A pre-defined access level group assigned to the username determines the access level of each administrative user. A **read only** option is available for each access level group to provide access to the appropriate sections for support roles that are not required to add records, edit details or upload files.

When the Issuer system is first installed, it creates the main administrative user, named **administrator**, by default. The **administrator** user has the highest level of access throughout the issuer system and can create other users that have restricted access rights, are restricted to certain tasks or are have limited access to a certain issuer.

The access level groups are:

- **System administrator**

  This is the highest level of access in the system with access to system options, issuer management, user management, cardholder management, transactions, reporting and audit log.

- **Issuer administrator**

  This level provides access to issuer configuration options, cardholder management, transactions, reporting and audit log.

- **IT security administrator**

  This level provides dedicated access to the **Audit Log**, for an issuer or issuer group

- **Member administrator**

  This level provides dedicated access to the **Admins** section (administration user management), for an issuer or issuer group

- **Business administrator**

The business level of access to the system provides access to cardholder management, transactions, reporting and audit log.

- **Helpdesk**

  The helpdesk user can access cardholder management and transactions.

> **Note**
>
> If the issuer has access to business rules functionality, **Business admin** and / or **Helpdesk** users can be granted access to the Rules section, refer to Section 3.1.3.4 - Issuer Details for further information.

The ActiveAccess issuer system is designed for simultaneous use by multiple issuers, with each access level being able to be restricted to a certain issuer or a group of issuers. This provides the flexibility of allowing a third party to manage multiple issuers on their behalf as well as allowing each issuer to manage their own system without having access or interfering with other issuers.

Normally when a new issuer signs up with the system, the system administrator creates a new issuer and a new issuer administrator. The issuer administrator can then create business administrator and helpdesk users as appropriate for their requirements.

***Admins** has the following menu options:*

- **Find Admin** for maintaining administrative users and their details
- **New Admin** for adding new administrative users

Find Admin

This page allows you to search for an administrative user based on Status, Group, Username, Full name, Issuer or Issuer group.

Admins > Find Admin

Use the following fields to search for an Admin user:
You can leave all fields at default or blank to display a list of all admin users.

- Select a **Status** or **All** from the drop down list. You can search for enabled or disabled administrative users or both.

- Select a **Group** or **All** from the drop down list. Depending on your access level you may be able to search for **System Admin**, **Issuer Admin**, **IT Security, Member Admin**, **Business Admin** or **Helpdesk** users.
- Enter all or part of the administrator's **Username**.
- Enter all or part of the administrator's **Full name.**
- Select an **Issuer** or **All** from the drop down list.
- Select an **Issuer Group** or **All** from the drop down list.
- ***Search*** button to display results

The **Search Result** page will be displayed.

Admin Search Results

Admins > Find Admin > Search Results

Administrative users are listed according to the search criteria you entered on the **Find Admin** page. You can select any administrative user and delete, enable or disable them.

> **Note**
>
> The main system administrator (administrator) is not displayed in the search results and cannot be disabled or removed.

You can also browse to the admin details page by following the link under **Username** or **Full name** and you can also use the **Change password** link to reset a user's password.

Use the following steps to delete, enable or disable an administrative user:

- Choose one or more users by clicking the **Select** checkbox adjacent to the **Username**
- Click the **Delete**, **Enable** or **Disable** button as appropriate.

  A confirmation message will be displayed.

Use the following steps to select an administrative user:

- Click the **Username** hyperlink for the user for which you wish to view or edit details.

  The **Admin Details** page is displayed.

Use the following steps to change an administrative user's password:

- Click the **Change password** hyperlink for the user whose password you wish to change.

  The **Change Password** page is displayed.

*Use the following steps to select **all** items that match the search criteria:*

- Click the checkbox under the **Select** column to select or unselect all items. This allows you to perform the desired action on all selected items.

> ⚠ **Warning**
>
> **Important:** The display of search results is limited to 400 records, however if you select all records, all records matching the search criteria will be affected by the action you choose to perform.

> ⚠ **Warning**
>
> Performing the selected action on a large number of records may take a long time to complete and will generate the equivalent number of audit log records. Use this functionality on a large number of records diligently and only where strictly necessary.

Admin Details

Admins > Find Admin > Search Results > Admin Details

This page allows administrative personnel with the appropriate access rights to update administrative user information.

> **Note**
>
> System administrators have access to all admin users. Issuer administrators have access to business admin and helpdesk users.

The following admin details are displayed on this page:

- **Status**

  Can be either **enabled** or **disabled**. A user in a disabled state will not be able to login to the system.

> **Note**
>
> The main administrator cannot be disabled.

- **Last login**

  Shows the date and time of last login by the user of this administrative account.

- **Group**

  Indicates the level of access a user has in the administration server and cannot be changed. There access levels are:

  - **System Admin**
  - **Issuer Admin**
  - **IT Security Admin**
  - **Member Admin**
  - **Business Admin**
  - **Helpdesk**.

  You can create a user at any one of these access levels with **Read only** access by selecting the Read only checkbox below.

  Only administrators that belong to the System Admin and Issuer Admin groups have access to the Admins section and can create new admin users. Issuer Admin group users may only create Business Admin and Helpdesk users. System Admin users may create users at any and all levels.

> **Note**
>
> The main administrator's group cannot be changed.

- **Issuer** or **Issuer Group** radio button

  Specifies which issuer or issuer group the issuer admin user can access. Issuer admin users may be assigned to a previously defined issuer group rather than a single issuer, which enables them to manage multiple issuers.

  Administrators who belong to System Admin group can always access all issuers and as such, issuer selection for system administrators is not required.

- **Username**

A unique name used to identify the administrative user and used for logging into the administration server. The main administrator's username is always **administrator** and cannot be changed.

- **Full name**

  Optional user information that is stored for housekeeping purposes.

- **Email address**

  Optional user information that is stored for housekeeping purposes.

- **Contact number**

  Optional user information that is stored for housekeeping purposes.

- **Address**

  Optional user information that is stored for housekeeping purposes.

- **Change Password** (***Admins > Find Admin > Search Results > Change Password***)

  While administrators with a higher access level cannot access or see other admin passwords, they can reset or change other users' password. The newly selected password may only be valid for first login if "User must change password at next logon" option is selected.

- **Read only access** checkbox

  Select this checkbox if the user performs a support role that is not required to add records, edit details or upload files, for example.

- **Two-factor authentication login** checkbox

  Select this checkbox if you want to enable two-factor authentication when this user logs in.

> **Note**
>
> An email will be sent to the user with a QR code, to be used with Google Authenticator. To use this option, mail server must be configured in ***System Management > Settings***. For more information, refer to Login.

- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

  OR

  Click the **Back** button to return to the **Search Results** page without saving any changes.

Use the following steps to change an administrative user's password:

- **Username** is displayed and cannot be changed.
- Enter the new **Password.**
- Confirm the new password in the **Re-enter new password** field.
- Click the **User must change the password at next logon** checkbox, if required.
- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

New Admin

Admins > New Admin

All ActiveAccess administrative users must be set up in this section.

Creating a new administrative user:

- **Status**

  Can be either **enabled** or **disabled**. A user in a disabled state will not be able to login to the system.

- **Group**

  Indicates the level of access a user has in the administration server. There access levels are:

  - **System Admin**
  - **Issuer Admin**
  - **IT Security Admin**
  - **Member Admin**
  - **Business Admin**
  - **Helpdesk**

  You can create a user at any one of these access levels with **Read only** access by selecting the **Read only access** checkbox.

  Only administrators that belong to the System Admin and Issuer Admin groups have access to the Admins section and can create new admin users.

System Admin users may create users at any and all levels. There is no interdependency between System Admin users and the other users they create.

- **Issuers** or **Issuer Groups**

  Choose the appropriate radio button and select an **Issuer** or an **Issuer group** from the drop down list.

  Administrators who belong to the System Admin group can always access all issuers and as such, issuer selection for system administrators is not required.

- **Username**

  A unique name used to identify the administrative user and used for logging into the administration server. The main administrator's username is always **administrator** and cannot be changed.

- **Password**

  Enter a password

- **Re-enter password** to confirm it.
- Select the **User must change password at next logon** checkbox if you want this password to be valid for the user's first login only.
- Select the **Two-factor authentication login** checkbox if you want to enable two factor authentication when this user logs in.

> **Note**
>
> An email will be sent to the user with a QR code, to be used with Google Authenticator. To use this option, mail server must be configured in ***System Management > Settings***. For more information, refer to Login.

- **Full name**

  Optional user information that is stored for housekeeping purposes.

- **Email address**

  May be used by the system in order to send email notifications, if the appropriate option is configured by the system administrator.

  If `Two-factor authentication login` is enabled, this email address will be used for sending a QR code to the user. Mail server must be configured in ***System Management > Settings***.

- **Contact number**

Optional user information that is stored for housekeeping purposes.

- **Address**

  Optional user information that is stored for housekeeping purposes.

- **Read only access** checkbox

  Select this checkbox if the user performs a support role that is not required to add records, edit details or upload files, for example.

- Click the **Apply** button to save changes.

  A confirmation message will be displayed.

> **Note**
>
> For further information on individual fields, please refer to Admin Details.

Cards

> *The **Cards** tab was previously named **Users***

System Administrators, **Issuer Administrators**, **Business Administrators**, **Helpdesk Users**

This section is used for registering and maintaining individual users or cards. You can search for users or cards; enable or disable users or cards; view user and card information (including the enrolment status); update user and card information; and pre-register new users or cards.

Info

Please see **Upload Registration Files** in the **Issuers** section for uploading card data for bulk registration or pre-registration of cardholders.

Note

This page will not be available for remote issuers.

Cards has the following sub menu options:

- **Find Card** - for maintaining cards and card details
- **New Card** - for adding new cards
- **Find User** - for maintaining users and user details
- **New User** - for adding new users

The first **Cards** page is **Find Card**.

Find Card

Cards > Find Card

This page allows you to access card related information by searching for cards based on name on card, card number, issuer, BIN, enrolment status, card status, device authentication enabled or disabled, pre-registration or registration date range.

> **Note**
>
> Finding a card using a card number is only possible if you enter the full card number. There is no partial number search or wild card search available.

> **Note**
>
> Search results display the first 400 cards only.

> **Note**
>
> An export function, which allows you to download lists, is available for the following:
>
> - Pre-registered cardholders for an issuer or issuer group, using the Confirmation Method
> - Cardholders for an issuer or issuer group using the Confirmation Method.
>
> Although the display is limited to the first 400 cards for the selected issuer or issuer group, the full list can be downloaded when the **Export** link is selected.

Use the following fields to find cards to download a list of pre-registered cards:

> **Note**
>
> Only Issuers or Issuer Groups that are using the Confirmation Method can download a list of pre-registered cards.

- Select an **Issuer** or **Issuer Group**
- Select Pre-registered as the **Enrolment Status**.
- Click the ***Search*** button

  The **Search Result** page will be displayed, showing the pre-registration date, in addition to the standard fields.
- Click the ***Export*** button to download a file containing the relevant cardholder data.

> **Note**
>
> Exporting is only available to administrators with System Admin and Issuer Admin access level.

Use the following fields to find cards to download a list of cardholders:

> **Note**
>
> It is only possible to download a list of cardholders for Issuers or Issuer Groups that are using the Confirmation Method. Cardholders can be filtered by confirmation status and confirmation date.

- Select an Issuer or Issuer Group
- Select Registered as the **Enrolment Status**.
- Click the ***Search*** button

  The **Search Result** page will be displayed, showing the pre-registration date, in addition to the standard fields.
- Click the ***Export*** button to download a file containing the relevant cardholder data.

> **Note**
>
> Exporting is only available to administrators with System Admin and Issuer Admin access level.

Use the following fields to search for a particular card:

- There are two options when searching for a card: by entering the card number or by entering the cardholder name (exactly as embossed on the card) and selecting the issuer from the drop down list.
- Enter the cardholder's full **Name on Card** and select the **Issuer** of the card from the drop down list to view all matching records. The cardholder name is not case sensitive.
- Enter the full **Card number**. Multiple search results are displayed when a card account has more than one cardholder.
- Enter the full **Authentication Method** to show cards from only one authentication scheme. J/Secure, ProtectBuy, SafeKey, SecureCode and VbV schemes available.
- Select the Issuer from the drop down list or select the Group from the drop down list.
- Select the **BIN** from the drop down list.

- Select the card's **Enrolment Status** from the drop down list. You can choose to search for **All**, **Pre-registered**, **Registered**, or **Re-activated** cards.
- Select the card's **Status** from the drop down list. You can choose to search for enabled, disabled or locked cards.
- Select to search for card for which **Device authentication** enabled or disabled. This allows you to limit the results for cards that support two-factor authentication over 3-D Secure or those that do not.
- Select the **Device type** that has been registered for the Card from the drop down list. You can choose to search for VASCO, SMS, RSA, Email, CAP (M-Chip 4), or CAP (M-Chip 2).
- Enter the **Device serial number** (unique device identifier) that has been registered for the Card.
- Enter the card's record identifier (**Card ID**) to locate a specific record. This is used for advanced diagnostics where the record identifier is obtained directly from the database.
- Specify an optional date range to limit search results based on the card's **Pre-registration Date**.
- Specify an optional date range to limit search results based on the card's **Registration Date**.
- Click the ***Search*** button.

The **Search Result** page will be displayed.

Card Search Result

Cards > Find Card > Search Result

Cards are listed according to the search criteria you entered on the **Find Card** page. You can select any card and delete, enable or disable them.

The search result page shows card number, name on card, expiry date, issuer enrolment status and card status. Expiry date is an optional field and is only displayed if it was provided at registration.

The card's enrolment status can be either **pre-registered** or **registered**.

The **Search Result** page may return multiple results for a single card number depending on whether this is an account with multiple cardholders or not. Card numbers with multiple cardholders can be distinguished based on the cardholder name.

> **Note**
>
> The issuer system uses the combination of card number and cardholder name (name on card) as the key identifier for authentication purposes.
>
> Card numbers with different card names are treated independently and as such each cardholder can have their separate authentication data. This also means that enabling/disabling registration are handled separately. *For example if you wish to completely remove a card from the issuer system, be sure to select and remove all cardholders.*

You can browse to the card details page by following the link under **Card Number** or **Name on Card**.

Use the following steps to delete, enable or disable a card:

- Choose one or more cards by clicking the **Select** checkbox adjacent to the **Card Number**
- Click the appropriate ***button***.

  A confirmation message will be displayed.

Use the following steps to select a card:

- Click the **Card Number** hyperlink for the card you wish to view or edit details.

  The **Card Details** page is displayed.

Use the following steps to select all items that match the search criteria:

- Click the box under the **Select** column to select or unselect all items. This allows you to perform the desired task on all selected items.

  You should note that all items matching the search criteria will be affected. This includes items displayed on other pages and even those omitted due to the large number of results (display of search results is limited to a maximum of 400 records).

> **Note**
>
> **Important:** If you are selecting a large number of records, you should remember that the operation can take a long time to complete and will generate an audit log record per affected item. Use this functionality on large number of records with diligence and where only strictly necessary.

Card Details

Cards > Find Card > Search Result > Card Details

The following card details can be viewed/ edited on this page:

- **Issuer**

  Shows card's issuing bank and cannot be changed.

- **BINs** - Displays a list of BINs assigned to the issuer. This field is for information only. Issuer BIN can be modified by an administrator with System Admin access level through **System Management > Issuers > Issuer Details > BIN Management** page.
- **Card ID** - Unique card number, which cannot be changed.
- **Status** - Can be **Enabled**, **Disabled** or **Locked**. A card is enabled when the cardholder is first enrolled.

