About Setup Guide

This section is a post installation guide for setting up ActiveAccess for testing. It describes, at a high level, the steps involved in setting up issuers, signing certificates and configuring cards for various payment scenarios, prior to testing. It also covers the steps involved in device configuration, setting up remote / external authentication, archiving and RBA. It should be read in conjunction with Administration UI, which provides additional information on completing each step.

Document Conventions

The following colours are used to indicate in which environment setup steps are to be performed.

Colour	Environment
	ActiveAccess Administration
	ActiveMerchant Test Payment Page (GPayments MPI (ActiveMerchant)) or an equivalent third-party MPI
	GPayments Licensing
	Certificate Authority

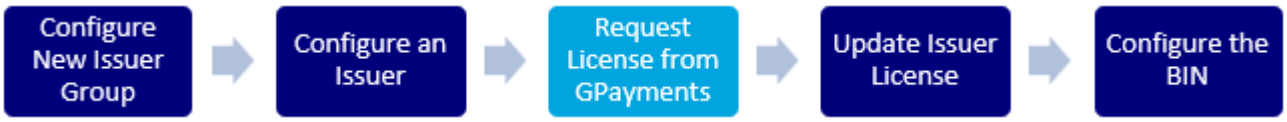
ACS URL

This section covers configurations related to *3DS1 only*.

System Management > ACS Settings > Authentication server: Local or Remote

1. Enter the **ACS URL** (e.g. https://yourserverip:port/acs/pa)
2. Click the **Apply** button.

Issuer Groups and Issuers



Configure a New Issuer Group (Optional)

System Management > Group Management

- Check for an Issuer Group relevant to the client by looking under the **Group Name** column.
- If the required Issuer Group exists, go to Configure an Issuer, otherwise click the *New Issuer Group* link
- Enter the Issuer Group **Name** (*e.g.* Company Issuer Group)
- You may skip the remaining fields or fill them, as appropriate
- Click the **Apply** button.

> **Note**
>
> Cryptographic keys are created for the issuer signing certificate and CAVV validation.

Configure an Issuer

System Management > Issuer Management

- Check for a relevant issuer by looking under the **Issuer Name** column or searching for it by **Issuer Name**
- If the issuer exists, go to Section 4.3 - Request and Update Issuer License, otherwise click the *New Issuer* link
- Enter the Issuer **Name** (e.g. Test Issuer, Test Bank)
- Select the Issuer Group, if one was created in Section 4.1 - Configure a New Issuer Group, from the **Parent group** drop down list and tick the checkboxes for **Use parent certificate, public and encryption keys** and **Use parent keys**

- You may skip the remaining fields or fill them, as appropriate
- Click the **Apply** button.

> **Note**
>
> Cryptographic keys are created for encrypting the cardholder and transaction data of the specified issuer.

Request and Update Issuer License

ActiveAccess License

- Contact GPayments and request a license key for the issuer created in Section 4.2 - Configure an Issuer
- Copy the license key provided to you by GPayments to your clipboard.

System Management > Issuer Management

- Find the issuer and click the *Issuer Name*
- On the **Issuer Details** page, paste the copied **License Key** into the text box
- Click the **Apply** button.

> **Note**
>
> If an error occurs, contact GPayments Tech Support.

Configure the BIN

System Management > Issuer Management

- Find the issuer and click the *Issuer Name*
- On the **Issuer Details** page, click the *BIN Management* link
- On the **BIN Management** page, click the *Add BIN* link
- On the **Add BIN** page, enter the **BIN** (e.g. 412345)
- Ensure **Status** is set to **Enabled**
- Select an option from the drop down list for **Device over 3-D Secure**, as appropriate

- Click the **Apply** button.

Certificate Signing Requests

Configure Issuer Group Signing Certificates

Issuer Group Signing Certificates should be configured individually for each provider.

Security > Issuer Certificate

- Click the *Create Certificate Request* link
- On the **Certificate Request** page
  - Select the **Issuer** or **Issuer Group** from the drop down list
  - Select the required **Provider** from the drop down list
  - Fill the remaining fields as appropriate
  - Click the **Apply** button.
- **Certificate Signing Request** (CSR) – Copy the contents of the CSR or click the **Download** button to save the CSR.

Sign the Certificate Signing Request (CSR)

- Sign the Certificate Signing Request (CSR) using a Certificate Authority.

Install the Certificate Request

Security > Issuer Certificate

- Click the *Install Certificate* link
- Select the **Issuer** or **Issuer Group** from the drop down list

- Select the required **Provider** from the drop down list (This must be the same as the provider selected for the Certificate Request in Section 5.1 - Configure Issuer Group Signing Certificates)
- Click the **Choose File** button to locate and select the **Signed Certificate** file or click the **Certificate content** radio button and paste the Signed Certificate content
- Click the **Apply** button
- Ensure that it is completed successfully.

Cards

This section covers configurations related to *3DS1 only*.

Add a New Card

Users > New Card

- Select **Issuer** from the drop down list
- Select the **Authentication method** from the drop down list (This should correspond to the card provider)
- Ensure **Status** is set to **Enabled**
- Enter the **Card number**
- Enter the cardholder name in **Name on card**
- Enter the **Expiry date**
- Set the **Internet PIN.** This will be used during Activation During Shopping when registering the Pre-registered card)
- Click the **Apply** button.

Note

Cards can also be uploaded in bulk through ActiveAccess Registration Requests and the GPayments Card Loader application. Refer to the ActiveAccess documentation, ActiveAccess Administration and GPayments Card Loader and Signer/Verification Application, for further information.

Configure Custom Pages

Upload Local Custom Pages

Issuers > Custom Pages

- Select the **Issuer** or **Issuer Group** radio button and select from the drop down list
- If matches are found, custom pages have previously been set up for this issuer, in which case go to Section 8 - Authentication Scenarios Setup
- If no matches are found, click the *Upload File* link
- Use the **Choose File** button to locate and upload the *Authentication.zip* file from the following path in ActiveAccess installation package: ActiveAccess/data/custompage/issuer/Any Bank

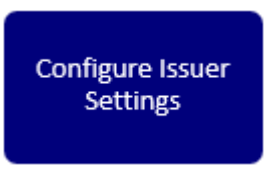
> **Note**
>
> You can customise the XSL pages as appropriate. Note that different custom pages are used for local and remote issuers.

- Click the **Apply** button.

Authentication Scenarios Setup

Each authentication scenario covered in this section should be set up and tested independently, *using a newly created card*, as individual scenarios may require a different configuration within the same issuer.

Activation During Shopping (ADS) Scenario



Configure Issuer Settings

Issuer > Settings

- Select the **Issuer** from the drop down list
- Set **Activation During Shopping** to **Enabled** for all requested/configured card providers
- Click the **Apply** button.

Perform a Test Transaction

- Go to Section 9 - Perform a Test Transaction.

Authentication Success Scenario

Configure Issuer Settings

Issuer > Settings

- Select the **Issuer** from the drop down list
- Set **Activation During Shopping** to **Enabled** for all requested/configured card providers
- Click the **Apply** button.

Register the Pre-Registered Card

Perform a test transaction with the card to register the card through Activation During Shopping (ADS). If you have access to the GPayments MPI (ActiveMerchant), follow the steps below.

ActiveMerchant Test Payment Page

- Go to the ActiveMerchant Test Payment page to register a newly created card set up in Section 6 - Configure Card Numbers
- Enter the **Card number** to perform a test transaction
- Click the **Submit** button
- On the confirmation page, click the **Submit** button

- On the registration page, enter **Name on Card** and **Internet Pin**, which were set up in Section 6 - Configure Card Numbers
- Click the **Submit / Activate** button
- Enter a **Personal Assurance Message**
- Set a **Password** to be used for authenticating the cardholder
- Click the **Submit** button
- On the next page, click the **Continue / OK** button to go to the Success page.

PERFORM A TEST TRANSACTION

- Go to Section 9 - Perform a Test Transaction.

Authentication Fail Scenario

Configure Issuer Settings

Issuer > Settings

- Select **Issuer** from the drop down list
- Set **Activation During Shopping** to **Enabled** for all requested/configured card providers
- Set an appropriate value for **Maximum unsuccessful attempts**. As the card will need to be locked for this scenario (Section 8.3.3 - Lock the Card), it is preferable to set a lower value, e.g. 3. Do not set the value to 0 (disable).
- Set **Automatic unlock** to 0 (disabled)

> **Note**
>
> Perform this step only if you would like the cards of this issuer to stay locked and provide results for the authentication failed scenario each time.

- Click the **Apply** button.

Register the Pre-Registered Card

Perform a test transaction with the card, to register the card through Activation During Shopping (ADS). If you have access to the GPayments MPI (ActiveMerchant), follow the steps below.

ActiveMerchant Test Payment Page

- Go to the ActiveMerchant Test Payment Page to register the card set up in Section 6 - Configure Card Numbers
- Enter the **Card number** to perform a test transaction
- Click the **Submit** button
- On the confirmation page, click the **Submit** button
- On the registration page, enter **Name on Card** and **Internet Pin** which were set in Section 6 - Configure Card Numbers
- Click the **Submit** button
- Enter a **Personal Assurance Message**
- Set a **Password** to be used for authenticating the cardholder
- Click the **Submit** button
- On the next page, click the **Continue / OK** button to go to the Success page.

