About Setup Guide

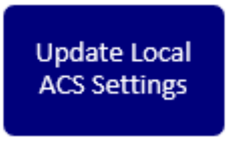
This section is a post installation guide for setting up ActiveAccess for testing. It describes, at a high level, the steps involved in setting up issuers, signing certificates and configuring cards for various payment scenarios, prior to testing. It also covers the steps involved in device configuration, 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

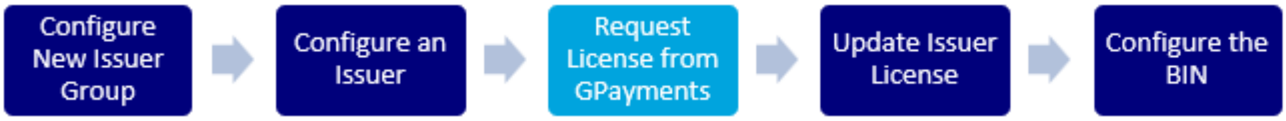
ACS URL



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 New Issuer Group → Configure an Issuer → Request License from GPayments → Update Issuer License → Configure the BIN

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.

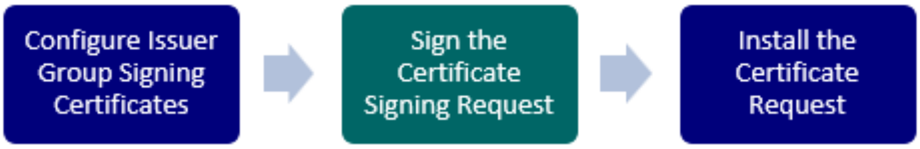
Configure the BIN

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
Sign the Certificate Signing Request
Install the Certificate Request

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.

Configuration - from end of installation

Configuration - ActiveAccess

The purpose of this section is to provide an overview of the steps required in order to configure the system for testing purposes. This requires you to set up at least one issuer, create test cards and upload the authentication and enrolment pages.

Creating a New Issuer

- Login to the Administration server using an account with system admin access (such as administrator)
- Use the **Issuer Management** section and create an issuer. The system creates an issuer and displays a 19-digit Issuer ID. Make a note of the Issuer ID for future use.

Note

At this stage the new issuer is not registered.

- Send the Issuer ID and Issuer Name to GPayments and request an ActiveAccess license key. Once you receive the license key for the issuer, copy the contents of the license key into the **Issuer Details** page. Apply the changes and make sure that the message **License key is valid** is displayed.

The Administration server creates a set of cryptographic keys for the issuer in the HSM local to the administration server. If ActiveAccess is installed on a separate server, and as such uses its own hardware security module, these keys need to be transferred to that server's HSM.

- Export the following keys to the ActiveAccess HSM:

  RSAVbV< Issuer_ID >_pub

  RSAVbV< Issuer_ID >_pri

  RSAMSC< Issuer_ID >_pub

  RSAMSC< Issuer_ID >_pri

  RSAJCB< Issuer_ID >_pub

RSAJCB< Issuer_ID >_pri

RSASK< Issuer_ID >_pub

RSASK< Issuer_ID >_pri

RSADC< Issuer_ID >_pub

RSADC< Issuer_ID >_pri

RSADEVICE< Issuer_ID >_pub

RSADEVICE< Issuer_ID >_pri

SPA< Issuer_ID >

VbVA< Issuer_ID >

VbVB< Issuer_ID >

JCBA< Issuer_ID >

JCBB< Issuer_ID >

MSCA< Issuer_ID >

MSCB< Issuer_ID >

SKA< Issuer_ID >

SKB<< Issuer_ID >

DCA< Issuer_ID >

DCB< Issuer_ID >

Card< Issuer_ID >

Where < Issuer_ID > is the actual Issuer ID provided in the previous steps.

Info

For further information on key export and import, please see section 0 - Key Transfer.

Note

If you have enabled the **Use parent keys** option, the only key generated for the issuer is Card< Issuer_ID >

- If the enrolment server or registration servers have been set-up on a different machine to administration server, these keys need to be transferred to their server HSM.

- Export the following keys to the enrolment or registration server HSM:

```
Card < Issuer_ID >
```

Where < Issuer_ID > is the actual Issuer ID provided in the previous steps.

> **Info**
>
> For further information on key export and import, please see section 0 - Key Transfer.

- Use the Certificates Details section to create a certificate request for the issuer.

> **Note**
>
> Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

- Send the certificate request to the appropriate Mastercard, Visa, JCB, American Express or Diners Club International certificate authority for signing.
- Import the signed certificate back to the system using the Certificates Details section (the certificate must be in p7b format and include all the certificates in the certification path)

> **Note**
>
> Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

- Upload the issuer public key certificate using the Public & Encryption Key Management function in the administration server.

> **Note**
>
> Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

- Upload the authentication and enrolment pages (if applicable) for the issuer using the Custom Pages function in the administration server.

Creating a New Issuer Group

- Login to the Administration server using an account with system admin access (such as administrator)
- Use the **Group Management** section to create an issuer group.