  For security reasons, administration staff may temporarily disable a card.

  A card may also be locked by the system if multiple unsuccessful authentication attempts are detected.

  If the cardholder is enrolled and the card is disabled or locked, it cannot be used to make authenticated payments.

  If the cardholder is not enrolled, the enrolment process cannot be completed if the card is disabled.

  Cards that are locked by the system can be unlocked by administration staff or after a time-out period, as specified in the issuer settings. A card cannot be manually locked.

- **BIN status** - Shows the BIN status, which is either **Enabled** or **Disabled**, indicating the availability of the 3-D Secure service for the card. Cards with a **Disabled** BIN cannot be enrolled, registered or authenticated.
- **Registration date** - Displayed if cardholder is enrolled.
- **Enrolment** - Shows the enrolment status, which is either registered or pre-registered, along with the **Pre-registration** and **Registration date**. If the Issuer is using the Confirmation method, the **Confirmation status** and **Confirmation** date will also appear in this section.
- **Authentication Method** - Specifies the card's authentication scheme and cannot be changed. Currently **SafeKey**, **ProtectBuy**, **J/Secure**, **SecureCode** and **Verified by Visa** schemes are supported.
- **Card number** - Full card number, partially masked.

> **Note**
>
> Please note that the card number must comply with the Luhn / mod 10 algorithm.

- **Name on Card** - Cardholder name as specified on the card.
- **Expiry date** - Card expiry date (MM/YYYY).
- **Device authentication** (if enabled) - Drop down list shows the status of two-factor authentication for 3-D Secure as Enabled. Select Disabled to disable device authentication for this card and the drop down list will be removed once you click ***Apply***.

  A card, for which device authentication is enabled, can use an authentication device in addition to the conventional 3-D Secure password as a second factor of authentication.
- **Number of ADS cancellations** - Shows the number of times a cardholder has refused to complete activation during shopping by either opting out of ADS or cancelling the transaction.
- **ADS proof of attempts granted** - Shows the number of times a cardholder has been granted proof of authentication attempt without being required to complete the activation during shopping process.

> **Note**
>
> Where Business Rules are being used and a rule has matched, this value is set to the maximum automatically and therefore the value may not be a true representation of the number of ADS proof of authentication attempts that have been granted to this cardholder.

- **Extended cardholder information** - Each card is also associated with one or more authentication or data fields. The issuer determines the format and number of these fields. Extended cardholder information is only displayed if the system administrator enables this option in the **Issuer Management** section.

  For example a card may be accompanied by / associated with:

  - A **PAM** (Personal assurance message or the greeting message as required in VbV, J/Secure, ProtectBuy, SafeKey and SecureCode schemes)
  - An **Internet PIN** (for secure online transactions). Fields such as Internet PIN are always displayed masked.
  - **Question** and **Answer** fields used for Challenge and Response.
  - A user's authentication **Password**

- **Assigned Devices** appears for cards for which device authentication is enabled and links to a Search Results page, which displays authentication devices assigned to this card.
- **Account History** links to Account History details page, which shows actions affecting account status or the devices attached to the account.
- **Show Transactions** links to the Search Results page, which displays all transactions for this card.
- **Generate Activation Code** link allows the administrator to generate an activation code for a replacement device. The link is only shown if the card's primary device is marked as lost or damaged. The cardholder requires this activation code before they can complete linking the replacement device with an existing account.

Assigned Devices

Cards > Find Card > Search Result > Card Details > Assigned Devices

Assigned Devices displays all devices attached to the selected card. It enables you to assign a new device to a card, remove an assignment or change the status of assigned devices to **Lost**, **Damaged** or **Temporarily disabled**.

The following fields and links are displayed:

- **Device Management** - links to the **Device Management** page for manually assigning a new or existing device to the card, or deleting an existing device.

The following fields and links are displayed for each assigned device:

- **Select** checkbox - for selecting the device to use in conjunction with the ***Remove Assignment*** button or ***Delete*** button. To remove assignment of all devices, click the select checkbox in the column heading and then click the ***Remove Assignment*** button. To completely delete a previously registered device from the system, click the adjacent **Select** checkbox and then click the ***Delete*** button.

  If you select all devices a Warning dialog is displayed asking you to confirm that you want to remove all records that match the search criteria.
- **Device ID** links to the **Device Details** page
- **Assign date** - Date and time device was assigned
- **Serial Number** - The unique device identifier
- **Device type** - The type/make of the device such as VASCO, RSA, Email, CHIP, etc

- **Status** - **Active**/**Lost/Damaged/Temporarily disabled**. An active device can be used in device authentication. If a device is reported lost, stolen, damaged, or temporarily disabled, it must be flagged accordingly. A lost or damaged device can no longer be used for authentication and the user must be issued with a new device. A temporarily disabled device allows administrators to generate a new backup token.
- **Mark as** -
  - **Lost** - click to change the status of the selected device to **lost**.
  - **Damaged** - click to change the status of the selected device to **damaged**.
  - **Temporarily disabled** - click to change the status of the selected device to **temporarily disabled**.
- **Generate Backup Token** link is only shown when the card's primary authentication device is marked as temporarily disabled. Providing the user with a backup token allows the user to continue using the service while they wait for the replacement authentication device to arrive.

  The application currently supports two mechanisms for generating backup tokens: a replacement password (the default) and SMS.

  A replacement password is a static password that can be used as the second factor of authentication for a limited time and for a limited number of times. Using a static password will not be as secure as using an authentication device. Administrators should only issue backup tokens if allowed by the issuer's security policy and if in line with the issuer's requirements for identifying a user.

  A more secure alternative is to use SMS as the backup token, if supported by the issuer device settings. This allows the admin to temporarily switch the user's authentication process to SMS authentication. The user will need to provide a mobile number to which the second factor of authentication will be sent via SMS.

  Note that the first SMS batch is not sent immediately. The SMS is sent when the user attempts to perform their next authentication. They may have to wait a few minutes, once they attempt to login next time, for the batch SMS to arrive. Once they receive the first batch SMS, they will continue to receive replacement batch SMS tokens when they use up all the numbers in their current batch.

Device Management

Device Management provides the option to manually assign a new or existing device to the card, or delete an existing device. This is useful for call centre assisted registration of cards. The user needs to provide a token generated by their device in order to complete the assignment. You can either find an existing device that is already registered in the system and verify it or specify a new device to assign and activate.

- Click the appropriate tab to select the following options:
    - **Find Device**
    - **Assign Existing Device**
    - **Assign New Device**.

Find Device

Cards >Card Details > Assigned Devices > Device Management > Find Device

- Select an **Issuer** or **All** from the drop down list
- Enter a **Creation date** and time (dd/mm/yyyy HH:MM) or specify a date and time range for the search result by entering dates and times in the **From** and **To** fields. The date and time format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.
- Select a **Device type**, such as VASCO, SMS, RSA, Email, CHIP, etc
- Enter a **Device Serial number** or specify a serial number range for the search result by entering serial numbers in the **Start** and **End** fields.
- Click ***Search***

A list of devices matching the search criteria will be displayed.

- To remove a device, click the ***Select*** radio button, adjacent to the appropriate **Device ID**, and click the ***Delete*** button.

  This will remove the device from the system.

Assign Existing Device

Cards > Card Details > Assigned Devices > Device Management > Assign Existing Device

Use the following fields to find an existing device:

- Select an **Issuer** or **All** from the drop down list
- Enter a **Creation date** and time (dd/mm/yyyy HH:MM) or specify a date and time range for the search result by entering dates and times in the **From** and **To** fields. The date and time

format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.

- Select a **Device type**, such as VASCO, SMS, RSA, Email, CHIP, etc
- Enter a **Serial number** or specify a serial number range for the search result by entering serial numbers in the **Start** and **End** fields.
- Click ***Search***

  A list of devices matching the search criteria will be displayed.
- Click the **Select** radio button, adjacent to the appropriate **Device ID**, and click the ***Apply*** button

  The **Verify Device** page is displayed

Assign New Device

Cards > Card Details > Assigned Devices > Device Management > Assign New Device

Use the following fields to assign a new device:

- Select the **Assign New Device** tab

NEW SMS DEVICE

- Select **SMS** from the **Device type** drop down list.
- Click the ***Apply*** button.

  The **New SMS Device** page is displayed.
- Select an **SMS centre** from the drop down list.
- Select the **Country calling code** for the country that the mobile number is registered to.
- Enter the **Mobile number** of the cardholder. Mobile number should be no longer than 20 characters, including the Country code. Allowed characters are 0-9, '(', ')', '-' and space.
- Click the ***Apply*** button

  A token will be sent to the mobile number and the **Activate Device** page will be displayed.

  Existing devices need to be verified and new devices need to be activated, using the token sent to the cardholder's mobile, which is generated by assigning the device.
- Enter the token received by the cardholder's mobile in **Enter the token sent to your mobile number**.
- Click the ***Apply*** button.

NEW EMAIL DEVICE

- Select **Email** from the **Device type** drop down list.
- Click the ***Apply*** button.

  The **New Email Device** page is displayed.
- Enter the **Email address** of the cardholder.
- Click the ***Apply*** button

  A token will be sent to the email address and the **Activate Device** page will be displayed.

  Existing email addresses need to be verified and new email addresses need to be activated, using the token sent to the cardholder's email address, which is generated by assigning the email address.
- Enter the token received by the cardholder's email address in **Enter the token sent to you by email**.
- Click the ***Apply*** button.

Generate Backup Token

Cards > Card Details > Assigned Devices > Generate Backup Token

When the user's primary authentication device is marked as lost or damaged, you can link from the **User Details > Assigned Devices** page to provide the user with a backup token, which all services can use until a replacement device is received.

- Select the Backup device type:
  - **Default** - supplies a static password that can be used as the second factor of authentication for a limited time and for a limited number of times.
  - **SMS** - displayed only if supported by the issuer device settings. This allows the admin user to temporarily switch the cardholder's authentication process to SMS authentication. The cardholder will need to provide the country calling code and a mobile number to which the second factor of authentication will be sent via SMS. Mobile number should be no longer than 20 characters, including the Country Code. Allowed characters are 0-9, '(', ')', '-' and space.
  - **Email** - displayed only if supported by the issuer's device settings. This allows the admin user to temporarily switch the cardholder's authentication process to Email authentication. The cardholder will need to provide the email address to which the second factor of authentication will be sent via email.

- Click the ***Generate*** button.

  A confirmation message will be displayed.

Show Transactions

Cards > Find Card > Search Result > Card Details > Show Transactions > Show Recent Transactions

Show Transactions allows access to lists of all recent and archived 3-D Secure (payment authentication) or ActiveDevice (two-factor authentication) transactions matching the selected card or user.

<!-- !!! note

```
If the bank supports RuPay PaySecure authentication, a separate administration
interface is available for viewing RuPay Transactions. ---!>
```

The following fields and links are displayed:

Show Archived Transactions - links to the **Archived Transactions** page which displays the archived 3-D Secure (payment authentication) or ActiveDevice (two-factor authentication) transactions matching the selected card or user.

Use the following steps to select a transaction and view its details:

- Click the **Date** (and time) hyperlink for the transaction you wish to view.
- The **Transaction Details** page displays the following fields and links:_
- **Show Recent Transactions** - links to the **Recent Transactions** page which displays the recent 3-D Secure (payment authentication) or ActiveDevice (two-factor authentication) transactions matching the selected card or user.

Use the following steps to select a transaction and view its details:

- Click the **Date** (and time) hyperlink for the transaction you wish to view.

  The **Transaction Details** page is displayed.

New Card

Cards > New Card

You can use the New Card function to manually register cardholders. This function pre-registers cardholders. Cardholders have to finalise their registration by going through the issuer's standard enrolment process.

Creating a new card:

- Select an **Issuer** from the drop down list of available issuers.

  All issuers that your username is assigned to will be listed here.
- **BINs**

  Displays a list of BINs assigned to the issuer. This field is for information purposes. When you enter a new card, the card's BIN number must be one of the existing BINs for the selected issuer.
- Select the **Authentication method** supported by the card
- Currently J/Secure, ProtectBuy, SafeKey, SecureCode and VbV schemes are supported.

> **Note**
>
> Please note that selecting the authentication method alone does not guarantee that the card can be used in the specified authentication scheme. Other pre-arrangements may also be required. For example in Verified by Visa, a card may not be able to participate before a valid card range that entails the card has been sent to the directory service.

- Select the **Status** of **Enabled** or **Disabled** from the drop down list.

  A card is normally enabled when the cardholder is first enrolled. The administration staff for security reasons may temporarily disable a card. A card may also be automatically locked by the system itself if multiple unsuccessful authentication attempts are detected.

  When a card is disabled or locked, it cannot be used to make authenticated payments if cardholder is enrolled or alternatively if cardholder has not enrolled yet, the enrolment process cannot be completed before this situation is resolved.
- Enter the full **Card number**

> **Note**
>
> The card number must comply with the Luhn / mod 10 algorithm.

- Enter the cardholder name as specified on the card as **Name on Card**

- Enter the card **Expiry date** using mm/yyyy format
- Enter information required for any **Extended cardholder information**
- Each card is also associated with one or more authentication or data fields. The issuer determines the format and number of these fields. Extended cardholder information is only displayed if the system administrator enables this option in the Issuer Management section.

  For example, a card may be accompanied by a **PAM** (Personal assurance message or the greeting message as required in VbV, J/Secure, ProtectBuy, SafeKey and SecureCode schemes) or may be associated with a **PIN** (for secure online transactions), etc. Fields such as Internet PIN are always displayed masked.

Find User

Cards > Find User

You can search for users based on the Issuer to which they belong, by specifying the complete username (or user ID). The username is case sensitive.

Use the following field to search for a particular user:

- Select an **Issuer** or **All** from the drop down list
- Enter the user's **Full Name**, which can be partial and case insensitive. Note that full name is not a mandatory field for a user account and may not be populated for all users.
- Select a **Status** - Can be All, Enabled, Disabled, Deleted or Locked.
- If you want to search for current users only, select the **Exclude deleted users from search results** checkbox.
- Click the ***Search*** button.

  The **Search Result** page will be displayed.

User Search Result

Cards > Find User > Search Result

Users matching the search criteria entered on the **Find User** page are listed. You can select any user and delete, enable or disable them.

The search result page shows username, full name, enrolment status and user status.

You can browse to the User Details page by following the **Username** link.

You can select all users by clicking the checkbox in the **Select** column heading. This will select all the items matching your search criteria (i.e. you are not only selecting the items on the current page but all the items on all pages). You can then apply the changes you want to all these items by pressing the corresponding action button.

You should remember that changing the status of items in this manner may take a long time depending on the number items selected. It will also create a huge amount of data in the database as the changes for each single item is saved in the audit log.

Use the following steps to delete, enable or disable a user:

- Choose one or more users by clicking the **Select** checkbox adjacent to the **Username**
- Click the appropriate ***button***.

  A confirmation message will be displayed.

Use the following steps to select a user:

- Click the **Username** hyperlink for the user you wish to view or edit details.

  The **User Details** page is displayed.

Use the following steps to select all items that match the search criteria:

- Click the box in the **Select** column heading to select or unselect all items. This allows you to perform the desired task on all selected items.

  You should note that all items matching the search criteria will be affected. This includes items displayed on other pages and even those omitted due to the large number of results (display of search results is limited to a maximum of 400 records).