Lock the Card

To lock the card, perform a test transaction with the card, entering an incorrect password until the card is locked. If you have access to the GPayments MPI (ActiveMerchant), follow the steps below.

ActiveMerchant Test Payment Page

- Go to the ActiveMerchant Test Payment page
- Enter the **Card number** to perform a test transaction
- Click the **Submit** button
- On the confirmation page, click the **Submit** button
- On the authentication page, enter an incorrect password. Repeat, until the message *This Account is Locked!* is displayed.
- Click the **OK** button.

Perform a Test Transaction

- Go to Section 9 - Perform a Test Transaction.

Forgot Password Scenario

Configure Issuer Settings

System Management > Issuer Management

- Find the issuer and click the *Issuer Name* to go to the **Issuer Details** page
- Set **Show extended account information** to **Yes** for Question and Answer fields be shown on **Card Details** page
- Click the **Apply** button.

Issuer > Settings

- Select the **Issuer** from the drop down list
- Set **Activation During Shopping** to **Enabled** for all requested/configured card providers
- Click the **Apply** button.

Register the Pre-Registered Card

To register the card through Activation During Shopping (ADS), perform a test transaction with the card. If you have access to the GPayments MPI (ActiveMerchant), follow the steps below.

ActiveMerchant Test Payment Page

- Go to the ActiveMerchant Test Payment page to register the card set up in Section 6 - Configure Card Numbers
- Enter the **Card number** to perform a test transaction
- Click the **Submit** button
- On the confirmation page, click the **Submit** button

- On the registration page, enter **Name on Card** and **Internet Pin** which were set in Section 6 - Configure Card Numbers
- Click the **Submit** button
- Enter a **Personal Assurance Message**
- Set a **Password** to be used for authenticating the cardholder
- Click the **Submit** button
- On the next page, click the **Continue / OK** button to go to the Success page.

Configure Question & Answer

Users > Find Card > Card Details

- Enter a **Question** and an **Answer**
- Click the **Apply** button.

Perform a Test Transaction

- Go to Section 9 - Perform a Test Transaction. During the transaction, click on the "Forgot your Password?" link.

Proof of Attempt Scenario

Configure Issuer Settings

Issuer > Settings

- Select **Issuer** from the drop down list
- Set **Activation During Shopping** to **Disabled** for all requested/configured card providers
- Set **Proof of Authentication Attempt** to **Enabled** for all requested/configured card providers
- Click the **Apply** button.

Perform a Test Transaction

- Go to Section 9 - Perform a Test Transaction.

PAN Not Enrolled Scenario

Configure Issuer Settings

Issuers > Settings

- Select **Issuer** from the drop down list
- Set **Activation During Shopping** to **Disabled** for all requested/configured card providers
- Set **Proof of Authentication Attempt** to **Disabled** for all requested/configured card providers
- Click the **Apply** button.

Perform a Test Transaction

- Go to Section 9 - Perform a Test Transaction.

Delay / Timeout Scenario

You can test scenarios such as delay or timeout in Verify Enrolment or Payer Authentication processes.

You can create a **responseTimeout.properties** file in ActiveAccess' **AA_HOME** directory. This configuration file can be used for testing purposes only and under no circumstances should be used in a real production environment. The properties in this configuration file should be in the following general format:

- **BIN.reqType**=waiting time (milliseconds)
- **BIN**: is the issuer specified BIN number for which you would like to cause a delay in the response to card numbers that match the BIN.
- **reqType (VE or PA)**: is the type of the request for which you would like to cause a given amount of delay. VE and PA stand for Verify Enrolment and Payer Authentication requests respectively.
- **Waiting time**: The delay in milliseconds that you would like to cause in the response of VE or PA requests.

To set a VE response delay, it is recommended that it is greater than the VERES time-out defined by the MPI.

To set PA response delay, it is recommended that it is greater than the PARes time-out defined by the MPI

Info

0 means unlimited

Example

412345.VE=15000

512345.PA=20000

341234.VE=0

ActiveAccess server should be restarted for changes to take effect.

Perform a Test Transaction

After configuring each of the authentication scenarios, perform a test transaction with the card. If you have access to the GPayments MPI (ActiveMerchant), follow the steps below.

ActiveMerchant Test Payment Page (3-D Secure 1)

- Go to the ActiveMerchant Test Payment page
- Enter the **Card number** to perform a test transaction
- Click the **Submit** button
- Ensure that the outcome corresponds with the authentication scenario.

Devices

This section covers the configuration of licenses and BINs to enable the use of devices for authentication. Examples of some common devices have been included below.

Note that when device configuration is complete, devices can be assigned to individual cards during transactions or via ActiveAccess Administration in Users > Find Cards > Card Details > Assigned Devices > Device Management.

Configure License and BINs

Request and Update License

For issuers to be device compatible, a license needs to be issued with ActiveDevice support.

ActiveAccess License

- Contact GPayments and request for a license key with ActiveDevice support for the issuer
- Copy the license key provided to you by GPayments to your clipboard

System Management > Issuer Management

- Find the issuer and click the *Issuer Name*
- On the **Issuer Details** page, paste the copied **License Key** into the text box
- Click the **Apply** button.

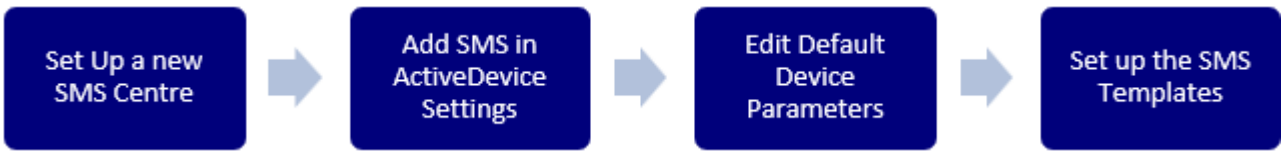
> **Note**
>
> If an error occurs, contact GPayments Tech Support.

Enable Device over 3-D Secure for BINs

System Management > Issuer Management > Issuer Details > BIN Management

- If the BIN has been created previously and has **Device over 3-D Secure** set to **Disabled**, follow the steps below:
  - Click on the *BIN* to go to the **BIN Details** page
  - Set **Device over 3-D Secure** to **Enabled**
  - Click the **Apply** button.
- If new BINs are being created, follow the steps below:
  - Click the *Add BIN* link
  - On the **Add BIN** page, enter the **BIN** (e.g. 412345)
  - Ensure **Status** is set to **Enabled**
  - Set **Device over 3-D Secure** to **Enabled**
  - Click the **Apply** button.

SMS



Set up a New SMS Centre

System Management > Device Management > Edit Default Device Parameters > Device Type: SMS > SMS Centres > New SMS Centre

- Enter a **Name** for the SMS centre
- Enter the **Domain/IP** of the SMS centre
- Enter the **Port** number of the SMS centre
- Enter **System ID**, **System type** and **Password**, if required
- Enter **Sender's mobile number**
- Click the **Apply** button.

Add SMS in ActiveDevice Settings

System Management > Issuer Management > Issuer Details > ActiveDevice Settings

- Under **Supported devices**, in the **Available** box, select SMS and click the **Add >>** button.
- Click the **Apply** button.

Edit Default Device Parameters

System Management > Device Management > Edit Default Device Parameters

- Select **SMS** from the **Device type** drop down list
- Update the device parameters as appropriate
- Click the **Apply** button.

Email

Add Email in ActiveDevice Settings

System Management > Issuer Management > Issuer Details > ActiveDevice Settings

- Under **Supported devices**, in the **Available** box, select Email and click the **Add >>** button.
- Click the **Apply** button.

Edit Device Parameters

System Management > Issuer Management > Issuer Details > ActiveDevice Settings > Device parameters

- Select **Email** from the **Device type** drop down list
- Untick **Use device's default parameters**
- Update the device parameters as appropriate
- Click the **Apply** button.

Set up Email Templates

System Management > Issuer Management > Issuer Details > ActiveDevice Settings > Device parameters > Device Type: Email > Email Templates

- Select a **Template name** from the drop down list
- Adjust the template as required using the **Template** textbox and check the **Preview** textbox for **Plain Context type** or click *Send Test Email* for **HTML Context type**.
- Click the **Apply** button.

> **Note**
>
> The settings and templates configured in **10.3.2 Edit Device Parameters** and **10.3.3 Set up Email Templates** will apply to the specific issuer only. To set default device parameters and templates that apply to all issuers, go to **System Management > Device Management > Edit Default Device Parameters**. The default configurations will apply to all issuers, unless **Use device's default parameters** is unticked in the issuer's device configurations.