⚠ **Warning**

Important: If you are selecting a large number of records, you should remember that the operation can take a long time to complete and will generate an audit log record per affected item. Use this functionality on large number of records with diligence and only where strictly necessary.

User Details

Cards > Find User > Search Result > User Details

This page can be used to view/ update user related information.

The following user details can be viewed/ edited on this page:

- **Issuer** - Shows user's bank and cannot be changed.
- **User ID** - Internal user identifier, which cannot be changed.
- **Status** - Can be **enabled**, **disabled**, **deleted** or **locked**. A user is normally enabled when they are first enrolled. The administration staff for security reasons may temporarily disable a user. A user may also be automatically locked by the system itself if multiple unsuccessful authentication attempts are detected.

  An authentication attempt by a user whose account is disabled or locked is denied.

  Users that are automatically locked can be either unlocked by the administration staff or after a time-out period as specified in the issuer settings. A user may not be manually locked, however.

  Changing the status of a user to 'deleted' simply marks the account for deletion. It does not physically remove the account from the system. An account that has been marked for deletion may be purged when the archive procedure is run. The archive procedure removes these accounts if they fall outside the specified retention period. For example if the data retention policy for your organisation is 12 months, all accounts that have been deleted for 12 or more months are removed by the archive procedure.

  You may undelete an account by simply changing the status of the account to any status other than **Deleted**.
- **Enrolment Status** - Shows the enrolment status, which is either registered or pre-registered, along with the registration or pre-registration date.
- **Username** - User's username or user ID as recognised by the issuer system
- **Full name** - optional full name for the user
- **Password**: An optional password can be specified for the user. This will require the user to enter a static password in addition to their device one-time password. The password should only be used where both the first factor and the second factor of the authentication is being handled by ActiveAccess.

> **Note**
>
> Using this field where the first factor of authentication is handled by the issuer system is not recommended.

- **Email** - optional information for sending notification message to users via email.
- **Assigned Devices** links to the **Search Results** page, which displays all devices attached to this account.
- **Account History** links to **Account History** details page, which shows actions affecting account status or the devices attached to the account
- **Show Transactions** links to the list of transactions performed by the user starting with the most current transactions.
- **Generate Activation Code** link allows the administrator to generate an activation code for a replacement device. The link is only shown if the user's primary device is marked as lost or damaged. The user requires this activation code before then can complete linking the replacement device with an existing account.

New User

Cards > New User

You can use the New User function to manually register users. This function pre-registers users. Users have to finalise their registration by going through the issuer's standard enrolment process.

Creating a new user:

- Select the **Issuer** to which this user belongs from the drop down list of available issuers.
- **Status** - select the initial status of the user.
- **Username** - Enter the user's username or user ID as recognised by the issuer system. The username can be an alphanumeric string up to 128 ASCII characters.
- **Full name** - You can specify an optional full name for the user up to 256 ASCII characters.

Note

The username and full name can contain international characters, which will be stored as UTF-8 encoded strings. The system allows for storage of international characters as long as the UTF-8 encoded equivalent does not exceed the ASCII size limit.

- **Password** - An optional password can be specified for the user. This will require the user to enter a static password in addition to their device one-time password. The password should only be used where both the first factor and the second factor of the authentication is being handled by ActiveAccess.

Note

Using this field where the first factor of authentication is handled by the issuer system is not recommended.

- **Email** - optional information for sending notification messages to users via email.

Transactions

> *The ability to search by 3DS version added.*

System Administrators, **Issuer Administrators**, **Business Administrators**, **Helpdesk Users**

This section is used for accessing 3-D Secure (payment authentication) or ActiveDevice (two-factor authentication) transactions, when required for user support purposes, dispute resolution etc. It has the following menu options:

- **Find 3-D Secure** - to search for and view transactions
- **Find ActiveDevice** - to search for and view devices

> **Info**
>
> It is important to note that in the context of this document, a transaction is an authentication record rather than a financial record. The relationship between the authentication record and the actual authorization record depends on the underlying authentication scheme.

Find 3-D Secure

Transactions > Find 3-D Secure

This page allows you to search for and access 3-D Secure authentication records including the proof of authentication, which can be used for dispute resolution for example.

You can search based on Issuer, Authentication method, Date, Amount, Currency, Account number, Merchant name, Transaction ID and AAV/CAVV (J/Secure, ProtectBuy, SafeKey, SecureCode and VbV) and more.

Use the following fields to search for a 3-D Secure Transaction:

- Select a **Target database** from the list to search for **Current** or **Archived** transactions, if archiving has been configured on the system.
- Select a **3-D Secure version** from the list to search for **All**, **3-D Secure 1** or **3-D Secure 2** transactions ➕
- Specify an **ACS Session ID** to search for a specific transaction.
- Select an **Issuer** (from the list of available issuers) to narrow down the search criteria or you can select **All**. If the Issuer has access to Rules, additional search options will be displayed below.
- Select the **Authentication method** from the drop down list. The options are **J/Secure**, **ProtectBuy**, **SafeKey**, **SecureCode**, **SPA** or **VbV**.
- You can specify an exact **Date** and time or a date and time range (inclusive) in the **From** and **To Date** fields. The date and time format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.

  By default the search is limited to the last 7 days, modify the **From** field if you wish to extend the search period.
- You can specify an exact amount or an amount range (inclusive) in the **From** and **To Amount** fields.
- Select the **Currency** from the drop down list.
- Enter the **Merchant name** in full or in part.
- Enter the full **Merchant ID**.
- Enter the full cardholder **Account number**.
- Enter the **Transaction ID** as specified by the merchant. Transaction ID can be entered in clear or base64 format but you need to the specify the entire Transaction ID (20 character in clear or 28 characters in base64)
- Enter the **AAV/CAVV/AEVV** to find the transaction for which this value was generated.

  AAV (Accountholder Authentication Value) / CAVV (Cardholder Authentication Verification Value) / AEVV (American Express Verification Value) is provided in 3-D Secure PARes for J/ Secure, ProtectBuy, SafeKey, SecureCode and VbV transactions.
- Enter the **Device serial number** to search for transactions that were authenticated using a particular two-factor authentication device.

- Select a **Device type** from the list to search for transactions performed with particular type of authentication device such as SMS or CAP, etc.

3-D Secure version 1 searches only

- Select a **Transaction type** from the list to limit the results to transactions that involved a second factor of authentication (**Device over 3-D Secure 1**) or conventional **3-D Secure 1** transactions.
- Select a **VERes status** from the list to search for transactions with a particular verify enrolment result. The **VERes status** can be:
  - **Y** - Cardholder is enrolled
  - **N** - Cardholder is not enrolled
  - **U** - Cardholder enrolment cannot be determined due to technical or other problems
  - **Error** - An error occurred whilst verifying the enrolment status of the cardholder.
- Select a **PARes status** from the list to search for transactions with a particular payer authentication result. The **PARes status** can be:
  - **Y** - Cardholder authentication successful
  - **A** - Cardholder is not enrolled but proof of authentication attempt provided to the merchant
  - **N** - Cardholder authentication failed
  - **U** - Cardholder authentication cannot be completed due to technical or other problems.
  - **N/A** - Cardholder authentication did not complete.
  - **Error** - An error occurred during cardholder authentication.

> **Note**
>
> Use PARes and VERes filters only if you are searching for 3-D Secure records, version 1.0.1 and above.

- Select the transaction **Status** from the list. The transactions can either be **In progress** or **Processed**. An **In progress** status indicates that either the cardholder has not yet finished the authentication process or the system has not yet sent the PATransReq message to the authentication history server. When you choose to search for all transactions regardless of their status, the system will first return all **In progress** transactions followed by **Processed** transactions. Please note that only the first 400 records are returned in total.
- Enter an **Error code/IReq code** to search for in the authentication response message.

- Enter an **Error message/IReq message** to search for in the authentication response message.

3-D Secure version 2 searches only

- Enter an **SDK transaction ID**
- Enter a **DS transaction ID**
- Enter an **3DS Server transaction ID**
- Select an **ARes status** from the list to search for transactions with a particular authentication response. The **ARes status** can be:
    - **Y** - **Authentication / account verification successful**
    - **N** - **Not Authenticated / account not verified** - transaction denied
    - **U** - **Authentication / account verification could not be performed** - technical or other problem, as indicated in ARes or RReq
    - **A** - **Attempts processing performed** - not authenticated / verified but a proof of attempted authentication/verification is provided
    - **C** - **Challenge required** - additional authentication is required using the CReq/CRes
    - **R** - **Authentication / account verification rejected** - Issuer is rejecting authentication / verification and requests that authorisation not be attempted.
- Select a **CRes status** from the list to search for transactions with a particular challenge response. The **CRes status** can be:
    - **Y** - **Authentication / account verification successful**
    - **N** - **Not Authenticated / account not verified** - transaction denied
- Select an **RReq status** from the list to search for transactions with a particular results request. The **RReq status** can be:
    - **Y** - **Authentication / account verification successful**
    - **N** - **Not Authenticated / account not verified** - transaction denied
    - **U** - **Authentication / account verification could not be performed** - technical or other problem, as indicated in ARes or RReq
    - **A** - **Attempts processing performed** - not authenticated / verified but a proof of attempted authentication/verification is provided
    - **C** - **Challenge required** - additional authentication is required using the CReq/CRes

  - **R** - **Authentication / account verification rejected** - Issuer is rejecting authentication / verification and requests that authorisation not be attempted.
- Select a **Message cateory** from the list to search for **All**, **Payment authentication** or **Non payment authentication** transactions.
- Select an **Authentication type** from the list to search for **All**, **Static**, **Dynamic** or **OOB** transactions.
- Select an **Device channel** from the list to search for **App based**, **Browser** or **3DS Requester Initiated** transactions.

Rules - displayed if specified Issuer has access to Rules. Where an issuer with **Rules** enabled is selected, additional fields will be available so that you can search for transactions by whether they match or do not match one or more rules.

- Select one of the following radio buttons:
  - **All** - all transactions, regardless of rules
  - **Matched** - transactions that match the rules selected from the adjacent list
  - **Mismatched** - transactions that do not match the rules selected from the adjacent list
- Select one or more **Rules** (Ctrl +click to select multiple rules) from the list:
  - **Amount Threshold**
  - **Domestic & International Transaction Threshold**
  - **Location Watchlist**
  - **Merchant Blacklist**
  - **Merchant Watchlist**
  - **Merchant Whitelist**
  - **Soft Launch List**
  - **Stand-In Transaction Threshold**
- If you have selected the **Matched** radio button, you can enter an **Error code** or **Error message** to search on.
- If you have selected merchant or location list rules, you can enter additional search parameters:
  - **Merchant ID**
  - **Merchant name**

  - **Acquirer BIN**
  - **Merchant country code**
- The **Registered after previous opt-outs or cancellations** option provides a way of searching for and listing transactions where cardholders have completed their registration after initially opting out or cancelling activation during shopping.
- Click **Search** to display the **Transaction Search Results**.

Transaction Search Results

Transactions > Find Transaction > Search Result

The search result page lists transactions matching the criteria you entered on the **Find Transaction** page and shows transaction date, amount, currency, account number, merchant name, issuer, method, status and transaction type.

Only the first six and the last four digits of the account number are shown. An **X** masks the rest of the digits. You can choose to display card number in plain text in Settings.

You can browse to the transaction details page by following the link under **Account Number**.

Use the following steps to select a transaction and view its details:

- Click the **Date** (and time) hyperlink for the transaction you wish to view.

  The **Transaction Details** page is displayed.

Transaction Details

Transactions > Find Transaction > Search Result > Transaction Details

This page shows the details for the Transaction selected on the Transaction Search Result page.

The following fields can be viewed on this page:

- **Issuer** - Shows the card's issuing bank.
- **Authentication method** - Shows the authentication method relevant to this transaction. The options are: J/Secure, ProtectBuy, SafeKey. SecureCode, or Verified by Visa.
- Relevant 3DS1 or 3DS2 **Status** (as described above in the search criteria)
- **Date** - Shows the date and time of the transaction.

- **SDK transaction ID**
- **DS transaction ID**
- **3DS Server transaction ID**
- **ARes status** - Authentication Result status.
- **ARes status reason** - Authentication Result reason.
- **CRes status** - Challenge Result status.
- **RReq status** - Results Request status.
- **Device channel** - Shows the device channel as App based, Browser or 3DS Requester Initiated.
- **Message category** - Shows the message category as Payment authentication or Non payment authentication.
- **Authentication type** - Shows the authentication type as Static, Dynamic or OOB.
- **Amount** - Shows the transaction amount, including the currency.
- **Account number** - Shows the last five digits of the account number, which is used in this transaction. Links to the **Card Details** page.
- **Merchant name** - Shows the merchant name.
- **Merchant ID** - (J/Secure, ProtectBuy, SafeKey, SecureCode and VbV) Acquirer-defined merchant identifier, up to 24 characters including the Card Acceptor ID and Card Acceptor Terminal ID.
- **Transaction ID** - Transaction ID as specified by the merchant (XID for J/Secure, ProtectBuy, SafeKey, SecureCode and VbV)
- **AAV/CAVV/AEVV** - Accountholder Authentication Value / Cardholder Authentication Verification Value / American Express Verification Value for J/Secure, ProtectBuy, SafeKey, SecureCode and VbV authentication.
- **Device serial number** - The unique identifier of the authentication device used in the transaction for two-factor authentication, if available.
- **Device type** - The type of authentication device used in the transaction for two-factor authentication, if available.
- **Transaction type** - 3-D Secure 1, Device over 3-D Secure 1, or 3-D Secure 2, depending on whether the transaction was a conventional password-based 3-D Secure 1 authentication, a two-factor authentication or a 3-D Secure 2 authentication.

- **Error code** - 0 if the authentication request was successfully completed. Any other value indicates an error condition.
- **Error text** - A descriptive message for the response code.
- **Error detail** - Detailed information for the error condition.
- **Matched rules** - Displays the rules against which the transaction matched, with links to the details of the rule at the time of the transaction.

  Where a transaction has matched the merchant blacklist rule, the Matched Rule Details display the matched rule highlighted in red.
- Click on the **Requests and Responses** link to see the details of 3-D Secure 1 messages (VEReq, VERes, PAReq, PARes, PATransReq, PATransRes) or 3-D Secure 2 messages (AReq, ARes, CReq, CRes, RReq, RRes).

> **Note**
>
> Refer to "3-D Secure Protocol Specification Core Functions" or "EMV® 3-D Secure Protocol and Core Functions Specification" documentation available from the Visa International or EMVCo website.

Find ActiveDevice

Transactions > Find ActiveDevice

Use this page in order to find ActiveDevice transactions and access the details of two-factor authentication records.

Use the following fields to search for an ActiveDevice Transaction:

- Select a **Target database** from the list to search for **Current** or **Archived** transactions.
- You must select an Issuer but you can leave the rest of the fields at default or blank to display a list of all available ActiveDevices. Select an **Issuer** (from the list of available issuers) to narrow the search criteria or you can select **All**.
- You can specify an exact date and time or a date and time range (inclusive) in the **From** and **To Date** fields. The date and time format is dd/mm/yyyy HH:MM. Leave the time field empty if you do not wish to limit your search for a particular time of day.

> **Note**
>
> By default the search is limited to the last 7 days, modify the **From** field if you wish to extend the search period.

- Enter a full **Username** to limit the search results to a particular user.
- Enter the **Device serial number** to search for transactions performed with the specified device.
- Select a **Device type** from the list to limit the search to transactions performed with a particular device.
- Select a **UERes status** from the list to search for transactions with a particular user enrolment result. The options are:
  - **All**
  - **Y** - User is enrolled
  - **R** - User is pre-registered
  - **N** - User is not enrolled
  - **E** - Error
  - **U** - User enrolment cannot be determined due to technical or other problems.
- Select a **UARes status** from the list to search for transactions with a particular user authentication result. The options are:
  - **Y** - User authentication successful
  - **N** - User authentication failed
  - **E** - Error

ActiveDevice Search Results

Transactions > Find ActiveDevice > Search Result

The search result page lists ActiveDevice transactions matching the criteria you entered on the **Find ActiveDevice** page and shows transaction date, username, device serial number, issuer, device type and status.

You can browse to the transaction details page by following the link under *Date*.

Use the following steps to select an ActiveDevice transaction and view its details:

- Click the *Date* hyperlink for the transaction you wish to view.

  The **ActiveDevice Details** page is displayed.

ActiveDevice Details

Transactions > Find ActiveDevice > Search Result > ActiveDevice Details

This page shows the details for the ActiveDevice transaction selected on the ActiveDevice Search Result page.

The following fields can be viewed on this page:

- Unique **Session ID**
- User's **Issuer**
- **Date** and time of the transaction
- **UERes status** - can be:

  Y - User is enrolled

  N - User is not enrolled

  R - User is pre-registered

  U - User enrolment cannot be determined due to technical or other problems.
- **UARes status** - can be:

  Y - User authentication successful

  N - User authentication failed

  U - User authentication cannot be completed due to technical or other problems
- User's login **Username**, which links to the **User Details** page
- **Serial number** of the authentication device used in the transaction.
- **Device type** of the token used for authentication
- **Response code**

  0 if the authentication request was successfully completed. Any other value indicates an error condition.
- **Response text**

A descriptive message for the response code.

- **Response detail**

  Detailed information for the error condition.

- Click on the **Requests and Responses** link to see the details of ActiveDevice protocol messages.

Reporting

System Administrators, Issuer Administrators, Business Administrators

This section provides various reports for cardholder and user activity, authentication, card and user enrolment and purchase volume.

Reports can be run for all issuers or any number of issuers or issuer groups. All reports except for the Summary return the total for all selected issuers. The Summary report returns the total and also breaks the report down based on the selected issuers.

Warning

A default time zone is set when the application is installed. This Time zone is displayed, for reference, on the menu bar, from where it can be modified at any time, as and when appropriate. The modification of the Time zone on the menu bar does not change the Time zone for the Issuer.

Note

If you modify the Time zone in the menu bar it will persist for the current session only. It will revert to the Time zone entered in the Issuer settings, the next time you login.

All search parameters for transactions, audit logs and reports (daily, monthly and annual) will be based on the Time zone specified on the menu bar at the time of the search.

IMPORTANT: If the time zone is changed in **Issuers > Settings**, it will impact the data displayed for issuer reports (daily, monthly and annual). When attempting to change the time zone, a warning message is displayed with the following options:

- **Continue and delete report** data - reports will not be available for the selected issuer until the next overnight report run, which will use the new time zone.

> **Note**
>
> If auto archive is enabled, archived data will no longer be collected and previous report data will be lost.

- **Continue and keep report data** - existing report data will be inaccurate due to the time change. Accurate reports will not be available until the next overnight report run, which will use the new time zone.
- **Cancel** - time zone will not be changed.

Reports *section has the following sub menu options:*

- **Card Summary** based reports: authentication attempts, successful authentications, number of enrolled, registered and existing cards and card activity broken down by 3-D Secure provider and selected issuers and issuer groups.
- **User Summary** based reports: authentication attempts, successful authentications, number of enrolled, registered and existing users and user activity.
- **Activity** based reports - remaining cards, active cards, and authentication method for selected issuers/ issuer groups and time period.
- **Authentication** based reports - Statistics on authentications broken down by the status of associated authentication messages for a given issuer and time period.
- **Enrolment Activity** based reports - enrolled cards, pre-registered cards, cancelled cards and authentication method for a given period.
- **Merchant Activity** based reports - total authentications, authentication status, and authentication method per merchant.
- **Purchases** based reports - purchase volumes, authentication method, and currency type for a given period.
- **User Authentication** reports - Statistics on device authentication attempts broken down by the status of associated authentication messages for a given issuer and time period.
- **User Activity** based reports - remaining users, active users, for ActiveDevice authentications for a given issuer and time period.
- **User Enrolment Activity** based reports - enrolled users, pre-registered users, cancelled users and authentication method for a given period.
- **Admin** based reports - number of administrators, broken down by user access type and selected issuers and issuer groups.

The first **Reports** page is **Card Summary**.

Card Summary Report

Reports > Card Summary

The summary report provides an overview of some the more important metrics of the system, including: the number of authentications, successful authentications, number of enrolled, registered and existing cards in the system and card activity. The report is broken down by 3-D Secure provider and can be customised to include one or more issuers or issuer groups. The report can be generated for a specified period of time.

Use the following fields to produce a card summary report:

- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select at least one **Authentication method**, by selecting/deselecting the appropriate checkboxes. All methods are selected by default with the report displaying values against only the selected methods.
- Select which issuers to run the report for; **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add >>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**

> ⚠ **Warning**
>
> Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- **Extend report by device type** by selecting the checkbox. If selected, at least one device should be selected to run the report.
- **3-D Secure Version** by selecting the **3DS1** and / or **3DS2** checkboxes, as appropriate.
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

The following are displayed for the Period specified:

- Date range of report
- Names of the issuer groups / issuers selected or 'for all issuers' if the **All Issuers** checkbox was selected
- Issuer
- Total for Issuers selected

Authentication

- Number of VbV authentication attempts
- Number of SC authentication attempts
- Number of J/S authentication attempts
- Number of SK authentication attempts
- Number of DC authentication attempts
- ***Number of Total number of authentication attempts***
- Number of Successful VbV authentications
- Number of Successful SC authentications
- Number of Successful J/S authentications
- Number of Successful SK authentications
- Number of Successful DC authentications
- ***Total number of successful authentications***

Note

If **Extend by device type** selected, the above are displayed for each device loaded in the system, for example:

- Backup token
- VASCO
- RSA
- SMS
- Email
- CAP (M-Chip 4)
- CAP (M-Chip 2)

Enrolment

- Number of pre-registered cards
- Number of fully registered cards
- ***Total number of cards enrolled***

Card Activity

- Number of active VBV cards
- Number of active SecureCode cards
- Number of active J/Secure cards
- Number of active SafeKey cards
- Number of Active ProtectBuy cards
- ***Total Number of active cards***

User Summary Report

Reports > User Summary

The user summary report provides an overview of some the more important metrics of the system, including: the number of authentications, successful authentications, number of enrolled, registered and existing users in the system and user activity. The report is broken down by device type and can be customised to include one or more issuers or issuer groups. The report can be generated for a specified period of time.

Use the following fields to produce a user summary report:

- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups**.

⚠ **Warning**

Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- Select at least one **Device** to run the report for.
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

The following are displayed for the Period specified:

- Date range of report
- Names of the issuer groups / issuers selected or 'for all issuers' if the **All Issuers** checkbox was selected
- Issuer
- Total for Issuers selected

Authentication

- VASCO authentication attempts
- SMS authentication attempts
- RSA authentication attempts
- Email authentication attempts
- CAP (M-Chip 4) authentication attempts
- CAP (M-Chip 2) authentication attempts
- Backup device authentication attempts
- ***Total number of authentication attempts***
- Successful VASCO authentications
- Successful SMS authentications
- Successful RSA authentications
- Successful Email authentications
- Successful CAP (M-Chip 4) authentications

- Successful CAP (M-Chip 2) authentications
- Successful backup device authentications
- ***Total number of successful authentications***

User Enrolment:

- Pre-registered users
- Fully registered users
- Total number of users

Device Enrolment:

- VASCO
- SMS
- RSA
- Email
- CAP (M-Chip 4)
- CAP (M-Chip 2)
- Backup
- ***Total number of devices***

User Activity:

- ***Total number of active users***

Activity Report

Reports > Activity

The activity report shows the total number of enrolled cards and active cards for a given period for all or selected issuers and/or issuer groups.

The report is also broken down by the authentication method. A card is said to be active in a given period if the cardholder has at least performed one successful authentication with the card in the specified period.

The default report shows monthly cardholder activity for the current year for all issuers. You may select any number of issuers or issuer groups; daily, monthly or annual report period; and specify a date range.

Use the following fields to produce an activity report:

- Select **Monthly**, **Daily** or **Annual Period** from the drop down list.
- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select at least one **Authentication method**, by selecting/deselecting the appropriate checkboxes. All methods are selected by default with the report displaying values against only the selected methods.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**

⚠ **Warning**

Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- Click the ***Go*** button to display the report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

Authentication Report

Reports > Authentication

This reports shows authentication statistics for a given period based on the status codes returned by **VERes** and **PARes** messages for **3DS1** and **AuthRes** messages for **3DS2**.

3DS1 statistics

The status code for **VERes** messages can be **Y** for 'enrolled users'**, N** for 'not enrolled users' or **U** for 'unable to determine the enrolment status of the user due to some technical difficulty'.

The report calculates **ER** (enrolment rate) as: (VERes=Y) / (VERes=Y+N+U)

The status code for **PARes** messages can be **Y** for 'successful authentication'**, N** for 'failed authentication', **A** for 'authentication attempt' or **U** for 'unable to authenticate the user due to some technical difficulty'.

The report calculates **AR** (authentication rate) as: (PARes=Y) / (PARes=Y+A+N+U)

3DS2 statistics

The status code for **ARes** and **CRes** messages can be **Y** for 'enrolled users'**, N** for 'not enrolled users' or **U** for 'unable to determine the enrolment status of the user due to some technical difficulty'.

The report calculates **AR** (authentication rate) as (ARes=Y+CRes=Y) / (ARes=Y+A+N+U+R+C)

The default report shows monthly authentication statistics for the current year for all issuers. You may select any number of issuers or issuer groups; a different daily, monthly or annual report period; and specify a date range.

Use the following fields to produce an authentication report:

- Select **Monthly**, **Daily** or **Annual Period** from the drop down list.
- Enter a date range in the **From** and **To** dates (mm/yyyy). Defaults are: **From: 01/** and **To: 12/**.
- Select at least one **Authentication method**, by selecting/deselecting the appropriate checkboxes. All methods are selected by default with the report displaying values against only the selected methods.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups**.

Warning

Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- **Extend report by device type** by selecting the checkbox. If selected, at least one device should be selected to run the report.

- **3-D Secure Version** by selecting the **3DS1** and / or **3DS2** checkboxes, as appropriate.
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

Enrolment Activity

Reports > Enrolment Activity

The enrolment report shows the total number of enrolled, pre-registered and cancelled cards for a given period. The report is also broken down by the authentication method.

The default report shows monthly card enrolments for the current year for all issuers. You may select any number of issuers and/or issuer groups, a different daily, monthly or annual report; and specify a period.

The **Enrolled Cards** column shows the total number of cards enrolled (fully registered) in the selected period. Some of these cards may have been cancelled, which appear in the **Cancelled Cards** column. The difference between Enrolled Cards and Cancelled cards is the number of enrolled cards remaining.

The **Pre-registered** cards column shows the number of cards, which have been pre-enrolled by the banks for those cardholders who have not yet finalised their registration. Some of these cards may be cancelled before the cardholder has finalised their enrolment. Currently the system does not log this event and the statistics for cancelled pre-registered cards is not available.

Use the following fields to produce an enrolment report:

- Select **Monthly**, **Daily** or **Annual Period** from the drop down list.
- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/** and **To: 12/**.
- Select at least one **Provider**, by selecting/deselecting the appropriate checkboxes. All providers are selected by default with the report displaying values against only the selected Providers.

- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**

> ⚠ **Warning**
>
> Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

Merchant Activity

Reports > Merchant Activity

The merchant activity report shows the total number of authentications initiated by top merchants for a given period. The report is also broken down by the authentication method and successful and failed authentications.

By default, the report shows top 10 merchants' activity for the current year based on total authentication requests send by the merchant. You may select a different period or view top 20 or 50 merchants instead. You may also select the report to be generated and sorted based on the authentication scheme or the number of successful and failed authentications.

Use the following fields to produce a merchant activity report:

- Select Top 10 Merchants (default), Top 20 Merchants or Top 50 Merchants from the **Show** drop down list
- Select the authentication type from the **Based on** drop down list. Defaults to **Total Authentications**.
- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select at least one **Authentication method**, by selecting/deselecting the appropriate checkboxes. All methods are selected by default with the report displaying values against only the selected methods.

- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups**.

⚠ **Warning**

Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- **Extend report by device type** by selecting the checkbox. If selected, at least one device should be selected to run the report.
- **3-D Secure Version** by selecting the **3DS1** and / or **3DS2** checkboxes, as appropriate.
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

Purchases Report

Reports > Purchases

The purchase report shows the total purchase volume for a given period. The report is also broken down by the authentication method. The purchase volume is divided based on the purchase currency.

The report shows monthly purchase volume for the current year by default. You may select a different daily, monthly or annual report and specify a period or choose a currency for the report.

✎ **Note**

Please note that authentication requests display the currency in which the transaction will be cleared by the merchant and do not specify any international exchange rates involved in the authorization process. As such the purchase report may have to be specified in multiple currencies.

Use the following fields to produce a purchases report:

- Select a **Currency** or **All** from the drop down list
- Select **Monthly**, **Daily** or **Annual Period** from the drop down list

- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select at least one **Authentication method**, by selecting/deselecting the appropriate checkboxes. All methods are selected by default with the report displaying values against only the selected methods.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add >>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups**.

> ⚠ **Warning**
>
> Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- **Extend report by device type** by selecting the checkbox. If selected, at least one device should be selected to run the report.
- **3-D Secure Version** by selecting the **3DS1** and / or **3DS2** checkboxes, as appropriate.
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

The following are displayed by the Period specified:

- Period - days, months or years
- Names of the issuer groups / issuers selected or 'for all issuers' if the **All Issuers** checkbox was selected
- Number of Transactions
- ***Total Amount for transactions by transaction currency***
- SecureCode Transactions
- SecureCode Total
- VbV Transactions
- VbV Total
- JCB J/Secure Transactions
- J/Secure Total

- American Express SafeKey Transactions
- SafeKey Total
- Diners Club International ProtectBuy Transactions
- ProtectBuy Total

User Authentication Report

Reports > User Authentication Report

This reports shows device authentication statistics for a given period.

This reports shows authentication statistics for a given period based on the status codes returned by UERes and UARes messages.

Status code for UERes messages:

Y - **enrolled users N** - **not enrolled users E** - **Error N** - **not enrolled users R** - **pre-registered users U** - **unable to determine the enrolment status of the user due to some technical difficulty**.

The report calculates **ER** (enrolment rate) as: UERes=Y+R/UERes=Y+R+N+U

The status code for UARes messages can be **Y** for 'successful authentication'**, N** for 'failed authentication', **A** for 'authentication attempt' or **U** for 'unable to authenticate the user due to some technical difficulty'.

The report calculates **AR** (authentication rate) as: UARes=Y/UARes=Y+N

The default report shows monthly authentication statistics for the current year. You may select a different daily, monthly or annual report period and specify a date range.