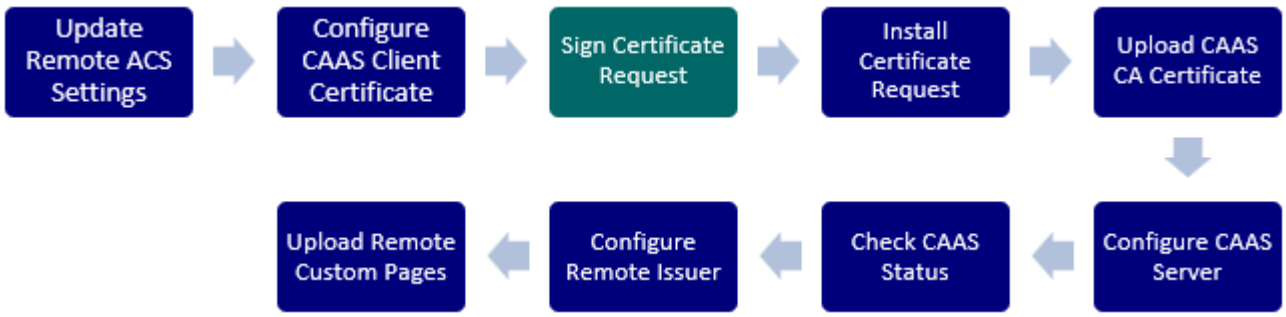
VASCO

Upload the VASCO File

System Management > Device Management > Upload File

- Select the Issuer from the **Issuer** drop down list
- Select **VASCO** from the **Device type** drop down list
- Click the **Choose File** button to locate and select the appropriate VASCO file
- Enter the **Key value**
- Set up a **Schedule** as required
- Click the **Apply** button.

Remote/External Authentication



- Before commencing remote authentication setup, make sure that the required Web services have been implemented and that the CAAS server is up and running.

Update Remote ACS Settings

System Management > ACS Settings > Authentication server: Remote (CAAS)

- Enter the **ACS URL** (e.g. https://yourserverip:port/acs/pa)
- Click the **Apply** button.

Configure CAAS Client Certificate

Security > CAAS Certificate

- Click the *Create Certificate Request* link
- On the **CAAS Certificate Request** page:
  - Enter the certificate details, as appropriate
  - Click the **Apply** button.
- Certificate Request – Copy the certificate contents or click the **Download** button to save the certificate request.

Sign Certificate Request

- Sign the Certificate Request using a Certificate Authority.

Install Certificate Request

Security > CAAS Certificate

- Click the *Install Certificate* link
- Use the **Choose File** button to locate and select the **Signed Certificate** file or click the **Certificate content** radio button and paste the Signed Certificate content.
- Click the **Apply** button.

Upload CAAS CA Certificate

Security > CA Certificate

- Click the *Import CA Certificate* link
- Select **CAAS client** from the **Provider** drop down list
- Click the **Choose File** button to locate and select the **CA Certificate** file
- Click the **Import** button.

Configure CAAS Server

Servers > CAAS Servers

- Click the *Add CAAS Server* link
- On the **Add CAAS Server** page:
  - Enter **CAAS URL** of the CAAS server
  - Enter a value for **CAAS Connection timeout**
  - Enter a value for **Maximum SMS request**
  - Fill the remaining fields as appropriate
  - Click the **Add** button.

Check CAAS Status

Servers > CAAS Servers

- Click the *CAAS URL* link
- On the **Edit CAAS Server** page, click the *Check CAAS Status* link

- On the **Check CAAS Status** page, ensure the message displayed indicates that CAAS is up and running.

Configure Remote Issuer

System Management > Issuer Management

- Find the issuer and click the *Issuer Name*
- If the issuer does not exist, refer to Section 4 - Issuer Group and Issuer Setup to configure issuer, license and BIN and then continue with the next step, otherwise click the *Issuer Name* link
- On the **Issuer Details** page:
  - Set **Authentication server** to **Remote (CAAS)**
  - Select the URL of the **CAAS Server** from the drop down list
  - Click the **Apply** button.

Upload Remote Custom Pages

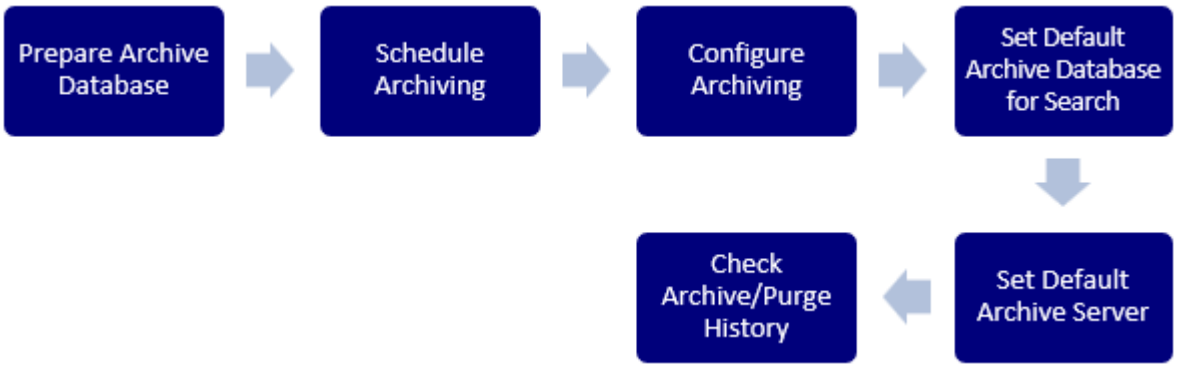
Issuers > Custom Pages

- Select the **Issuer** or **Group** radio button and select from the drop down list
- Click the *Upload File* link
- Use the **Choose File** button to locate and upload the *Authentication.zip* file from the following path in ActiveAccess installation package: ActiveAccess/data/custompage/issuer/AnyBank_Remote

> **Note**
>
> You can customise the XSL pages as appropriate. Note that custom pages are different for local and remote issuers.

- Click the **Apply** button.

Database Archiving



Prepare Archive Database

- Create a new database user with the appropriate permissions
- Connect to the database user and run *archive_schema.sql* from the **Archive** folder in ActiveAccess installation package.
- To give access to the current ActiveAccess database user
- In the *archive_grant.sql* from the **Archive** folder in ActiveAccess installation package, replace the tags **< archiveusername >** with the newly created database user for archiving, **< dbname >** with the database owner name, and **< dbuser >** with the database user name that accesses the database. In a simple configuration the database user name may be the same as the database owner name.

> **Note**
>
> The < dbname > and < dbuser > can be found in **AA_HOME/activeaccess.properties** as **DBNAME** and **DBUSERNAME** respectively.

- Run the updated **archive_grant.sql** with a sys/system connection.

Schedule Archiving

System Management > Archive Management

- Click the *Edit* link
- Tick the **Automatic archive** checkbox to enable automatic archiving
- Fill the remaining fields as appropriate

- For purging the archived data:
  - Tick the **Automatic archive purge** checkbox to enable automatic archiving
  - Fill the remaining fields as appropriate
- Click the **Apply** button.

Configure Archiving

System Management > Archive Management > Archive Databases > New Archive Database

- Enter the **Archive Database link** or **Database user**
- Click the **Apply** button.

Set Default Archive Database for Search

System Management > Archive Management > Archive Databases

- If you only have one archive database configured, it will automatically be set as the default for search. If you have more than one archive database configured, click the *Set as default for search* link for the desired archive database.

Set Default Archive Server

Servers > MIA Servers

- Click the *Set as default archive server* link for the desired MIA Server.

Check Archive/Purge History

System Management > Archive Management > Archive Databases

- Click the *Archive database* link to go to the **Archive Database Details** page

  A list of archive and purge history reports will appear under **Archive History** and **Purge History** tabs

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.
Visa Secure		A program developed by Visa to make online payments more secure through 3-D Secure 2.

Document Control

new item item changed item removed no change to item

Date	AA Ver	Doc Ver	Change Details
[30/07/2021]	9.0.0	9.0.0:1	**Product Architecture** (Installation Guide) Added **Payer Authentication Server**, **Decoupled Authentication Adapter** **Whitelisting Server** in Internal Components Changed **Authentication Server (3DS2)** and **Challenge Server (3DS2)** in I Components Changed Logical view of ActiveAccess diagram.
			External Components (Installation Guide) Changed the SQL commands in Find Transactions Performance Added **OOB** and **Decoupled Authentication** in Two-Factor Authentication
			Installation (Installation Guide) Removed **AA_Administration**, **MIA_DB_DESede** key aliases, and **the issu alias (e.g.** `Card< Issuer_ID >` **)** in Prerequisites and Installation of Individua Components Added new step for removing **enrolment.war** in Upgrades Added **Whitelisting** in Deploying WAR packages and Installation of Indivi Components Added an **important notice** in Post Installation Added Whitelist Server Removed **Module** in Additional Administration Server Configuration Para
			About the Issuer Administration Server (Admin UI) Added **Note** in Login.
			Settings (Admin UI) Added **Whitelisting server URL** in Settings.