Use the following fields to produce a device authentication report:

- Select **Monthly**, **Daily** or **Annual Period** from the drop down list
- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**

⚠ **Warning**

Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- Select a **Device** to run the report for (optional).
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

User Activity Report

Reports > User Activity

This reports shows device authentication activity statistics for a given period for a specified issuer.

The default report shows device authentication activity for the current year. You may select a different issuer, daily, monthly or annual report period and specify a date range.

Use the following fields to produce an ActiveDevice activity report:

- Select **Monthly**, **Daily** or **Annual Period** from the drop down list
- Enter a date range in the **From** and **To** dates (mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**

⚠ **Warning**

Run the report for **All Issuers** with caution as it may take a significant time to produce the report.

- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.

- Click the ***Back*** button to modify the search criteria.

User Enrolment Activity Report

Reports > User Enrolment Activity

This report shows ActiveDevice user enrolment statistics for a given period.

The default report shows monthly user enrolments for the current year. You may select a different daily, monthly or annual report and specify a period.

The **Enrolled Users** column shows the total number of users enrolled in the selected period. Some of these users may have been cancelled, which appear in the **Cancelled Users** column. The difference between enrolled users and cancelled users is the number of enrolled users remaining.

The **Pre-registered Users** column shows the number of users, which have been pre-enrolled by the banks but have not yet finalised their registration. Some of these users may be cancelled before they have finalised their enrolment. Currently the system does not log this event and the statistics for cancelled pre-registered users is not available.

Use the following fields to produce an enrolment report:

- Select **Monthly**, **Daily** or **Annual Period** from the drop down list
- Enter a date range in the **From** and **To** dates (dd/mm/yyyy). Defaults are: **From: 01/01/** and **To: 31/12/**.
- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**
- Click the ***Go*** button to display the new report.
- Click the ***Export*** button in order to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the ***Back*** button to modify the search criteria.

Admin Report

Reports > Admin

This report provides a summary of administrative user accounts by issuer. The report is broken down by user access type and can be customised to include one or more issuers or issuer groups.

Use the following fields to produce an admin report:

- Select which issuers to run the report for. **All Issuers** is selected by default. To run the report for one or more Issuer Groups and/or Issuers, deselect the **All Issuers** checkbox and use the **Add>>**, **<<Remove** buttons to select **Issuers** or **Issuer Groups.**
- Click the ***Go*** button to display the new report.

The admin report is broken down into three sections: summary, admin users per issuer and admin users per group. Summary shows the total number of admin users across the system based on their access type and available to system users only. Issuer and group based reported show admin users per issuer and group, respectively.

- Click the **Export** link to export the currently displayed report as a Comma Separated Value (CSV) file.
- Click the **Back** link to modify the search criteria.

Audit Log

System Administrators, Issuer Administrators, IT Security Administrators

This section is used for keeping a record of all critical actions performed by administrative users. It has the follow menu options:

Find Audit Log

This section is used to locate and view audit logs. You can search for an audit log by Date Range, Username, User ID, Issuer or Issuer Group, Access type, Event type and Table.

Audit Log > Find Audit Log

Use the following field to search for an audit log:

You can leave all fields at default or blank to display a list of all logs.

- Select a **Target database** from the list to search for **Current** or **Archived** audit logs.
- Enter a date range in dd/mm/yyyy format in the **From** and **To** fields.
- Enter all or part of the **Username**
- Enter a **User ID**, which is a unique ID assigned to each user when first created. Unlike username, user ID remains unchanged and can be used to identify a user, in case the username has changed.
- **Access type** defaults to **All.** Deselect the **Access type** checkbox to select from the drop down list. Select multiple Access types using Ctrl+click.
- When **Access Type** is set to **Event** or **All**, **Event type** defaults to All. Deselect the **Event type** checkbox to select from the drop down list. Select multiple Event types using Ctrl+click.
- For all Access types, other than **Event**, you can optionally select a database **Table** which limits the results to actions performed on the selected table.

Tables defaults to **All.** Deselect the **Tables** checkbox to select from the **Available** list and then click the **Add>>** button to transfer the **Table** to the **Selected** list. Select multiple Tables using Ctrl+click.

- ***Search*** button to display results.

Search Result

This page displays logs matching your search criteria.

Use the *No* or *Date* links to view details for a log.

Audit Log > Find Audit Log > Search Result

Fields & links displayed on this page:

- **No** - records are numbered for reference purposes only for each search performed - this field links to **Audit Log Details** page for selected record
- **Date** link to **Audit Log Details** page for selected record.
- **Time** log was recorded
- Database **Table** accessed
- Type of **Access** - Event, Update, Insert or Delete
- **Username**
- **Issuer**
- **Group**

Log Details

This page displays full details for the audit log record selected on the **Search Result** page.

Audit Log > Find Audit Log > Search Result > Log Details

Fields displayed on this page:

- **Access ID**
- **Access date**
- **Username**
- **User ID**

- **Type of access**
- **Description**
- **Client IP**
- **Object name**
- **Issuer**
- **Group**

Fields displayed for the database table changed:

- **Field**
- **Old Value**
- **New Value**

Profile Management

> **All Admin Users** can edit their profile and change their password.

It is recommended that you change your password on a regular basis for security reasons or if you suspect that security has been compromised by another user logging in with your username and password.

The Change Password function is accessed via the **Edit Profile** link displayed on the right of the title bar area. You can also use this link to keep your contact details up to date.

- Click the Edit Profile hyperlink

  The **Edit Profile** page is displayed.

Edit Profile

Use the following fields to change your details or password:

- The **Username** of the user currently logged on is displayed and cannot be changed.
- User Details
- Enter your **Full name**.
- You must enter a valid **email address**
- Enter your **Contact number**.
- Enter your **Address**.

  Password Details
- Enter your current password as **Old password**.
- Enter the **New Password** you have chosen.

Warning

Always choose a password that you have not used for the Administration Server previously. The Administration System keeps a history of the last 10 passwords and does not allow you to reuse passwords in the history. For example, you cannot keep two favourite passwords and rotate them. If you try to reuse a password stored in the history a message is displayed: **This password has been selected before**.

- Re-enter your new password as **Re-enter Password**.
- **Two-factor authentication login** checkbox

  Select this checkbox if you want to enable two-factor authentication when logging in.

Note

After clicking **Apply**, a **Secret key** and a **QR code** will be displayed, to be used with Google Authenticator. For more information, refer to Login.

- Click the **Apply** button to save your details.

Error Codes

Server Error Codes

Server Error Codes			
Code	**Message**	**Details**	**Usage**
1	Root element invalid.	Exception message and its cause FourDSecure ThreeDSecure	Yes
2	Message element not a defined message.	Exception message and its cause VVRQ PPRQ Undefined CRReq	Yes
3	Required element missing.	PaReq TermUrl MD Id | VEReq.Extension.Id | PAReq.Extension id VEReq.version | version | PAReq.version Pan | VEReq.Pan PAReq.Merchant.name | name PAReq.Merchant.country | country PAReq.Merchant.url | url PAReq.Purchase.xid | xid PAReq.Purchase.date | date PAReq.Purchase.amount | amount PAReq.Purchase.purchAmount | purchAmount PAReq.Purchase.currency | currency PAReq.Purchase.exponent | exponent PAReq.CH.acctID | acctID PAReq.CH.expiry | expiry Message.Id | Id Message	Yes
4	Critical element not recognized.	Extension | VEReq.Extension | PAReq.Extension	Yes

Server Error Codes			
5	Format of one or more elements is invalid according to the specification.	Exception message and its cause version | VEReq.Version | PAReq.Version Pan | VEReq.Pan VEReq.Extension.Id | Extension.Id VEReq.Browser.deviceCategory | devicCategory Extension.Critical PAReq.Merchant.name | name | Merchant.name PAReq.Merchant.country | country | Merchant.country PAReq.Purchase.xid | xid | Purchase.xid PAReq.Purchase.date | date | Purchase.date PAReq.Purchase.amount | amount | Purchase.amount PAReq.Purchase.purchAmount | purchAmount | Purchase.purchAmount PAReq.Purchase.currency | currency | Purchase.currency PAReq.Purchase.exponent | exponent | Purchase.exponent PAReq.Purchase.desc | desc | Purchase.desc PAReq.Purchase.Recur.frequency | frequency | Recur.frequency PAReq.Purchase.Recur.endRecur | endRecur | Purchase.Recur.endRecur PAReq.Purchase.install | install | .Purchase.install PAReq.CH.acctID | acctId | CH.acctID PAReq.CH.expiry | expiry | CH.expiry Message.Id | Id Merchant Merchant.merID	Yes
6	Protocol version too old.	Protocol version too old. Protocol version is not supported by ProtectBuy.	Yes
98	Transient system failure.	Contact your vendor with this 'ACS Session ID': %sessionId%	Yes
99	Permanent system failure.	%s	No

Server Error Codes			
1001	Invalid http request	Invalid HTTP request: PAHndler.run() Invalid HTTP request:	Yes
1002	Process timed out	Process timed out	Yes
1003	Invalid xml request	Invalid XML request process.	No
1004	Error in ThreeDS.service(): %s	Error in ThreeDS.service(): %s	No
1005	Permission denied	Permission denied	Yes
1006	An extension is not currently associated with this request	An extension is not currently associated with this request	Yes
1007	ACS failed to start successfully.	ACS failed to start successfully	Yes
1008	Error in inflating PAReq	Error in inflating PAReq ver 1.0.1	Yes
1009	Error in deflating PARes	Error in deflating PARes ver 1.0.1	No
1010	This session is invalid. Please try again.	This session is invalid. Please try again.	Yes
1011	Your session has now expired. Please try again.	Your session has expired. Please try again.	Yes
1012	Internal error: Unable to save session.	Internal error: Unable to save session.	No
1013	Invalid authentication result in ThreeDS.service(): %s	Invalid authentication result in ThreeDS.service(): %s	No
1014	'%s' request length is too large	'HTTP' request length is too large 'XML' request length is too large	Yes
1015	Invalid cardholder name for PARes 10X in ThreeDS.service()	Invalid cardholder name for PARes 10X in ThreeDS.service()	No

Server Error Codes			
1016	The process has been successfully completed. One or more required parameters were not specified.	The process has been successfully completed. One or more required parameters were not specified.	Yes
1017	Cannot find any authentication data.	Authentication data not found.	Yes
1018	Issuer's BIN does not support device authentication over 3-D Secure.	This issuer BIN range does not support device authentication for 3-D Secure.	No
1019	Issuer does not support any devices.	Issuer does not support any devices.	Yes
1020	Invalid request.	ACS records show the card type is MasterCard but the request was received as on Visa VE server. ACS records show the card type Visa but the request was received as on MasterCard VE server. ...	Yes
1021	There is no assigned device.	There is no device assigned.	Yes
1022	Different card types.	Cards belong to different card schemes.	Yes
1023	Invalid character	There is an invalid character in parameter (%s)	No
1024	Invalid card in authentication process	Card is pre-registered and cannot be used in the authentication process.	Yes
1025	Illegal process	Illegal process 'Authorization'	Yes
1026	Server is in reinitializing state	Server is in reinitializing state.	Yes
1027	Invalid authentication URL	'Url' is invalid	Yes
1028	Cannot find all the required parameters for PA processing	Cannot find all the required parameters for PA processing 'URI'.	Yes

Server Error Codes			
1029	Page and process do not match	The 'page name' page cannot be displayed while in the duplicate cardholder process.	Yes
1030	Invalid parameter value		No
1031	Email Device Param not initialized		Yes

User Error Codes

User Error Codes			
Code	**Message**	**Details**	**Usage**
1	Root element invalid.	Device	Yes
2	Message element not a defined message.	Name of undefined element	Yes
3	Required element missing.	Name of missing element	Yes
4	Critical element not recognized.	Extension	Yes
5	Format of one or more elements is invalid according to the specification.	Name of invalid element	Yes
50	Issuer %s does not participate in device authentication.	%s	Yes
55	Transaction data not valid.	%s	Yes
56	Signature verification failed.	%S	Yes
70	Invalid request	%S	Yes
71	Session is invalid.	%S	Yes

User Error Codes			
72	Session is expired.	%S	Yes
98	Transient system failure	%S	Yes
99	Permanent system failure.	%S	Yes
1001	Invalid HTTP request	Invalid request	No
1002	Process timed out	Process timed out	No
1003	Invalid XML request	Invalid XML request	No
1004		%s does not exist or has an incorrect format	No
1005	Permission denied	Permission denied	No
1006	An extension is not currently associated with this request	An extension is not currently associated with this request	No
1007	Server has not started correctly	Server has not started correctly	No
1008		Error in serializing the %s XML Document	No
1009		Session '%s' has expired	No
1010	Invalid request length	'%s' request length is too large	No
1011		The process has been successfully completed. One or more required parameters were not specified	No
1012		Error in inflating UAReq ver 1.0.1	No
1013		Error in deflating UARes ver 1.0.1	No
2001	User not registered		No

User Error Codes			
2002	User is locked		Yes
2003	Action cancelled		Yes
2004	User is disabled		Yes
2005	Maximum number of transactions exceeded		Yes
2010	Device not registered		Yes
2011	Cannot find any active devices		Yes
2012	Device type is not supported. Type = %s		Yes
2013	Invalid device extension, %s		Yes
2014	Invalid token		Yes
2015	Invalid password		Yes
2016	One-way authentication is not supported for device type %s		Yes
2017	Maximum number of SMS resend request exceeded		Yes
2050	Issuer %s does not participate in device authentication		Yes
2051	License key does not allow for device authentication, %s		Yes
2052	Invalid password for issuer %s		Yes
2053	Device type %s is not supported for issuer %s		Yes

User Error Codes			
2054	The interface is disabled for issuer %s		Yes
2055	Device type %s is not supported by the device owner (issuer: %s)		Yes
2056	The process has been successfully completed. One or more required parameters were not specified.		Yes
2057	Duplicate UAReq not allowed		Yes

Account Error Messages

Account Error Messages		
Code	**Message**	**Usage**
101	Please re-enter the field(s) highlighted in red	Yes
102	Required field missing	Yes
103	Invalid number	No
104	Invalid password	Yes
105	Invalid activation code	No
106	Data verification error	Yes
107	Field length exceeded	Yes
108	Invalid one time password	Yes
109	Invalid cardholder name	Yes

Account Error Messages		
110	Invalid cardholder	No
111	Invalid password length	No
112	Passwords do not match	Yes
113	Invalid answer	Yes
114	Invalid username	Yes
115	Invalid full name	Yes
116	Invalid personal assurance message (PAM)	Yes
117	Invalid expiry date	Yes
118	Invalid card number	Yes
120	Invalid question	No
121	Invalid device type selected	Yes
122	Resynchronization failed	Yes
123	Invalid cardID	Yes
124	Password must be between [%1] to [%2] characters long	Yes
125	Password must contain at least [?] number(s)	Yes
126	Password must contain at least [?] capital letter(s)	Yes
127	Unicode characters cannot be used	Yes
128	Invalid character	No
129	The parameter ([?]) is required	Yes

Account Error Messages		
130	Invalid PriSec	Yes
131	The Personal Message must not contain your Verified by Visa password or Password Hint	Yes
132	The Password Hint must not contain your Verified by Visa password	Yes
133	The account should have ([?]) authentication data	Yes
134	Invalid Hint	Yes
135	Invalid Data Format	Yes
136	[%1] does not match the confirmation [%2]	Yes

Authentication Device Messages

Authentication Device Messages		
Code	**Message**	**Usage**
101	Please re-enter the field(s) highlighted in red	No
102	Required field missing	Yes
103	Invalid number	No
104	Invalid password	No
105	Invalid Activation Code	No
106	Data verification error	No
107	Field length exceeded	Yes
108	Invalid one time password	Yes

Authentication Device Messages		
301	Current Token:	Yes
302	Please enter the one time password from one of your existing devices here	Yes
303	Invalid one time password	Yes
304	Invalid serial number	Yes
305	Device is lost	Yes
306	Device is damaged	Yes
307	Device is already assigned	Yes
401	Current Token:	No
402	Please enter the one time password from one of your existing devices here	No
403	Invalid one time password	Yes
404	Invalid serial number	Yes
405	Device is lost	Yes
406	Device is damaged	Yes
407	Device is already assigned	Yes
501	SMS Token:	Yes
502	Please enter the one time password which was sent to you via SMS	Yes
503	Invalid SMS one time password	Yes
504	Invalid mobile number	Yes
505	Invalid mobile network provider	Yes

Authentication Device Messages		
506	Invalid country calling code	Yes
507	Please enter the mobile number only, without the country code or prefixes	Yes
508	Mobile number is temporarily disabled	Yes
509	Phone is damaged	Yes
510	Phone is lost	Yes
511	The mobile number entered already exists and has been assigned to a different SMSC	Yes
512	Your mobile number and confirmation do not match. Please re-enter	Yes
513	Phone is already assigned	Yes
601	Current Token:	No
602	Please enter the one time password from one of your existing devices here	No
603	Invalid one time password	Yes
604	Invalid PAN	Yes
605	Device is not active	Yes
606	Device is lost	Yes
607	Device is damaged	Yes
608	Device is already assigned	Yes
701	Email Token:	No
702	Please enter the one time password which was sent to you via Email	No

Authentication Device Messages		
703	Invalid Email one time password	Yes
704	Invalid Email Address	Yes
705	Email is lost	Yes
706	Email is damaged	Yes
707	Your Email and confirmation do not match. Please re-enter	Yes
708	Email is already assigned	Yes
709	Unicode characters are not accepted	Yes

Local Pages Errors

Local Pages Errors	
Code	**Message**
101	Please re-enter the field(s) highlighted in red
102	Required field missing
103	Invalid number
104	Invalid SecureCode Invalid Verified by Visa Password Invalid JSecure Password Invalid SafeKey Invalid ProtectBuy Password
105	Invalid activation code
106	Data verification error
107	Field length exceeded

Local Pages Errors	
108	Invalid one time password
109	Invalid cardholder name
112	Your SecureCode and confirmation do not match. Please re-enter. Your Verified by Visa Password and confirmation do not match. Please re-enter. Your JSecure and confirmation do not match. Please re-enter Your SafeKey and confirmation do not match. Please re-enter. Your ProtectBuy Password and confirmation do not match. Please re-enter.
113	Invalid answer
114	Invalid username
115	Invalid full name
116	Invalid personal assurance message (PAM)
117	Invalid expiry date
118	Invalid card number
119	Invalid CVC
120	Invalid question
121	Invalid device type selected
122	Resynchronization failed
123	Invalid Password length Your SecureCode must be less "maxPassLen" characters long Your Verified by Visa Password must be less than "maxPassLen" characters long Your SecureCode must be less "maxPassLen" characters long Your Verified by Visa Password must be less than "maxPassLen" characters long Your JSecure Password must be less than "maxPassLen" characters long Your SafeKey must be less than "maxPassLen" characters long Your Password must be less than maxPassLen" characters long

Local Pages Errors	
124	Your SecureCode must be less "maxPassLen" characters long Your Verified by Visa Password must be less than "maxPassLen" characters long
125	Your SecureCode must contain at least "minPassDigit" digit(s) Your Verified by Visa must contain at least "minPassDigit" digit(s) JSecure must contain at least "minPassDigit" digit(s) SafeKey must contain at least "minPassDigit" digit(s) Password must contain at least "minPassDigit" digit(s)
126	Your SecureCode must contain at least "minPassCapital" capital letter(s) Your Verified by Visa must contain at least "minPassCapital" capital letter(s) Your JSecure must contain at least "minPassCapital" capital letter(s) Your SafeKey must contain at least "minPassCapital" capital letter(s) Your Password must contain at least "minPassCapital" capital letter(s)
127	Unicode characters are not accepted
128	Invalid character
129	Device is already assigned
130	Invalid PriSec
131	The Personal Message must not contain your Verified by Visa password or Password Hint
132	The Password Hint must not contain your Verified by Visa password
150	This field cannot be left blank
303	Invalid one time password
304	Invalid serial number
305	Device is lost
306	Device is damaged
307	Device is already assigned

Local Pages Errors	
403	Invalid one time password
404	Invalid serial number
405	Device is lost
406	Device is damaged
407	Device is already assigned
503	Invalid SMS one time password
504	Mobile number does not match the specified mobile restriction pattern
505	Invalid mobile network provider
506	Invalid country phone code
507	Please only enter mobile phone number without country code and prefixes
508	Mobile number has been temporarily disabled
509	Mobile phone for this number has been reported as damaged
510	Mobile phone for this number has been reported as lost
511	There is an already existing mobile number which has been assigned to a different SMSC
512	Your Mobile Number was not correctly confirmed. Please make sure that the Mobile Number and confirmation match
513	Phone is already assigned
603	Invalid one time password
604	Invalid PAN
605	Device is not active

Local Pages Errors	
607	Device is damaged
608	Device is already assigned

Glossary

This page provides a list of terms relating to 3D Secure 1 and 2, some are not used elsewhere in this documentation but are included for completeness of the subject area. Familiarise yourself with them now or refer back to this page when you come across an unfamiliar word, phrase or acronym.

Term	Acronym	Definition
2-F Authentication		A generic functionality, which allows for strong authentication of any transaction, commercial or otherwise, for example, strong authentication of users when they login to an Internet banking site or when they authorise funds transfer to a third party. 2-F authentication requires two independent ways to establish identity and privileges as opposed to traditional password authentication, which requires only one 'factor' (knowledge of a password).
3-D Secure **3D Secure** **3D Secure 1** **3D Secure 2**	**3DS** **3DS1** **3DS2**	A payer authentication standard (3D Secure 1 (3DS1)) introduced by Visa (Verified by Visa) and subsequently adopted by Mastercard (Mastercard SecureCode and Mastercard SecureCode), JCB (JCB J/Secure), American Express (SafeKey) and Diners Club International / Discover (ProtectBuy) designed to reduce online credit card fraud and chargeback. The 3DS standard provides an additional layer of protection in card-not-present credit card transactions for the three domains involved: Issuer domain of the card issuing bank, the Interoperability domain of the card scheme's infrastructure and the Acquirer domain of the merchants. The second version of the standard, 3D Secure 2 (3DS2) (EMV 3-D Secure protocol), is facilitated by EMVCo, a six member consortium comprised of American Express, Discover, JCB, Mastercard, UnionPay and Visa. It creates a frictionless payment experience for cardholders by facilitating a richer cardholder data exchange, allowing risk-based authentication by issuers for low risk transactions, instead of authentication challenges to the cardholder, such that most authentication activity will be invisible to the cardholder. 3DS2 also supports authentication of app-based transactions on mobile and other consumer connected devices, and cardholder verification for non-payment transactions, such as adding a payment card to a digital wallet.

Term	Acronym	Definition
3DS Client		The consumer-facing component, such as a browser-based or mobile app online shopping site, which facilitates consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.
3DS Integrator		An EMV 3-D Secure participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer.
3-D Secure Provider		An entity such as American Express, Diners Club International, Discover, JCB, Mastercard or Visa, which provides interoperability services for issuers and merchants who participate in the authentication process. The 3-D Secure provider is normally in charge of managing the directory server, managing the authentication history server and issuing the digital certificates required for participation in the authentication scheme.
3DS Requestor		The initiator of the EMV 3-D Secure Authentication Request, known as the AReq message. For example, this may be a merchant or a digital wallet requesting authentication within a purchase flow.
3DS Requestor App		An App on a Consumer Device that can process a 3-D Secure transaction through the use of a 3DS SDK. The 3DS Requestor App is enabled through integration with the 3DS SDK.
3DS Requestor Environment		This describes the 3DS Requestor controlled components of the Merchant / Acquirer domain, which are typically facilitated by the 3DS Integrator. These components include the 3DS Requestor App, 3DS SDK, and 3DS Server. Implementation of the 3DS Requestor Environment will vary as defined by the 3DS Integrator.
Three Domain Secure Software Development Kit	**3DS SDK**	3-D Secure Software Development Kit. A component that is incorporated into the 3DS Requestor App. The 3DS SDK performs functions related to 3-D Secure on behalf of the 3DS Server.
3DS Requestor Initiated	**3RI**	3-D Secure transaction initiated by the 3DS Requestor for the purpose of confirming an account is still valid. The main use case being recurrent transactions (TV subscriptions, utility bill payments, etc.) where the merchant wants perform a Non-Payment transaction to verify that a subscription user still has a valid form of payment.
3DS Server		Refers to the 3DS Integrator's server or systems that handle online transactions and facilitate communication between the 3DS Requestor and the Directory Server.

Term	Acronym	Definition
3-D Secure	**3DS**	**Three Domain Secure**. An eCommerce authentication protocol that for version 2 onwards enables the secure processing of payment, non-payment and account confirmation card transactions.
Access Control Server	**ACS**	A component that operates in the Issuer Domain, which verifies whether authentication is available for a card number and device type, and authenticates specific Cardholders.
Accountholder Authentication Value	**AAV**	A value providing proof of cardholder authentication, which is generated by the issuer's access control server for each transaction. The AAV is passed by the merchant to the acquirer and then by the acquirer to the issuer through the UCAF field.
Acquirer		A financial institution that has a relationship with a merchant and processes payment transactions for that merchant.
ActiveAccess		GPayments' access control server for card issuers and service providers.
ActiveDevice		GPayments' device agnostic two-factor authentication component.
ActiveMerchant		GPayments' payment authentication platform (merchant plug-in) for merchants.
ActiveServer		GPayments' 3DS Server for payment processors and merchants (see *3DS Server*).
Attempts		Used in the EMV 3DS specification to indicate the process by which proof of an authentication attempt is generated when payment authentication is not available. Support for Attempts is determined by each DS.
Authentication		In the context of 3-D Secure, the process of confirming that the person making an eCcommerce transaction is entitled to use the payment card.
Authentication Device		A physical device capable of generating a token to be used in the verification of a user's identity.
Authentication Request Message	**AReq**	An EMV 3-D Secure message sent by the 3DS Server, via the DS, to the ACS to initiate the authentication process.

Term	Acronym	Definition
Authentication Response Message	**ARes**	An EMV 3-D Secure message returned by the ACS, via the DS, in response to an Authentication Request message.
Authentication Token		An unpredictable piece of information generated by an authentication device, which is used to verify the identity of a user. The term token may sometimes be used to refer to the physical device that generated the token as well.
Authentication Value	**AV**	A cryptographic value generated by the ACS to provide a way, during authorisation processing, for the authorisation system to validate the integrity of the authentication result. The AV algorithm is defined by each Payment System.
Authorisation		A process by which an Issuer, or a processor on the Issuer's behalf, approves a transaction for payment.
Authorisation System		The systems and services through which a Payment System delivers online financial processing, authorisation, clearing, and settlement services to Issuers and Acquirers.
Bank Identification Number	**BIN**	The first six digits of a payment card account number that uniquely identifies the issuing financial institution. Also referred to as an Issuer Identification Number (IIN) in ISO 7812.
BankNet		Mastercard's proprietary payment network.
Base64		Encoding applied to the Authentication Value data element as defined in RFC 2045.
Base64 URL		Encoding applied to the 3DS Method Data, Device Information and the CReq/CRes messages as defined in RFC 7515.
Card		Card is synonymous with the account of a payment card, in the *EMV 3-D Secure Protocol and Core Functions Specification*.
Certificate Authority	**CA**	
Cardholder		An individual to whom a card is issued or who is authorised to use that card.

Term	Acronym	Definition
Cardholder Activation During Shopping		A 3D-Secure 1 process by which cardholders can enrol with the authentication system at the time of making a purchase at a participating merchant eCommerce website.
Centralised Authentication and Authorisation Service	**CAAS**	A remote ACS, see *Access Control Server*.
Challenge		The process where the ACS is in communication with the 3DS Client to obtain additional information through Cardholder interaction.
Challenge Flow		A 3-D Secure flow that involves Cardholder interaction as defined in the *EMV 3-D Secure Protocol and Core Functions Specification*.
Challenge Request Message	**CReq**	An EMV 3-D Secure message sent by the 3DS SDK or 3DS Server where additional information is sent from the Cardholder to the ACS to support the authentication process.
Challenge Response Message	**CRes**	The ACS response to the CReq message. It can indicate the result of the Cardholder authentication or, in the case of an App-based model, also signal that further Cardholder interaction is required to complete the authentication.
Chip Card		A card with an on-board integrated circuit chip.
Consumer Device		Device used by a Cardholder such as a smartphone, laptop, or tablet that the Cardholder uses to conduct payment activities including authentication and purchase.
Cryptography		A process that encrypts information for the purpose of protecting it. Information is decrypted when required.
Device		see *Authentication Device*.
Device Channel		Indicates the channel from which the transaction originated. Either: • App-based (01-APP) • Browser-based (02-BRW) • 3DS Requestor Initiated (03-3RI)
Device Information		Data provided by the Consumer Device that is used in the authentication process.

Term	Acronym	Definition
Directory Server	**DS**	A server component operated in the Interoperability Domain; it performs a number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Directory Server Certificate Authority	**DS CA** or **CA DS**	A component that operates in the Interoperability Domain; generates and Certificate Authority (DS distributes selected digital certificates to components participating in 3-D Secure. Typically, the Payment System to which the DS is connected operates the CA.
Directory Server ID (directoryServerID)		Registered Application Provider Identifier (RID) that is unique to the Payment System. RIDs are defined by the ISO 7816-5 standard.
Electronic Commerce Indicator	**ECI**	Payment System-specific value provided by the ACS to indicate the results of the attempt to authenticate the Cardholder.
Digital Signature		Equivalent of the physical signature in the digital world. Digital signatures can verify the identity of owner of a piece of information or a document in the digital world.
Enrolment		A cardholder must pass an initial online authentication procedure in 3D-Secure 1, which is verified by the Issuer prior to gaining eligibility for participation in American Express SafeKey, Diners Club International ProtectBuy, JCB J/Secure, Mastercard SecureCode or Verified by Visa authentication.
Frictionless		Used to describe the authentication process when it is achieved without Cardholder interaction.
Frictionless Flow		A 3-D Secure flow that does not involve Cardholder interaction as defined in EMVCo Core Spec Section 2.5.1.
Issuer		A financial institution that provides cardholders with credit cards.
J/Secure		JCB's standard for cardholder authentication, based on 3-D Secure.
Message Authentication Code	**MAC**	

Term	Acronym	Definition
Mastercard SecureCode / Identity Check		Mastercard's payer authentication brand, which includes SPA Algorithm for the Mastercard Implementation of 3-D Secure, SPA and chip card authentication program (CAP).
Mastercard 3-D Secure		The SPA Algorithm for the Mastercard Implementation of 3-D Secure that provides a browser authentication experience to the cardholder (see also *3-D Secure)*.
Mastercard Identity Check		see *Mastercard SecureCode / Identity Check*.
Merchant		Entity that contracts with an Acquirer to accept payments made using payment cards. Merchants manage the Cardholder online shopping experience by obtaining the card number and then transfers control to the 3DS Server, which conducts payment authentication.
Merchant Plug-in (MPI)		A software module which can be integrated into a merchant's eCommerce website or run as a managed service on behalf of a number of merchants to provide 3-D Secure authentication.
Non-Payment Authentication	**NPA**	.
One-Time Passcode	**OTP**	A passcode that is valid for one login session or transaction only, on a computer system or other digital device.
Out-of-Band	**OOB**	A Challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed. ACS authentication methods or implementations are not defined by the 3-D Secure specification.
Payer Authentication Request	**PAReq**	Message sent from the MPI to the Access Control Server at the cardholder's issuer via the cardholder browser.
Payer Authentication Response	**PARes**	A digitally signed message sent from the Access Control Server to the Merchant Plug-in which communicates whether the cardholder authentication was successful or not.