Date	AA Ver	Doc Ver	Change Details
			System Management (Admin UI) Added **Visa CEMEA region** in New Issuer Group, Issuer Group Details Added notes in Issuer Details Changed notes in Issuer Details Added **Whitelisting** in BIN Management Added **Decoupled Authenticator** in Edit Device Parameters.
			About Authentication Management (Admin UI) Added **Decoupled Authenticator Management** to **About Authentication Management**.
			Device Management (Admin UI) Removed all instances of **CAP** and **RSA** device types.
			Risk Management (Admin UI) Added **Adapter ID** and **Generate** in Register Risk Adapter.
			OOB Management (Admin UI) Added **Adapter ID** and **Generate** in Register / Edit OOB Adapter.
			Decoupled Authenticator Management (Admin UI) Added new page: Decoupled Authenticator Management.
			Security (Admin UI) Added new section: Decoupled Authenticator Certificate.
			Migrate to Data Key Utility (Admin UI) Added new page: Migrate to Data Key Utility.
			Issuers (Admin UI) Added **Name on card verification** in Local Issuer Settings Added **ACS Reference Number** in Provider Settings Added displayed key details for **General keys** in Key Management Changed **Info** in New Key.

Date	AA Ver	Doc Ver	Change Details
			Cards (Admin UI) Added **Decoupled Authenticator** in Find Card Added **Whitelisting** in Cards Details Added new section: Whitelisting Removed sections: **Find User** and **New User** in Cards.
			Transactions (Admin UI) Changed **3-D Secure version** in Search Fields Added **Frictionless by review** in Transaction Details Removed section: **Find ActiveDevice** in Transactions.
			Reports (Admin UI) Added **Decoupled Authenticator** in Card Summary Added new section: Device Summary Removed sections: **User Summary**, **User Authentication**, **User Activity** ar **Enrolment Activity** in Reports.
			SMS via JMS Messaging (Specifications) Changed **Tag** of **message_payload** in Optional Parameters.
			Out of Band (OOB) Authentication Adapter (Specifications) Added **threeDSRequestorAppURL**, **callbackUrl** and **instruction** to Out of E (OOB) Authentication Adapter.
			Codes (Transaction Status Codes) Added new conditions in Transaction Status Codes.
			Codes (RReq Authentication Method Codes) Added **11 = PUSH CONFIRMATION** in RReq Authentication Method Code
			Removed all instances of **ActiveDevice/User Authentication** Removed all instances of **Enrolment Server** Removed all instances of **CAP** and **RSA** device types.
[17/06/2021]	**8.5.8**	**8.5.8:1**	**External Components** (Installation Guide) Added note regarding Tomcat 7 in Application Server

Date	AA Ver	Doc Ver	Change Details
			Installation (Installation Guide) Added new configuration parameter **AMOUNT_FORMATTER** in Common Configuration Parameters
			Issuers (Admin UI) Added note in Upload Registration Files
			Cards (Admin UI) Added note in New SMS Device
			Local Messaging (Specifications) Added acceptable values for **Status** in Update Registration Request.
[30/04/2021]	**8.5.6**	**8.5.6:1**	**SMS via JMS Messaging** (Specifications) Added **Tag** and **Size** columns in Optional Parameters Changed all values in **Type** column in Optional Parameters Added new field names in Optional Parameters Added examples for **CLIENTID** in Examples.
[05/02/2021]	**8.5.3**	**8.5.3:1**	**Installation** (Installation Guide) Added **WS_POOL** to ActiveAccess Configuration File.
18/12/2020	**8.5.0**	**8.5.0:1**	**Product Architecture** (Installation Guide) Added **Oracle WebLogic Server 14c** and **Database Oracle 19c** in Hardwa Software Requirements.
			External Components (Installation Guide) Added additional steps for Oracle 19c in Oracle Database.
			Installation (Installation Guide) Changes made to Prerequisites Added installation steps for Upgrades to v8.5.x and later Added new configuration parameters **MASTER_HSM_LIB_DIR** and **MASTER_HSM_SLOT** to Common Configuration Parameters Changes made to Installation of Individual Components.
			Risk Management (Admin UI) Added details about authentication method and **Score range for frictionl review** in Add/Edit Risk Chain.

Date	AA Ver	Doc Ver	Change Details
			Servers (Admin UI) Added new section Edit ACS Server.
			Key Retiring Utility (Admin UI) Changes made to Retiring keys automatically.
			Issuers (Admin UI) Changes made to the description of Key Management Added **Export**, **KeyStore type** and a note for **Delete** to Key Management Added **HMAC keys** and an **Info** box to New Key Added **Export** and **KeyStore type** to Key Management Added **KeyStore type** to Key Details Removed **New Key** link from Key Details Added new section Export Data Key.
			Remote Messaging (Specifications) Added **purchaseDate** to **OobInfo** in Table 14 - InitAuthReq Added item 6 to **Code** in Table 17 - VerifyAuth.
			Out of Band (OOB) Authentication Adapter (Specifications) Added **NOT_AUTHENTICATED_END** to OobAuthenticationResult Data Ele
			Risk Engine Adapter (Specifications) Added **frictionless with review** in How RBA works.
[25/11/2020]	**8.4.4**	**8.4.4:1**	**Remote Messaging** (Specifications) Added **Attributes** and **Descriptions** to Table 4 - Transaction, Table 10 - PreAuthReq, Table 11 - HeaderParams and Table 12 - AdditionalParams.
[29/10/2020]	**8.4.1**	**8.4.1:1**	**System Management** (ACS URL) Added details to **ACS challenge URL** for OOB's WebSocket and callback U 3-D Secure 2 Settings.
			System Management (Issuer Management) Added a note to **ACS Challenge URL** for OOB's WebSocket and callback U New Issuer Group, Issuer Group Details and Issuer Details.
			Remote Messaging (Specifications) Added notes to AuthType and AuthTypeSup at Table 6 - CardInfo.

Date	AA Ver	Doc Ver	Change Details
			Codes (RReq Authentication Method Codes) Added new page: RReq Authentication Method Codes.
[16/10/2020]	**8.4.0**	**8.4.0:1**	**Settings** (Admin UI) Added a note to **Log level** in Settings.
			Issuer Management (Admin UI) Added **Verified by Visa CAVV format** and **Visa Secure CAVV format** to N Issuer Group and Issuer Details Added **IAV generation algorithm**, **Verified by Visa CAVV format** and **Visa CAVV format** to Issuer Group Details Added **ACS URL** to New Issuer.
			Issuers (Admin UI) Added a note to Custom pages.
			Transactions (Admin UI) Added **Failed reason** and **IAV generation algorithm** to Transaction Detail
			Remote Messaging (Specifications) Added **callBack** to Table 14 - InitAuthReq.
			Out of Band (OOB) Authentication Adapter (Specifications) Added **purchaseDate** to TransactionInfo Data Elements.
29/05/2020	**8.3.0**	**8.3.0:1**	**Installation** (Installation Guide) Added an option to change **RMI port** in Additional Administration Server Configuration Parameters.
			Issuer Management (Admin UI) Added **IAV generation algorithm** to New Issuer Group Added a warning to **Supported devices** in ActiveDevice Settings.
			Device Management (Admin UI) Added **OOB** to Edit Default Device Parameters and OOB.
			Risk Management (Admin UI) Added Upload Connector Encryption Key.

Date	AA Ver	Doc Ver	Change Details
			OOB Management (Admin UI) ➕ Added Upload Connector Encryption Key.
			Cards (Admin UI) ➕ Added **Deactivated device type** to **Status** in Assigned Devices.
			CardLoader (Specifications) ➕ Added encryption of sensitive data to **Log directory** in Open dialog for se XML file to verify.
			Remote Messaging (Specifications) ➕ Added **acsTransId**, **threeDSTransId** and **dsTransId** to Table 4 - Transactic
			Out of Band (OOB) Authentication Adapter (Specifications) ➕ Added samples to Get OOB Adapter Information and Request OOB Challe ➕ Added new **Length** for `acctNumber` in TransactionInfo Data Elements an `cardholderName` in CardHolderInfo Data Elements ➕ Added **Message Inclusion** for `clientId` and `deviceId` in AdditionalInfo Elements.
			Risk Engine Adapter (Specifications) ➕ Added **AReqWithTransStatus Data Elements** ➕ Added new **Length** for `acctNumber` and `cardholderName` in AReq Data E ➕ Added **Message Inclusion** for `clientId` in AdditionalInfo Data Elements
24/04/2020	**8.2.3**	**8.2.3:1**	**Risk Engine Adapter** (Specifications) 🔺 Changes made to **Parameter Data Elements** 🔺 Change made to **Condition Data Elements** ➕ Added **ValueType Data Elements**, **ConditionAssessor Data Elements**, an **TxCallback Data Elements** 🔺 Changes made to **ConditionValue Data Elements** ➕ Added **Range Data Elements** 🔺 Change made to **messageExtension Data Elements** ❌ Removed **AdapterRiskAssessmentOutput Data Elements**.
17/4/2020	**8.2.0**	**8.2.0:2**	**Remote Messaging** (Specifications) ➕ Added attribute lengths to the **Usage** column of Table 2 - VerifyRegReq, T Card, Table 4 - Transaction and Table 14 - InitAuthReq.