Term	Acronym	Definition
Payment Gateway		A software system provided by an acquirer or a third party which accepts transactions from the Internet and transfers them to a payment network such as BankNet or VisaNet.
Preparation Request Message	**PReq**	3-D Secure message sent from the 3DS Server to the DS to request the ACS and DS Protocol Versions that correspond to the DS card ranges as well as an optional 3DS Method URL to update the 3DS Server's internal storage information.
Preparation Response Message	**PRes**	Response to the PReq message that contains the DS Card Ranges, active Protocol Versions for the ACS and DS and 3DS Method URL so that updates can be made to the 3DS Server's internal storage.
Proof or authentication attempt		Refer to Attempts.
ProtectBuy		Diners Club International and Discover standard for cardholder authentication, based on 3-D Secure.
Registered Application Provider Identifier	**RID**	Registered Application Provider Identifier (RID) is unique to a Payment System. RIDs are defined by the ISO 7816-5 Standard and are issued by the ISO/IEC 7816-5 Registration Authority. RIDs are 5 bytes.
Results Request Message	**RReq**	Message sent by the ACS via the DS to transmit the results of the authentication transaction to the 3DS Server.
Results Response Message	**RRes**	Message sent by the 3DS Server to the ACS via the DS to acknowledge receipt of the Results Request message.
Risk-Based Authentication	**RBA**	During risk-based authentication, the rich cardholder data exchanged in AReq is taken into account to determine the risk profile associated with that transaction. The complexity of the challenge is then decided based on the risk profile.
SafeKey		American Express standard for cardholder authentication, based on 3-D Secure.

Term	Acronym	Definition
Secure Payment Application (SPA)		Mastercard's payer authentication standard designed to reduce online credit card fraud and chargeback using a client-side applet. Also known as Mastercard's PC Authentication Program, Mastercard SecureCode, Mastercard SPA and SPA.
Secure Sockets Layer (SSL)		A protocol designed to maintain the integrity and confidentiality of communication over the Internet.
SecureCode		see *Mastercard SecureCode / Identity Check*.
Token:		see *Authentication Token*.
Two Factor Authentication		see *2-F Authentication*
Uniform Resource Locator (URL)		Address system for locating unique sites on the Internet.
Universal Cardholder Authentication Field (UCAF)		Data element 48 sub element 43 as defined in Mastercard BankNet to carry authentication data. Mastercard SecureCode uses this element to transport AAV from the acquirer to the issuer.
Verified by Visa	**VbV**	A payer authentication standard introduced by Visa (see *3-D Secure*).
VisaNet		Visa's proprietary payment network.

Document Control

+ new item Δ item changed X item removed 🟦 no change to item

Date	AA Ver	Doc Ver	Change Details
[05/09/2019]	8.0.1	8.0.1:1	**Product Architecture** (Installation Guide) Δ Disaster Recovery and Clustering diagrams added.
			Installation (Installation Guide) Δ Changes made to Upgrades from v7.4.x and New installations.
			Security (Admin UI) + Create Certificate Request: New **Key type** field added.
			Risk Engine Adapter (Specifications) Δ **ParameterDataElements**: **Validator** field description updated Δ **RemoteAssessmentRequest Data Elements**: **PreviousData** field format updated + **AReqWithTransStatusDataElements** added Δ **AReq Data Elements**: **ThreeDSCompInd** and **ThreeDSRequestorAuthenticationInd** field updated.
			Remote Messaging (Specifications) Δ **InitAuthReq** table: Usage of **oobInfo** changed.
			Out of Band (OOB) Authentication Adapter (Specifications) Δ Change the URL in **Restful API version of OOB Adapter** Δ Change `NOT__AUTHENTICATED` to `NOT_AUTHENTICATED` Δ Update MobilePhone Data Elements, HomePhone Data Elements, and WorkPhone Data Elements.

Date	AA Ver	Doc Ver	Change Details
15/08/2019	8.0.0	8.0.0:1	**Product Architecture** (Installation Guide) Δ Components labelled with (3DS1) or (3DS2) as relevant + Challenge Server (3DS2) added. + Risk Engine Adapter added + Out of Band (OOB) Authentication Adapter added Δ Logical view of ActiveAccess diagram updated Δ Hardware and Software Requirements updated X Removed references to **RuPay** components.
			External Components (Installation Guide) Δ Application Server dependency removed, supports compatible Java Application Servers.
			Installation (Installation Guide) Δ ActiveAccess installation and setup process simplified.
			System Management (Admin UI) + **Authentication Management** section added with tabs for: Δ Device Management previously under **System Management** + Risk Management for 3DS2 risk management + OOB Management for OOB processing support.
			System Management (Admin UI) - **Issuer Management** Δ Device Settings: OOB added as a supported device.
			Security (Admin UI) + Directory Server Certificate section added + OOB Certificate section added + Risk Certificate section added.
			Issuers (Admin UI) Δ Providers parameters moved to a new page, and linked, from the **Settings** page. New fields added.

Date	AA Ver	Doc Ver	Change Details
			Rules (Admin UI) Δ Rule Management section replaces previous ***Authentication Exemption*** and ***Force Registration*** sections Tabs for: + Registration previously ***Force Registration*** tab under **Rules** Δ Authentication previously ***Authentication Exemption*** tab under **Rules** 🟦 Settings.
			Cards (Admin UI) Δ **Users** tab renamed to **Cards**.
			Reports (Admin UI) Δ Reports support reporting by 3-D Secure version.
			Transactions (Admin UI) Δ **Find 3-D Secure**: supports search by 3-D Secure version. New fields added.
			Admins (Admin UI) Δ Admin User Details and User Profile: added **2-factor authentication** login option
			Local Messaging (Specifications) Δ Final Registration Request: updated with OOB device registration request.
			Remote Messaging (Specifications) Δ **Transaction** table: **issuerName** and **theeDSProtocolVersion** added + **HeaderParams** table added + **AdditionalParams** table added + **PreAuthResp** table: **AuthType** added + **InitAuthReq** table: new OTP types for **AuthType** and **oobInfo** added Δ Sample Request Response: changed **CVD** to NULL.

Date	AA Ver	Doc Ver	Change Details
			CHANGES TO DOCUMENTATION STRUCTURE ➕ All documentation moved online with the ability to print to PDF ***To print the entire ActiveAccess documentation***: click the ⤓ button on the Introduction page. ***To print a section***: click the ⤓ button on that section. ***Tip***: hovering your mouse over the ⤓ button will let you see which section will be printed. Δ **See Documentation change details** for full details of the changes in the documentation moving from PDF to online format.
26/02/2019	7.4.6	7.4.6.1	**Remote Messaging** Δ **initAuthReq** table: added AuthType Δ **CardInfo** table: RegToken definition updated.
06/07/2018	7.4.0	7.4.0:1	➕ Addition of options in **System Management > Settings** to allow administrators at specified access levels to view Card Number (plaintext) and AAV/CAVV/AEVV Δ Updated description of Soft Launch List ➕ Addition of ActiveAccess Error Codes in Appendix A.

Documentation change details

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
Introduction		
Installation Guide >		A11-Install_Maint_TechRef.pdf
	Product Architecture	
	External Components	
	Installation	
Administration UI >		AA12-ActiveAccess Administration.pdf
	About the Issuer Administration Server	AA12 / Added support for two-factor authentication for logging into the Administration UI
	System Management >	AA12
	About System Management	AA12
	Settings	AA12
	ACS Settings	AA12
	Issuer Management	AA12
	- Group Management	AA12
	- *Authentication Mgmt >*	➕ **New Subsection**
	- About Authentication Management	➕ **New**

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	- Devices	Δ AA12, previously Device Management
	- Risk	+ **New**
	- OOB	+ **New**
	Public & Encryption Key Management	AA12
	Exchange Configuration	AA12
	Archive Management	AA12
	Security	AA12
	- Issuer Certificate	AA12
	- AHS Certificate	AA12
	- CAAS Certificate	AA12
	- Directory Server Certificate	+ **New**
	- OOB Certificate	+ **New**
	- Risk Certificate	+ **New**
	- CA Certificate	AA12
	Servers	AA12
	- MIA Servers	AA12
	- Access Control Servers (ACS)	AA12
	- Authentication History Servers (AHS)	AA12

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	- Centralised Authentication and Authorisation Servers (CAAS	AA12
	- Out of Band Authentication Servers (OOB)	AA12
	- Risk Servers	AA12
	Utilities >	
	Utilities	AA12
	Key Retiring Utility	AA12
	Issuers	AA12
	- Settings	AA12
	- Upload Registration Files	AA12
	- Custom Pages	AA12
	- Key Management	AA12
	Rules	
	- Registration -- Amount Threshold -- Merchant Blacklist	AA12
	- Authentication -- Soft Launch List Rule -- Merchant Whitelist Rule -- Merchant Watchlist -- Location Watchlist - Location Watchlist Search Results -- Domestic & International Transaction Amount Threshold -- Stand-In Transaction Threshold	AA12

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	- Settings	AA12
	Admin Users	AA12
	Cards	AA12 Δ **Users** renamed to **Cards**
	Transactions	AA12
	Reporting	AA12
	Audit Log	AA12
	Profile Management_	AA12
Specifications		
	Local Messaging >	
	Local Messaging	AA61-Messaging Specification.pdf
	Card Loader	AA32-GPayments Card Loader.pdf
	Remote Messaging >	
	Remote Messaging	AA71-Remote System Messaging Specification.pdf
	Country and Currency Codes	AA71-Remote System Messaging Specification.pdf Appendix A
	Sample Card	AA71-Remote System Messaging Specification.pdf Appendix B
	Sample Request Response	AA71-Remote System Messaging Specification.pdf Appendix C
	SMS via JMS	AA83-ActiveAccess - SMS via JMS Library.pdf
	Out of Band Authentication Adapter	+ **New**

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	Risk Engine Adapter	➕ **New**
Error Codes		AA12 - Appendix A
Glossary		AA12
Document Control>		
	Document Control	AA12
	Documentation Changes (*this page*)	➕ **New**
Release Notes		Δ Previously included in the ActiveAccess package
Legal Notices		AA12

Release Notes

ActiveAccess v8.0.1

[05/09/2019]

[EOL: Two years after the subsequent version's release date]

Type	Issue Number	Description	Components
ENHANCEMENT	#169	EULA update	Issuer Administration
ENHANCEMENT	#208	Grant scripts run automatically during setup	Setup
FIX	#172	Device selection page isn't being shown	Access Control Server
FIX	#182	Device registration fails when issuer has OOB device enabled	Access Control Server
FIX	#186	Exception raised during Diners Club remote authentication	Access Control Server
FIX	#188	ChallengeResponse failure in remote authentication	Access Control Server
FIX	#189	Risk adapter configuration page issue	Issuer Administration
FIX	#193	Generate RSA 2048 when the EC key generation fails	Setup, Issuer Administration, Access Control Server
FIX	#196	CardLoader setup.sh doesn't work	CardLoader
FIX	#203	Upgrade issue from 7.4.2 to 8.0.0 with currency exchange rate	Setup

Type	Issue Number	Description	Components
FIX		Minor bug fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.0.0

[15/08/2019]

[05/09/2021]

Type	Issue Number	Description	Components
ENHANCEMENT	#93	Enhancements to the Administration interface (MIA)	Issuer Administration
ENHANCEMENT	#5468	Support incremental database schema changes in Setup	Setup
ENHANCEMENT	#5801	Web Container Neutralization	Setup
ENHANCEMENT	#6659	Support for 3-D Secure 2.1	Setup, Issuer Administration, Access Control Server, Registration Server
ENHANCEMENT	#6661	3DS2 Transaction search based on 3DS version	Issuer Administration
ENHANCEMENT	#6663	Support for 3DS2 Risk Management	Issuer Administration, Access Control Server
ENHANCEMENT	#6664	Support 3DS2 Reporting	Issuer Administration
ENHANCEMENT	#7207	Support for OOB Processing	Issuer Administration, Access Control Server
ENHANCEMENT	#7383	Substitute Triple DES encryption in ActiveAccess with stronger cryptography	Issuer Administration, Access Control Server

Type	Issue Number	Description	Components
ENHANCEMENT	#7845	Removal of RuPay component	Setup, Issuer Administration
ENHANCEMENT	#7880	Two-factor authentication for MIA login	Issuer Administration
ENHANCEMENT	#8082	Simplify the setup process	Setup
ENHANCEMENT	#8310	SPA2 algorithm for AAV generation	Setup, Issuer Administration, Access Control Server
FIX	#5425	MIA allows exceeded password length and updates it successfully	Access Control Server
FIX	#7297	Adminlog and AuditlogCollectorErrors have been updated to fix the errors that occurred during scheduler job	Access Control Server
FIX	#8160	Authentication Exemption Rules for CAAS server	Access Control Server

ActiveAccess v7.4.7 (Patch)

[23/03/2019]

[EOL: 15/08/2021]

Access Control Server		
FIX	#8147	Fixed the purchAmount field to avoid the mismatch of value between PARes and PAReq

ActiveAccess v7.4.6 (Patch)

[05/03/2019]

[EOL: 23/03/2021]

Issuer Administration		
FIX	#8022	Removing "+" sign when sending message via JMS.

Access Control Server		
FIX	#8022	Removing "+" sign when sending message via JMS.

ActiveAccess v7.4.5 (Patch)

[01/02/2019]

[EOL: 05/03/2021]

Access Control Server		
ENHANCEMENT	#7843	Displaying the Mobile Number on Remote Authentication pages.
ENHANCEMENT	#7893	Adding PurchaseExponent attribute to the transaction table of requests to CAAS.

ActiveAccess v7.4.4 (Patch)

[27/09/2018]

[EOL: 01/02/2021]

Issuer Administration		
FIX	#7748	SMS delivery fails as ACS sends the phone number without the '+' sign to SMPP client. ACS now includes the + sign when sending SMS.

Access Control Server		
FIX	#7748	SMS delivery fails as ACS sends the phone number without the '+' sign to SMPP client. ACS now includes the + sign when sending SMS.

ActiveAccess v7.4.3 (Patch)

[18/09/2018]

[EOL: 27/09/2020]

Issuer Administration		
FIX	#7718	Card Registration File Upload Errorcard file. Clearing the timer to prevent "java.lang.IllegalStateException: Timer already canceled" exceptions.

ActiveAccess v7.4.2

[20/08/2018]

[EOL: 07/06/2020]

Issuer Administration		
ENHANCEMENT	#7543	ISO 3166 Update country details for Eswatini
ENHANCEMENT	#7654	ISO 4217 Amendment Number 169

Active Control Server		
ENHANCEMENT	#7543	ISO 3166 Update country details for Eswatini
ENHANCEMENT	#7654	ISO 4217 Amendment Number 169
FIX	#7677	CurrencyExchange error in ActiveAccess startup

Registration Server		
FIX	#7639	Card Registration File Upload

ActiveAccess v7.4.1 (Patch)

[08/08/2018]

[EOL: 20/08/2020]

Issuer Administration		
FIX	#7557	Verification code not received for Email device type

Active Control Server		
FIX	#7482	Custom Pages layout updates
FIX	#7557	Verification code not received for Email device type

ActiveAccess v7.4.0

[06/07/2018]

[EOL: 08/08/2020]

Setup		
ENHANCEMENT	#6479	External HSM setup - PKCS #11 Support
ENHANCEMENT	#7470	Update key type for CVC2 process
ENHANCEMENT	#7471	HMAC key length update for MC
ENHANCEMENT	#7477	Support HSMs in which DES is not available
ENHANCEMENT	#7519	Upgraded log4j from 1.2.13 to the 1.2.17 version
FIX	#7380	Visa 3-D Secure Security Program - Encryption of CAVV/AAV values
FIX	#7518	Updated GET_CARDS procedure

Issuer Administration		
ENHANCEMENT	#6479	External HSM setup - PKCS #11 Support
ENHANCEMENT	#7359	ISO 4217 Amendment Number 166

Issuer Administration		
ENHANCEMENT	#7470	Update key type for CVC2 process
ENHANCEMENT	#7471	HMAC key length update for MC
ENHANCEMENT	#7477	Support HSMs in which DES is not available
ENHANCEMENT	#7519	Upgraded log4j from 1.2.13 to the 1.2.17 version
FIX	#7329	Public key for the Issuer Group
FIX	#7380	Visa 3-D Secure Security Program - Encryption of CAVV/AAV values
FIX	#7520	Purge processor is already running error

Access Control Server		
ENHANCEMENT	#6479	External HSM setup - PKCS #11 Support
ENHANCEMENT	#7359	ISO 4217 Amendment Number 166
ENHANCEMENT	#7482	Combining two device registration custom pages into one
ENHANCEMENT	#7519	Upgraded log4j from 1.2.13 to the 1.2.17 version
FIX	#7047	Updating the path of caaswarning.properties to keep it unchanged during the upgrade process
FIX	#7380	Visa 3-D Secure Security Program - Encryption of CAVV/AAV values
FIX	#7518	Updated GET_CARDS procedure

Enrolment Server		
ENHANCEMENT	#6479	External HSM setup - PKCS #11 Support
ENHANCEMENT	#7519	Upgraded log4j from 1.2.13 to the 1.2.17 version

Registration Server		
ENHANCEMENT	#6479	External HSM setup - PKCS #11 Support
ENHANCEMENT	#7519	Upgraded log4j from 1.2.13 to the 1.2.17 version

ActiveAccess v7.3.3 (Patch)

[25/05/2018]

[EOL: 06/07/2018]

Access Control Server		
FIX	#7402	Incorrect JCB transaction status with 'Card Not Found' from CAAS

ActiveAccess v7.3.2 (Patch)

[29/03/2018]

[EOL: 25/05/2020]

Access Control Server		
FIX	#7160	Remove error on missing MD field

ActiveAccess v7.3.1 (Patch)

[20/02/2018]

[EOL: 29/03/2020]

Access Control Server		
FIX	#7116	JCB VEReq with Browser.deviceCategory=1

ActiveAccess v7.3.0

[29/01/2018]

[EOL: 20/02/2020]

Setup		
FIX	#6334	Correction to the casing for SafeNet in setup/sample.ini
FIX	#6338	Remove WebSphere application server option from setup
FIX	#6986	Decryption error during notification report process
FIX	#7052	Notification reports - java.lang.NullPointerException

Issuer Administration		
FIX	#6406	Exception thrown when clicking Back on Matched Rule Details page
FIX	#6244	Update the default value for AMEX 'Maximum forgot password attempts
FIX	#6620	MIA incorrectly searches the WEB-INF folder for cacerts, instead of the config folder
FIX	#6645	Cards do not get assigned to the most detailed BIN
FIX	#7052	Notification reports - java.lang.NullPointerException
ENHANCEMENT	#4131	Authentication pages compatibility with mobile devices
ENHANCEMENT	#5935	New authentication method Email OTP
ENHANCEMENT	#6252	ISO 3166 Update country details for Moldova and Gambia
ENHANCEMENT	#6308	Addition of a message on MIA's blank screen for admin users of Issuers with an invalid license key
ENHANCEMENT	#6377	Option to defer application of Setting changes to next server restart

Issuer Administration		
ENHANCEMENT	#6463	ISO 4217 Currency Code Service - Amendment number 163
ENHANCEMENT	#6527	Mastercard Identity Check Support
ENHANCEMENT	#6688	JCB Attempt process
ENHANCEMENT	#6727	Security enhancements
ENHANCEMENT	#6765	All PANs must now comply with the Luhn algorithm and pass a Mod-10 check
ENHANCEMENT	#6773	ISO 4217 Amendment Number 164
ENHANCEMENT	#6823	Rules Settings challenge option for 'not exempted authentications' as per IDC requirements
ENHANCEMENT	#6981	ISO 4217 Amendment Number 165

Access Control Server		
FIX	#5686	Proof of Attempt = Disabled still displays the opt-out link during ADS
FIX	#6244	Update the default value for AMEX 'Maximum forgot password attempts
FIX	#6417	PAReq is not logged by ACS when the Authentication Exemption Rules are used
FIX	#6687	Updating error details wording to match 3DS v1.0.2 document
FIX	#6693	Errors related to JCB compliance test
FIX	#7037	Authentication Exemption rules do not apply during transactions
ENHANCEMENT	#4131	Authentication pages compatibility with mobile devices
ENHANCEMENT	#5935	New authentication method Email OTP
ENHANCEMENT	#6209	Style applied to XML formatted error pages displayed during authentication

Access Control Server		
ENHANCEMENT	#6252	ISO 3166 Update country details for Moldova and Gambia
ENHANCEMENT	#6463	ISO 4217 Currency Code Service - Amendment number 163
ENHANCEMENT	#6527	Mastercard Identity Check Support
ENHANCEMENT	#6652	Compliance with JCB J/Secure
ENHANCEMENT	#6688	JCB Attempt process
ENHANCEMENT	#6689	Addition of new data elements in JCB Authentication page and updates to the masking format of PAN
ENHANCEMENT	#6691	Remove AHS support for JCB
ENHANCEMENT	#6692	Multi-language support of JCB pages
ENHANCEMENT	#6727	Security enhancements
ENHANCEMENT	#6765	All PANs must now comply with the Luhn algorithm and pass a Mod-10 check
ENHANCEMENT	#6773	ISO 4217 Amendment Number 164
ENHANCEMENT	#6823	Rules Settings challenge option for 'not exempted authentications' as per IDC requirements
ENHANCEMENT	#6981	ISO 4217 Amendment Number 165

Enrolment Server		
ENHANCEMENT	#6705	The effect of 'Uses confirmation' field in Enrolment
ENHANCEMENT	#6727	Security enhancements

Registration Server		
FIX	#6396	CardLoader error message does not correspond with Registration logs
ENHANCEMENT	#5935	New authentication method Email OTP
ENHANCEMENT	#6527	Mastercard Identity Check Support
ENHANCEMENT	#6727	Security enhancements

ActiveAccess v7.2.1

[20/04/2017]

[EOL: 29/01/2020]

Setup v7.2.1

Issuer Administration v7.2.1

Access Control Server v7.2.1

Enrolment Server v7.2.1

Registration Server v7.2.1

Setup		
ENHANCEMENT	#6289	Encode hsmpassword parameter (Base64) in RuPay config file.

Issuer Administration		
FIX	#4584	PCI Key Retiring utility performance issue.
FIX	#6182	Certificate creation failure.
ENHANCEMENT	#6289	Encode hsmpassword parameter (Base64) in RuPay config file.

Access Control Server		
FIX	#4584	PCI Key Retiring utility performance issue.
FIX	#6186	Error while processing a custom page.
ENHANCEMENT	#4217	Addition of JCB XSL pages into the standard release package.
ENHANCEMENT	#6289	Encode hsmpassword parameter (Base64) in RuPay config file.

Enrolment Server		
ENHANCEMENT	#6289	Encode hsmpassword parameter (Base64) in RuPay config file.

Registration Server		
ENHANCEMENT	#6289	Encode hsmpassword parameter (Base64) in RuPay config file.

ActiveAccess v7.2.0

[22/12/2016]

[EOL: 20/04/2019]

Setup v7.2.0

Issuer Administration v7.2.0

Access Control Server v7.2.0

Enrolment Server v7.2.0

Registration Server v7.2.0

Rupay v1.1.0

Card Loader 1.1.41

Setup		
SUPPORT:	#5806	nCipherKM.jar being removed in installation
ENHANCEMENT:	#5474	Support silent mode installation
ENHANCEMENT:	#5939	Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files
ENHANCEMENT:	#5574	Remove usage of deprecated JRE classes
FEATURE:	#5546	Supports Amex Safekey compliance (rev 2016)

Issuer Administration		
FIX:	#5525	Encrypt critical data in case of registration failure
FIX:	#5899	Archive history details page display error
SUPPORT:	#5729	Visa Intermediate SHA2 CA cert added for new installations
ENHANCEMENT:	#5574	Remove usage of deprecated JRE classes
ENHANCEMENT:	#5740	Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries
ENHANCEMENT:	#5829	Remove restriction on using previous CAVV key
ENHANCEMENT:	#5874	Support p7 and der files when installing certificates
ENHANCEMENT:	#5939	Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files
FEATURE:	#5546	Supports Amex Safekey compliance (rev 2016)

Access Control Server		
FIX:	#4584	Improve PCI Key Retiring utility performance*

Access Control Server		
FIX:	#5965	CAAS Card Auth Data format not found error. The error message is logged in ACS logs during a remote transaction regardless of success of the transaction.
FIX:		Various spelling corrections in application and XSL files
SUPPORT:	#5748	Error in restarting Number of authentication exemptions and Sum of exempted authentications' amounts when empty cardholder name is received from CAAS server
SUPPORT:	#5785	Unable to establish connection to CAAS
SUPPORT:	#5903	Optimise GET_CARDS procedure
SUPPORT:	#5952	Update American Express SafeKey logo
ENHANCEMENT:	#5054	Support SafeNet Network HSM (Cloud HSM/Luna SA)
ENHANCEMENT:	#5546	Compliance with American Express Safekey (revision 2016)
ENHANCEMENT:	#5574	Remove usage of deprecated JRE classes
ENHANCEMENT:	#5740	Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries
ENHANCEMENT:	#5939	Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files
FEATURE:	#5546	Supports Amex Safekey compliance (rev 2016)

Enrolment Server		
FIX:		Various spelling corrections in application and XSL files
ENHANCEMENT:	#5574	Remove usage of deprecated JRE classes

Enrolment Server		
ENHANCEMENT:	#5740	Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries
ENHANCEMENT:	#5939	Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files

Registration Server		
SUPPORT:	#5767	Changing request Id length in notification request to be at most 1024 characters
ENHANCEMENT:	#5574	Remove usage of deprecated JRE classes
ENHANCEMENT:	#5740	Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries
ENHANCEMENT:	#5939	Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files

RuPay		
FIX:	#5482	Search by Error Code field in Transaction screens
FIX:	#6025	RuPay verifyRegistration did not forward contextBlob to initAuthentication. contextBlob now included
FIX:	#6026	Support authType in addition to authTypeSupList in RuPay

Card Loader		
FIX:	#5779	CardLoader now supports Java 8
SUPPORT:	#5767	Changing request Id length in notification request to be at most 1024 characters
ENHANCEMENT:	#5574	Remove usage of deprecated JRE classes

ActiveAccess v7.1.4

[03/10/2016]

[EOL: 22/12/2018]

Setup v7.1.4

Issuer Administration v7.1.4

Access Control Server v7.1.4

Enrolment Server v7.1.4

Registration Server v7.1.4

Issuer Administration		
Support	#5703	Database connectivity issue
Bug	#5720	ActiveAccess 7.1.4 beta 5 installation error: no record found
Enhancement	#5715	Version class in ActiveAccess should be filtered in Maven
Support	#5664	Login issue with remote issuers' business and helpdesk admins without access to rules
Support	#5548	FileNotFoundException: auditconfig.properties changed from an Error to a Warning
Bug	#5745	CSR Export Issue

Access Control Server		
Support	#5703	Database connectivity issue
Bug	#5689	CAAS: ISO currency & country codes
Enhancement	#5523	Risk Based Authentication
Bug	#5674	DB Warning Logger in ACS log file

Access Control Server		
Enhancement	#5715	Version class in ActiveAccess should be filtered in Maven
Enhancement	#5688	Copyright of XSL pages
Bug	#5685	AHS logging PATransReq twice in the acs log file
Support	#5646	Merchant URL Must be URL pattern
Support	#5634	PARes with parameter SSID to MPI
Support	#5616	A null priSec value results in NullPointerException
Enhancement	#5596	Support for unmasked CH.fullPAN in PATRANSReq messages

Enrolment Server		
Enhancement	#5715	Version class in ActiveAccess should be filtered in Maven

Registration Server		
Enhancement	#5715	Version class in ActiveAccess should be filtered in Maven

Setup		
Bug	#5735	RuPay tables missing in database after installation
Enhancement	#5715	Version class in ActiveAccess should be filtered in Maven
Bug	#5678	RuPay module being installed without being selected (Centos 6.x)
Bug	#5562	No rupay WAR files found in tomcat/webapps when installing AA with Rupay option

ActiveAccess v7.1.3

[03/09/2016]

[EOL: 03/10/2018]

Setup v7.1.3

Issuer Administration v7.1.3

Access Control Server v7.1.3

Enrolment Server v7.1.3

Registration Server v7.1.3

Access Control Server		
Bug	#5619	SignatureMethod must be SHA1

No changes in other components

Legal Notices

Confidentiality Statement

GPayments reserves all rights to the confidential information and intellectual property contained in this document. This document may contain information relating to the business, commercial, financial or technical activities of GPayments. This information is intended for the sole use of the recipient, as the disclosure of this information to a third party would expose GPayments to considerable disadvantage. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any process without prior written permission. This information is provided under an existing non-disclosure agreement with the recipient.

Copyright Statement

All third party product and service names and logos used in this document are trade names, service marks, trademarks, or registered trademarks of their respective owners.

The example companies, organizations, products, people and events used in screenshots in this document are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

Disclaimer

GPayments Pty Ltd makes no, and does not intend to make any, representations regarding any of the products, protocols or standards contained in this document. GPayments Pty Ltd does not guarantee the content, completeness, accuracy or suitability of this information for any purpose. The information is provided "as is" without express or implied warranty and is subject to change without notice. GPayments Pty Ltd disclaims all warranties with regard to this information, including all implied warranties of merchantability and fitness for a particular purpose and any warranty against infringement. Any determinations and/or statements made by GPayments Pty

Ltd with respect to any products, protocols or standards contained in this document are not to be relied upon.

Liability

In no event shall GPayments Pty Ltd be liable for any special, incidental, indirect or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) whether in an action of contract, negligence or other tortuous action, rising out of or in connection with the use or inability to use this information or the products, protocols or standards described herein, even if GPayments has been advised of the possibilities of such damages.

GPayments