Date	AA Ver	Doc Ver	Change Details
			Out of Band (OOB) Authentication Adapter (Specifications) Changes made to **Out of Band (OOB) Authentication Adapter** (Specificat
28/02/2020	**8.2.0**	**8.2.0:1**	**Installation** (Installation Guide) Added **TOMCAT_KEYSTORE**, **TOMCAT_KEYSTORE_PASS**, **TOMCAT_TRUSTSTORE** and **TOMCAT_TRUSTSTORE_PASS** to configuratior
			Issuer Management (Admin UI) Added **IAV generation algorithm** to Issuer Details.
			Risk Management (Admin UI) Change made to **Score range for device** in Add / Edit Risk Chain.
			Servers (Admin UI) Added **OOB info template** to Edit CAAS Server.
			Issuers (Admin UI) Added **Maximum interaction** to Remote Issuer Settings.
			Cards (Admin UI) Added **Client ID** to Find Card and Card Details Added note to **Expiry date** in New Card and Card Details.
			Transactions (Admin UI) Added **Client ID** to Find 3-D Secure Added **Risk decision** and **Client ID** to Transaction Details.
			Local Messaging (Specifications) Additions & changes made for **Client ID** to: Sample pre-registration request Sample final registration request for traditional 3-D Secure Sample final registration request for two-factor authentication over 3-D S Sample update registration request Card Device Update Request Sample Registration Notification Sample Device Update Notification Sample Opt-Out Notification Sample Lock Notification Cardholder Registration DTD.

Date	AA Ver	Doc Ver	Change Details
			Remote Messaging (Specifications) ➕ Added **LanCode** to Table 3 - Card and Table 6 - CardInfo ➕ Added **twoFA** to Table 6 - CardInfo.
			Out of Band (OOB) Authentication Adapter (Specifications) 🔺 Changes made to Adapter Interface Methods 🔺 Change made to **Response Description** of Get OOB Adapter information 🔺 Change made to **Response Description** of Request OOB Challenge 🔺 Change made to **Request Method** and **Response Description** of Get OOB authentication result ➕ Added AdapterInfo Data Elements 🔺 Change made to `acctNumber` **Description** in TransactionInfo Data Eleme ➕ Added `deviceId` to AdditionalInfo Data Elements ➕ OobRequestChallengeResult Data Elements added ➕ OobAuthenticationResult Data Elements added.
10/01/2020	**8.1.2**	**8.1.2:1**	**Installation** (Installation Guide) ➕ Added **JSON Response Elements** in ACS, MIA, Registration and Enrolmer
			Profile Management (Admin UI) 🔺 Change made to **2-factor authentication** login option in User Profile.
			Remote Messaging (Specifications) 🔺 Change made to **Description** and **Sample Value** of **AuthType** in Pre Authentication Response.
			Local Messaging (Specifications) 🔺 Changes made to **Request** and **Response** of **Cardholder Registration** 🔺 Changes made to **Request** and **Response** of **Notification** 🔺 Changes made to **Critical Card Data Encryption and Decryption** 🔺 Changes made to **Cardholder Registration** 🔺 Changes made to **Notification**.
06/12/2019	**8.1.1**	**8.1.1:1**	**Installation** (Installation Guide) ➕ Added monitoring of the availability of ACS, MIA, Registration and Enrolr
			Device Management (Admin UI) ➕ Added `Plus (+) prefix` in SMS Center.

Date	AA Ver	Doc Ver	Change Details
			Issuers (Admin UI) Change made to Language selection during authentication: add *authenti* *process of 3-D Secure 1* Change made to Provider Settings: add JSON format examples.
			Local Messaging (Specifications) Change made to Request: Update EncVectorIV Update Sample final registration request for traditional 3-D Secure Change made to Cancel Registration Request: Make name attribute of ca optional Change made to Critical Card Data Encryption and Decryption: Change ke algorithm to AES Change made to Cardholder Registration DTD: Change `Name CDATA` to `I`
			Out of Band (OOB) Authentication Adapter (Specifications) Added `Swagger API URL` to Restful API version of OOB Adapter.
			Risk Engine Adapter (Specifications) Added `Swagger API URL` to RESTful API Risk Adapter.
			Codes (Error Codes) Added Error codes to Server Error Codes.
15/11/2019	**8.1.0**	**8.1.0:1**	**Installation** (Installation Guide) Removed **HSM_LIB_DIR** parameter from Upgrades to v8.x.x.
			System Management (Admin UI) Change made to New Issuer Group, Issuer Group Details, and Issuer Deta Changes `MAC Algorithm` to **3DS1 only** and changed `Use parent certifica` `public and encryption keys`. Change made to Public & Encryption Key Management: Change key algo **AES**.
			Security (Admin UI) Added new section: SDK certificate.
			Cards (Admin UI) Change made to New Card: The card Expiry date is mandatory for Maste

Date	AA Ver	Doc Ver	Change Details
			Risk Engine Adapter (Specifications) Removed one method of `TxCallback` from Parameter Data Elements. Removed `resultWhenTransmissionError` from RemoteCondition Data E Added `range` field into ConditionValue Data Elements
06/11/2019	**8.0.3**	**8.0.3:1**	**Risk Engine Adapter** (Specifications) Change made to AdapterInfo Data Elements: Removed round brackets fr **Token** Sample Value. Change made to AssessmentResult Data Elements: Change the descripti `whatToDoNext` `range` field added into ConditionValue Data Elements
09/10/2019	**8.0.2**	**8.0.2:2**	**Remote Messaging** (Specifications) Change made to Table 16 - VerifyAuthReq: Removed round brackets from **Token** Sample Value.
			Out of Band (OOB) Authentication Adapter (Specifications) Change made to **oobAuthenticationResult**: Add `PENDING` as a valid value
			Risk Engine Adapter (Specifications) Changed **Risk chain setup diagram**.
02/10/2019	**8.0.2**	**8.0.2:1**	**Installation** (Installation Guide) Changes made to Upgrades to v8.x.x: Addition of **HSM_LIB_DIR** paramet updates to JAR files which must be removed. Addition of **HSM_LIB_DIR**, **HSM_SLOT**, **TESTING_MODE**, **PROVIDER_TES TEST_AUTH_SERVER**, and **ACS_REFERENCE_NUMBER_TEST** to Common configuration parameters.
			Remote Messaging (Specifications) Added **Response code = 3**.
			Codes (Transaction Status Codes) Added new page: Transaction Status Codes.
05/09/2019	**8.0.1**	**8.0.1:1**	**Product Architecture** (Installation Guide) Added Disaster Recovery and Clustering diagrams.
			Installation (Installation Guide) Changes made to Upgrades to v8.0.x and New installations.

Date	AA Ver	Doc Ver	Change Details
			Security (Admin UI) Added new **Key type** field to Create Certificate Request.
			Risk Engine Adapter (Specifications) Changed **Validator** field description in **ParameterDataElements** Chenged **PreviousData** field format in **RemoteAssessmentRequest Data Elements** Added **AReqWithTransStatusDataElements** Changed **ThreeDSCompInd** and **ThreeDSRequestorAuthenticationInd** fie **AReq Data Elements**.
			Remote Messaging (Specifications) **InitAuthReq** table: Usage of **oobInfo** changed.
			Out of Band (OOB) Authentication Adapter (Specifications) Change the URL in **Restful API version of OOB Adapter** Change `NOT__AUTHENTICATED` to `NOT_AUTHENTICATED` Update MobilePhone Data Elements, HomePhone Data Elements, and W Data Elements.
15/08/2019	**8.0.0**	**8.0.0:1**	**Product Architecture** (Installation Guide) Components labelled with (3DS1) or (3DS2) as relevant Added Challenge Server (3DS2). Added Risk Engine Adapter Added Out of Band (OOB) Authentication Adapter Changed Logical view of ActiveAccess diagram Changed Hardware and Software Requirements Removed references to **RuPay** components.
			External Components (Installation Guide) Application Server dependency removed, supports compatible Java Appl Servers.
			Installation (Installation Guide) ActiveAccess installation and setup process simplified.

Date	AA Ver	Doc Ver	Change Details
			System Management (Admin UI) **Authentication Management** section added with tabs for: Device Management previously under **System Management** Risk Management for 3DS2 risk management OOB Management for OOB processing support.
			System Management (Admin UI) - **Issuer Management** Device Settings: Added **OOB** as a supported device.
			Security (Admin UI) Added Directory Server Certificate section Added OOB Certificate section Added Risk Certificate section.
			Issuers (Admin UI) Providers parameters moved to a new page, and linked, from the **Setting** New fields added.
			Rules (Admin UI) Rule Management section replaces previous ***Authentication Exemption*** a ***Registration*** sections Tabs for: Registration previously ***Force Registration*** tab under **Rules** Authentication previously ***Authentication Exemption*** tab under **Rules** Settings.
			Cards (Admin UI) **Users** tab renamed to **Cards**.
			Reports (Admin UI) Reports support reporting by 3-D Secure version.
			Transactions (Admin UI) **Find 3-D Secure**: supports search by 3-D Secure version. New fields adde
			Admins (Admin UI) Admin User Details and User Profile: added **2-factor authentication** login

Date	AA Ver	Doc Ver	Change Details
			Local Messaging (Specifications) Changed Final Registration Request with OOB device registration request
			Remote Messaging (Specifications) Added **issuerName** and **theeDSProtocolVersion** in **Transaction** table Added **HeaderParams** table Added **AdditionalParams** table Added **AuthType** in **PreAuthResp** table Added new OTP types for **AuthType** and **oobInfo** in **InitAuthReq** table Sample Request Response: changed **CVD** to NULL.
			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 w printed. **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** Added **AuthType** in **initAuthReq** table Changed RegToken definition in **CardInfo** table.
06/07/2018	**7.4.0**	**7.4.0:1**	Addition of options in **System Management > Settings** to allow administ specified access levels to view Card Number (plaintext) and AAV/CAVV/AEV Changed 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	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 **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		Previously included in the ActiveAccess package
Legal Notices		AA12

Release Notes

ActiveAccess v9.0.0

[30/07/2021]

[EOL: Two years after the subsequent version's release date]

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#235		EMV 3DS 2.2: Whitelisting	Whitelisting Server
ENHANCEMENT	#317		Support for EMV 3D Secure 2.2	Issuer Administration, Access Control Server, Registration Server, Whitelisting Server
ENHANCEMENT	#381		EMV 3DS 2.2: Support for Decoupled Authentication, ARes.TransStatus=D	Access Control Server
ENHANCEMENT	#385		EMV 3DS 2.2: Support HTTP Protocol HTTP/1.1 and higher	Access Control Server
ENHANCEMENT	#386		EMV 3DS 2.2: Support Informational Request	Access Control Server
ENHANCEMENT	#442	#9320	Update ACS UI Data Elements	Access Control Server
ENHANCEMENT	#458		Deprecated features: ActiveDevice/User Authentication, Enrolment Server, Device types: CAP and RSA	Issuer Administration, Access Control Server, Registration Server, CardLoader

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#466		Mastercard Extension for RBA	Issuer Administration, Access Control Server
ENHANCEMENT	#473	#8958	EMV 3DS 2.2: Remove Continue button from OOB page - Local Issuer	Access Control Server
ENHANCEMENT	#474		EMV2.2: OOB authentication page content	Access Control Server
ENHANCEMENT	#501		EMV 3DS 2.2: Update shared key generation	Access Control Server
ENHANCEMENT	#507		Visa Secure: Support Authentication for Non-Payment Authentication	Access Control Server
ENHANCEMENT	#511	#9093	Implement general error pages	Issuer Administration
ENHANCEMENT	#526		Add option to configure cardholder name validation	Issuer Administration, Access Control Server, Registration Server
ENHANCEMENT	#573		Allow admin to enter adapterId when registering adapter	Issuer Administration
ENHANCEMENT	#577		Visa secure: using CAVV algorithm U3V7 update status	Issuer Administration, Access Control Server
ENHANCEMENT	#579	#9161	MasterCard: Acquirer Strong Consumer Authentication (SCA) Exemption support in ACS	Access Control Server
ENHANCEMENT	#590		Visa Secure: Support for 3RI payments	Access Control Server

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#592		Add option 3D Secure 2.2 in transaction search	Issuer Administration
ENHANCEMENT	#593		EMV 3DS 2.2: Reporting	Issuer Administration
ENHANCEMENT	#594		EMV2.2: Archive for new protocol version	Issuer Administration
ENHANCEMENT	#600		Visa Secure: Secure Corporate Payment (SCP)	Access Control Server
ENHANCEMENT	#607	#9022	SessionID logging	Access Control Server
ENHANCEMENT	#614		New Key Management and HSM connectivity - Phase II - Including Migrate to Data Key Utility	Issuer Administration, Access Control Server, Registration Server
ENHANCEMENT	#634		EMV 3DS 2.2: ThreeRI handling	Access Control Server
ENHANCEMENT	#684		Visa Secure: transStatusReason=21 no longer supported in VISA	Access Control Server
ENHANCEMENT	#653		Selecting CAVV/IAV algorithm in Issuer Groups	Issuer Administration
ENHANCEMENT	#662		EMV 3DS 2.2: Whitelisting API	Issuer Administration, Access Control Server, Registration Server
ENHANCEMENT	#669	#9043	Create New CAVV/AAV/SPA Key as Inactive	Issuer Administration

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#680	#9320	EMV 3DS 2.2: UI elements in CRes for SDK transactions	Access Control Server
ENHANCEMENT	#681		Support for Tomcat 9	Setup, Issuer Administration, Access Control Server, Registration Server, Whitelisting Server
ENHANCEMENT	#688	#9320	Support both portrait and landscape UI templates - Local Issuer	Access Control Server
ENHANCEMENT	#689	#9299	Dynamic Linking - SMS/Email OTP verification issue	Access Control Server
ENHANCEMENT	#696		Whitelisting API for audit logs	Whitelisting Server
ENHANCEMENT	#726	#9320	Support both portrait and landscape UI templates - Remote Issuer	Access Control Server
ENHANCEMENT	#798		EMV 3DS 2.2: EMVCo ReferenceNumber update	Setup
FIX	#337	#8044	Card registration flow - "Unable to assign device as it is not active"	Registration Server
FIX	#487	#9035	Errors after successful completion of 3DS2 transaction	Access Control Server
FIX	#524	#9108	Custom pages do not scale	Access Control Server
FIX	#615	#9208	Incorrect purchase date processing by ACS	Access Control Server
FIX	#616	#9184	Invalid procedure FIND_NESTED_VISA_CAVV_FORMAT	Setup

Type	Issue Number	External ID	Description	Components
FIX	#627	#9207	Authentication report bug: MIA Reports - Incorrect 3DS2 authentication data	Issuer Administration
FIX	#637		3DS2 archived transaction details	Issuer Administration
FIX	#730		Authentication with two SMS devices	Access Control Server
FIX	#731		Authenticate card with damaged/lost/ temporary disabled device	Access Control Server
FIX	#747	#9424	threeDSCompInd processing issue	Access Control Server
FIX			General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.5.10

[17/06/2021]

[EOL: 30/07/2023]

Type	Issue Number	External ID	Description	Components
FIX	#761	#9451	Error in MQ data processing for transactions where merchant name contains non-Latin letters	Access Control Server

ActiveAccess v8.5.9

[28/05/2021]

[EOL: 17/06/2023]

Type	Issue Number	External ID	Description	Components
FIX	#732	#9382	Data element not in the required format or value is invalid as defined	Access Control Server

ActiveAccess v8.5.8

[17/05/2021]

[EOL: 28/05/2023]

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#597	#9153	Change Display Amount Format for VND currency	Setup, Access Control Server
FIX	#676	#9313	Incorrect displaying sms parameters	Issuer Administration
FIX	#714	#9366	ACS: session expired	Access Control Server

ActiveAccess v8.5.7

[04/05/2021]

[EOL: 17/05/2023]

Type	Issue Number	External ID	Description	Components
FIX	#712	#9285	Issue in setting ClientId on queued SMS tokens	Access Control Server, Issuer Administration

ActiveAccess v8.5.6

[30/04/2021]

[EOL: 04/05/2023]

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#682	#9285	ClientID parameter in SMS via JMS	Access Control Server
FIX	#608	#9346	Element 'param' validation error	Access Control Server
FIX	#694	#9331	Successful authentication without CReq field in POST request	Access Control Server

ActiveAccess v8.5.5

[09/04/2021]

[EOL: 30/04/2023]

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#670	#9291	Visa Secure: Support Visa CEMEA Region CAVV generation for different transStatus values	Access Control Server
ENHANCEMENT	#678		EMV2.x: avoid padding in base64Url	Access Control Server
FIX	#672	#9291	Error generating CAVV value in 3DS1 transaction	Access Control Server
FIX	#673	#9298	Local 3DS1 authentication issue with OOB devices	Access Control Server

ActiveAccess v8.5.4

[02/03/2021]

[EOL: 09/04/2023]

Type	Issue Number	External ID	Description	Components
FIX	#641	Errors during functional test of the interaction between the OOB Server and ACS	Access Control Server	
FIX	#656	ACS start up issue with the new OpenJDK Vendor Name	Setup	
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server	

ActiveAccess v8.5.3

[05/02/2021]

[EOL: 02/03/2023]

Type	Issue Number	External ID	Description	Components
ENHANCEMENT	#645	Making thread pool size configurable	Access Control Server	
FIX	#626	Notification Report for current date	Registration Server	
FIX	#629	App-based authentication issue	Access Control Server	
FIX	#630	Incorrect value of $PurchaseDateTime in SMS messages	Access Control Server	
FIX	#632	EMV 3DS2.1 - Recurring transactions processing	Access Control Server	

ActiveAccess v8.5.2

[15/01/2021]

[EOL: 05/02/2023]

Type	Issue Number	Description	Components
FIX	#610	Fixed an Issue in creating certificate for AnyBank during setup	Access Control Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.5.1

[24/12/2020]

[EOL: 15/01/2023]

Type	Issue Number	Description	Components
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.5.0

[18/12/2020]

[EOL: 24/12/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#422	Enabling migration of ACS application server from Tomcat to WebLogic	Issuer Administration, Access Control Server, Registration Server, Enrolment Server

Type	Issue Number	Description	Components
ENHANCEMENT	#463	New Key Management and HSM connectivity - Phase I	Setup, Issuer Administration, Access Control Server, Registration Server, Enrolment Server
ENHANCEMENT	#468	Support for Oracle 19c	Setup, Issuer Administration, Access Control Server, Registration Server, Enrolment Server
ENHANCEMENT	#522	Addition of purchaseDate to CAAS Server's oobInfo	Access Control Server, Issuer Administration
ENHANCEMENT	#543	Mask critical data in log	Access Control Server
ENHANCEMENT	#557	Improved RMI support	Issuer Administration
FIX	#372	Incorrect CRes transStatus when RReq communication failed	Access Control Server
FIX	#431	New issuer creation error	Setup, Issuer Administration, Access Control Server
FIX	#445	CAVV U3v0 for RBA EMV 3DS	Access Control Server, Issuer Administration
FIX	#459	SMS counter issue when card has multiple devices	Access Control Server
FIX	#494	Extended logs for xslTransform not finished	Access Control Server
FIX	#555	Ending OOB transaction when not authenticated	Access Control Server
FIX	#556	threeDSReqAuthData missing	Access Control Server
FIX	#561	CAAS 3DS2 back issue	Access Control Server
FIX	#567	Set label `Challenge` for C&R in 3DS2 pages	Access Control Server

Type	Issue Number	Description	Components
FIX	#583	Invalid date and time in authentication landing page (2.1 version)	Access Control Server
FIX	#596	CardLoader/Registration API: can't load cards	Registration Server
FIX	#598	billAddrState, shipAddrState field validation (ISO 3166-2 codes)	Access Control Server
FIX	#599	SMS Templates	Issuer Administration
FIX	#601	OOB without continue button - Shutdown issue	Access Control Server
FIX	#602	ACS should display OOB Continue button when WS is unreachable	Access Control Server
FIX	#603	OOB without continue button - reduce CLOSE_WAIT time	Access Control Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.4.4

[25/11/2020]

[EOL: 18/12/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#550	Update Risk Engine Integrated in CAAS	Access Control Server
FIX	#572	SDK issue for remote issuer	Access Control Server

Type	Issue Number	Description	Components
FIX	#574	HMAC256 key creation error for Luna Provider	Access Control Server, Issuer Administration

ActiveAccess v8.4.3

[13/11/2020]

[EOL: 25/11/2022]

Type	Issue Number	Description	Components
FIX	560	Fixed 3DS1 remote authentication issue when authType = 10	Access Control Server
FIX	563	Fixed issue of formatting purchase date in CAAS API logs	Access Control Server
FIX	564	Fixed acs.war issue of formatting purchase date displaying in Remote/Local issuer authentication challenge page	Access Control Server

ActiveAccess v8.4.2

[27/10/2020]

[EOL: 13/11/2022]

Type	Issue Number	Description	Components
ENHANCEMENT		Enhancement on the remote issuer custom pages: both 3DS1 and 3DS2 remote authentication custom pages should be uploaded	Access Control Server
FIX	549	Added version in schema.xsd at acs.war/WEB-INF/lib/caas.client-*.jar	Access Control Server

Type	Issue Number	Description	Components
FIX	552	Restore authType compatibility: authType can be used for authentication methods 1-15	Access Control Server

ActiveAccess v8.4.1

[16/10/2020]

[EOL: 27/10/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#528	Support multi-instance for OOB Notifier	Access Control Server
FIX	#485	Update authentication methods	Access Control Server
FIX	#514	Mastercard 3DS2.1: generation of authentication method dropdown on the page	Access Control Server
FIX	#525	PAReq - invalid session	Access Control Server
FIX	#530	Issue with adding sms-centers to issuers on MIA	Issuer Administration
FIX	#533	Issue retrieving the wsUrl (Remote Issuer)	Access Control Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.4.0

[02/10/2020]

[EOL: 16/10/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#348	Support new Visa Secure CAVV Usage 3, Version 7 and add an option to select the algorithm	Access Control Server, Issuer Administration
ENHANCEMENT	#383	Separate SDK html pages from BRW html pages	Access Control Server
ENHANCEMENT	#387	Remove Continue button & add support for auto-submission of OOB page - Remote Authentication	Access Control Server, Issuer Administration
ENHANCEMENT	#455	Display IAV generation algorithm in Transaction Details	Access Control Server, Issuer Administration
ENHANCEMENT	#457	Extend OOB Adapter Challenge Request API with purchase date and time element	Access Control Server
ENHANCEMENT	#467	Assign multiple SMS devices to cards that have different SMSC	Registration Server
ENHANCEMENT	#482	Configurable log for number of DB connections	Access Control Server
ENHANCEMENT	#498	Compatibility with Visa authentication page requirements	Access Control Server
FIX	#437	Pages do not stretch to the entire height of the device - AnyBank_Remote Custompages_3DS2 - incorrect page display	Access Control Server
FIX	#440	Error during decryption in CardDeviceUpdate	CardLoader, Registration Server
FIX	#454	Failed 3DS2 transaction details in MIA	Access Control Server, Issuer Administration
FIX	#460	Error during retrieving messageExtension from session	Access Control Server

Type	Issue Number	Description	Components
FIX	#462	Actions for when OobAuthenticationResult indicates cardholder did not perform OOB auth or there was a connection issue	Access Control Server
FIX	#483	SessionID logging	Access Control Server
FIX	#486	CAVV issue - PAN length must be 16	Access Control Server
FIX	#492	Amount without separator	Access Control Server
FIX	#493	Fix $PurchaseDateTime format in SMS messages	Access Control Server
FIX	#494	The xslTransform not finished	Access Control Server
FIX	#495	3DS2 Challenge errors flow	Access Control Server
FIX	#499	Incorrect data in MIA Reports	Issuer Administration
FIX	#503	Error during parsing sessionInfo when cardId is UUID for Remote Issuers	Access Control Server
FIX	#504	Remote page issue - OOB initAuth error	Access Control Server
FIX	#509	SDK sessionKey should be saved in DB	Access Control Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.3.6

[07/08/2022]

[EOL: 02/10/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#450	Save valid messages with Invalid ISO codes	Access Control Server
FIX	#437	Text displayed incorrectly when token is entered on Remote Authentication pages	Access Control Server
FIX	#446	Display issue for 3DS1 Local Authentication when OOB + SMS was assigned to the card	Access Control Server
FIX	#447	Disabled the validation of cardholder name for 3DS2 authentication	Access Control Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.3.5 (Patch)

[16/07/2020]

[EOL: 07/08/2022]

Type	Issue Number	Description	Components
FIX	#441	AAV generation issue for 3DS1 Mastercard transactions	Access Control Server

ActiveAccess v8.3.4 (Patch)

[09/07/2020]

[EOL: 16/07/2022]

Type	Issue Number	Description	Components
FIX	#441	Removing cancel button in XSL pages for SDK transactions	Access Control Server

ActiveAccess v8.3.3 (Patch)

[06/07/2020]

[EOL: 09/07/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#441	Additional logs added for 3DS1 Mastercard transactions	Access Control Server

ActiveAccess v8.3.2 (Patch)

[26/06/2020]

[EOL: 06/07/2022]

Type	Issue Number	Description	Components
FIX	#441	Extending the Message Length for SDK transactions	Access Control Server

ActiveAccess v8.3.1 (Patch)

[12/06/2020]

[EOL: 26/06/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#441	Additional logs added for SDK transactions	Access Control Server

ActiveAccess v8.3.0

[29/05/2020]

[EOL: 12/06/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#158	OTP & password option for OOB	Issuer Administration, Access Control Server
ENHANCEMENT	#274	Encrypting critical data such as cardnumber in adapters	Issuer Administration, Access Control Server
ENHANCEMENT	#325	Encryption of card number in CardLoader logs	CardLoader
ENHANCEMENT	#343	IAV method option for Mastercard PSD2 in Issuer groups	Issuer Administration, Access Control Server
ENHANCEMENT	#328	RMI configuration option	Setup, Issuer Administration, Access Control Server
ENHANCEMENT	#403	Add 3DS2 transactional data into CAAS messages	Access Control Server
ENHANCEMENT	#423	MIA to notify user when device is removed from Issuer's Active Device list	Issuer Administration
ENHANCEMENT	#429	Remove case sensitivity of OobRequestChallengeResult.requestChallengeEnum accepted values	Access Control Server
FIX	#370	OOB deviceId length issue	Registration Server

Type	Issue Number	Description	Components
FIX	#373	FileNotFoundException during RBA and OOB startup	Access Control Server
FIX	#421	10-CR challenge authentication issue	Access Control Server
FIX	#427	Updated ECI values for AMEX, JCB and Diners	Access Control Server
FIX	#438	Change SecureCode HMAC 256 key	Issuer Administration
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.2.6 (Patch)

[07/05/2020]

[EOL: 29/05/2022]

Type	Issue Number	Description	Components
FIX	#375	Stop ACS from uploading CustomPages for AnyBank at start up	Issuer Administration
FIX	#420	NullPointer Exception during SMS device loading	Access Control Server
FIX	#426	MIA Report error	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.2.5 (Patch)

[04/05/2020]

[07/05/2022]

Type	Issue Number	Description	Components
FIX	#420	NullPointer Exception during SMS device loading	Access Control Server

ActiveAccess v8.2.4 (Patch)

[28/04/2020]

[04/05/2022]

Type	Issue Number	Description	Components
FIX	#420	NullPointer Exception during SMS device loading	Access Control Server

ActiveAccess v8.2.3 (Patch)

[24/04/2020]

[28/04/2022]

Type	Issue Number	Description	Components
FIX	#419	Issue with ACS authentication pages and authentication results cannot be seen	Access Control Server

ActiveAccess v8.2.2

[17/04/2020]

[24/04/2022]

Type	Issue Number	Description	Components
FIX	#371	Fixes to Frictionless Flow, Browser, PA (Result = N)	Access Control Server
FIX	#412	Luna HSM KeyStore loading issue	Access Control Server, Setup
FIX	#413	RSA key size for new issuers and issuer groups changed to 2048	Access Control Server, Setup
FIX	#416	Fixes to Frictionless Flow, 3RI, and NPA (Result = Y)	Access Control Server

ActiveAccess v8.2.1

[09/04/2020]

[EOL: 17/04/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#331	Addition of cancel link to 3DS2 authentication pages	Access Control Server
ENHANCEMENT	#369	Addition of "store name", "date" and "amount" to authentication page	Access Control Server
FIX	#349	null cardName in verifyRegResp produces an error	Access Control Server
FIX	#371	Changes to the validation date of cardLoader generated certificate	CardLoader
FIX	#393	Misplacement of elements in responsive view of custom pages	Access Control Server
FIX	#394	NullPointerException error while processing regStatus=1 in CAAS	Access Control Server

Type	Issue Number	Description	Components
FIX	#395, 400	ClientID=null not to be included in Notification Reports, OOB & RBA APIs	Access Control Server, CardLoader, Registration Server
FIX	#396	Exception during initializing LunaProvider in gpcomp.updater	Setup
FIX	#397, #399	Archive database schema upgrade from ActiveAccess v7.3 to ActiveAccess v8.2	Issuer Administration, Setup
FIX	#407	Configuration of "ACS challenge URL" for issuers	Access Control Server

ActiveAccess v8.2.0

[27/03/2020]

[EOL: 09/04/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#151	Support push notifications during OOB authentication	Access Control Server, Registration Server
ENHANCEMENT	#174	IAV method option for Mastercard PSD2	Access Control Server, Issuer Administration
ENHANCEMENT	#192	Displaying OTP+StaticPassword for CAAS	Access Control Server
ENHANCEMENT	#221	Displaying risk decision in Transaction Details page	Issuer Administration
ENHANCEMENT	#307	Addition of a new card attribute: ClientID	Access Control Server, CardLoader, Issuer Administration, Registration Server

Type	Issue Number	Description	Components
ENHANCEMENT	#316	Card and Transaction search performance improvement	Issuer Administration
ENHANCEMENT	#319	"Score range for device" in RBA allows for selection from all devices including OOB	Access Control Server
ENHANCEMENT	#323	Addition of "Maximum interaction" limit for Remote Issuers	Access Control Server, Issuer Administration
FIX	#234	Fix for CAASSESSION table lock issue	Access Control Server
FIX	#315	Fix for archive and purge features	Issuer Administration
FIX	#353	Reverting Card Expiry Date to optional	Issuer Administration, Registration Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.1.2

[10/01/2020]

[EOL: 28/02/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#228	Adding forgot password link for browser device channel	Access Control Server
ENHANCEMENT	#251	Send tokens only when the Resend OTP link is clicked	Access Control Server
ENHANCEMENT	#268	Changes to PreAuth in Remote Authentication model	Access Control Server

Type	Issue Number	Description	Components
ENHANCEMENT	#299	Improvements to enabling 2FA for admin users	Issuer Administration
ENHANCEMENT	#300	Device selection when two OOB devices are assigned to a card	Access Control Server
ENHANCEMENT	#312	Addition of DESede support to CardLoader and Registration for backward compatibility	Registration Server, CardLoader
FIX	#271	Fixing Ping Command connection issue	Issuer Administration, Access Control Server, Registration Server, Enrolment Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.1.1

[06/12/2019]

[EOL: 10/01/2022]

Type	Issue Number	Description	Components
ENHANCEMENT	#267	Add new CancelReg request with optional cardholder name	Registration Server, CardLoader
ENHANCEMENT	#271	ActiveAccess Ping command improvement	Issuer Administration, Access Control Server, Registration Server, Enrolment Server
FIX	#303	Invalidate empty cardholder name in PreReg and FinalReg	Registration Server, CardLoader

ActiveAccess v8.1.0

[15/11/2019]

[EOL: 06/12/2021]

Type	Issue Number	Description	Components
ENHANCEMENT	#92	Acceptable values for `App unsupported devices` updated	Access Control Server, Issuer Administration
ENHANCEMENT	#131	Supporting two-factor authentication for local authentication	Access Control Server, Issuer Administration
ENHANCEMENT	#142	Changing the risk/rule decision process	Access Control Server
ENHANCEMENT	#143	Provide a mechanism to test OOB and RBA restful adapters connect/read timeouts	Access Control Server, Issuer Administration
ENHANCEMENT	#179	Including more data in RBA call back	Access Control Server
ENHANCEMENT	#198	Updating the approach of populating the historical transaction for RBA	Access Control Server
ENHANCEMENT	#201	Create a swagger for OOB and Risk restful adapters	Access Control Server
ENHANCEMENT	#246	Enabling language selection during authentication for 3DS1	Access Control Server, Issuer Administration
ENHANCEMENT	#273	Http protocol version for external connections	Access Control Server
FIX	#53	3DS method notification post data	Access Control Server
FIX	#95	ACS decision based on risk chain score in remote authentication	Access Control Server
FIX	#260	HSM installation issues	Setup

Type	Issue Number	Description	Components
FIX	#266	Detach SDK certificates from Issuer Certificates	Setup
FIX	#278	CAAS Server throws NullPointer when message category is NPA	Access Control Server

ActiveAccess v8.0.4

[06/11/2019]

[EOL: 15/11/2021]

Type	Issue Number	Description	Components
FIX	#281	Invalid Request to Remote Server	Access Control Server

ActiveAccess v8.0.3

[25/10/2019]

[EOL: 06/11/2021]

Type	Issue Number	Description	Components
FIX	#277	Deployment of registration.war during startup	Registration
FIX	#278	CAAS throws a NullPointer when message category is NPA	Access Control Server

ActiveAccess v8.0.2

[09/10/2019]

[EOL: 25/10/2021]

Type	Issue Number	Description	Components
ENHANCEMENT	#51	Support 3DS2 purchase amount 0 for Mastercard IDC	Access Control Server
ENHANCEMENT	#98	Update ECI for Message Category NPA for Mastercard IDC	Access Control Server
ENHANCEMENT	#219	Making acsReferenceNumber configurable for testing purposes	Issuer Administration, Access Control Server
ENHANCEMENT	#223	Addition of decline code to preAuthResp of CAAS	Access Control Server
ENHANCEMENT	#229	Addition of KeyStore and TrustStore for RBA Server	Access Control Server
ENHANCEMENT	#233	Addition of KeyStore and TrustStore for OOB Server	Access Control Server
FIX	#132	Updates to Mastercard IDC status codes	Access Control Server
FIX	#148	Remote CAAS PreAuth changes	Access Control Server
FIX	#226	Setup could not generate RSA2048 keys for the MAP error during Luna PKCS11 installation/upgrade	Setup
FIX	#242	Verified by Visa references changed to Visa Secure in the content of authentication pages	Access Control Server
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.0.1

[05/09/2019]

[EOL: 02/10/2021]

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
FIX		General fixes, performance and security enhancements	Setup, Issuer Administration, Access Control Server, Registration Server

ActiveAccess v8.0.0

[15/08/2019]

[EOL: 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
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

Type	Issue Number	Description	Components
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

Active Control Server		
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
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

Issuer Administration		
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
ENHANCEMENT	#6463	ISO 4217 Currency Code Service - Amendment number 163
ENHANCEMENT	#6527	Mastercard Identity Check Support
ENHANCEMENT	#6688	JCB Attempt process

Issuer Administration		
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
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

Access Control Server		
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

Registration Server		
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.

Access Control Server		
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

Setup		
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*
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

Access Control Server		
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
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
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

Access Control Server		
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