  Administration server creates a set of cryptographic keys for the issuer group in the HSM local to the administration server. If ActiveAccess is installed on a separate server, and as such uses its own hardware security module, these keys need to be transferred to that server's HSM.
- Export the following keys to the ActiveAccess HSM:

  RSAVbV< Group_ID >_pub

  RSAVbV< Group_ID >_pri

  RSAMSC< Group_ID >_pub

  RSAMSC< Group_ID >_pri

  RSAJCB< Group_ID >_pub

  RSAJCB< Group_ID >_pri

  RSASK< Group_ID >_pub

  RSASK< Group_ID >_pri

  RSADC< Group_ID >_pub

  RSADC< Group_ID >_pri

  RSADEVICE< Group_ID >_pub

  RSADEVICE< Group_ID >_pri

  SPA< Group_ID >

  VbVA< Group_ID >

  VbVB< Group_ID >

  JCBA< Group_ID >

  JCBB< Group_ID >

  MSCA< Group_ID >

  MSCB< Group_ID >

  SKA< Group_ID >

SKB< Group_ID >

DCA< Group_ID >

DCB< Group_ID >

- Where < Group_ID > is the group's unique identifier as displayed in the issuer group details page.

Note

Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

Info

For further information on key export and import, please see section 0 - Key Transfer.

- Use the Certificate Details section to create a certificate request for the group.

Note

Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

- Send the certificate request to the appropriate Mastercard, Visa, JCB, American Express, or Diners Club International certificate authority for signing.

Note

Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

- Import the signed certificate back to the system using the Certificate Details section (the certificate must be in p7b format and include all the certificates in the certification path)

Note

Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

- Upload the group public key certificate using the Public & Encryption Key Management function in the administration server.

Note

Skip this step if you have enabled the Use parent certificate, public and encryption keys option.

Configuring an Issuer for ActiveDevice

To activate device authentication for an issuer:

- Login to the Administration server using an account with system admin access (such as administrator)
- Use **System Management > Issuer Management** to find issuer's account and access issuer details
- Install a license key with ActiveDevice functionality enabled. If an appropriate license key is installed the license status shows **Device authentication enabled**.

Note

Contact GPayments if you don't have a license key with the ActiveDevice option enabled.

- Create and install an issuer signing certificate for ActiveDevice, make sure that the CA is in the ActiveDevice's trusted CA list (in ActiveAccess)
- Click on the ActiveDevice settings link. Select the appropriate token type for the issuer (e.g. VASCO) and apply the changes.
- Upload two-factor authentication pages customised for this issuer. Use **Issuer > Custom Pages > Upload File** to locate and upload the two-factor custom pages. If testing you can use the sample two-factor pages which can be found in the **/pkg/Custom Pages/Samples/** directory.

Cards

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
Register the Pre-Registered Card

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 → Register the Pre-Registered Card → Lock the Card

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.

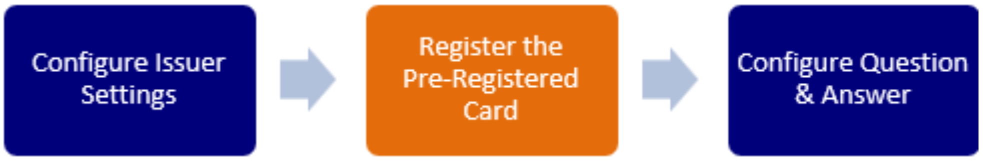
ActiveMerchant Test Payment Page

- 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
Register the Pre-Registered Card
Configure Question & Answer

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)

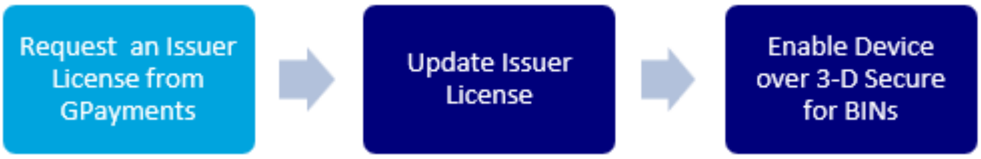
- Go to the ActiveMerchant Test Payment page
- Enter the **Card number** to perform a test transaction
- Click the **Submit** button
- Ensure that the outcome corresponds with the authentication scenario.

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 an Issuer License from GPayments
Update Issuer License
Enable Device over 3-D Secure for 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.

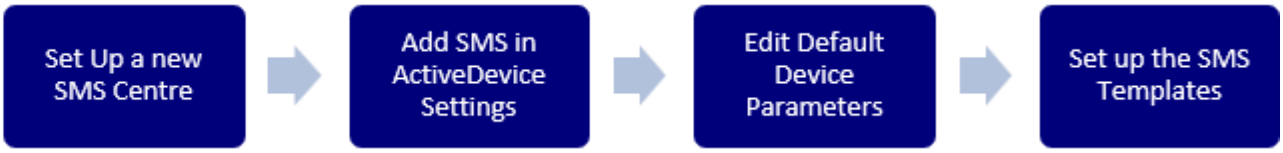
> **Note**
>
> If an error occurs, contact GPayments Tech Support.

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

Add SMS in ActiveDevice Settings

Edit Default Device Parameters

Set up the SMS Templates

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

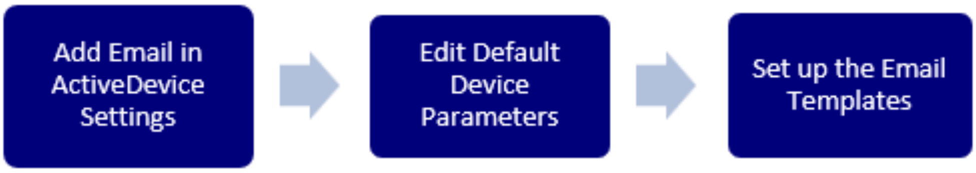
- Under **Supported devices**, in the **Available** box, select SMS and click the **Add >>** button.
- Click the **Apply** button.

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
Edit Default Device Parameters
Set up the Email Templates

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

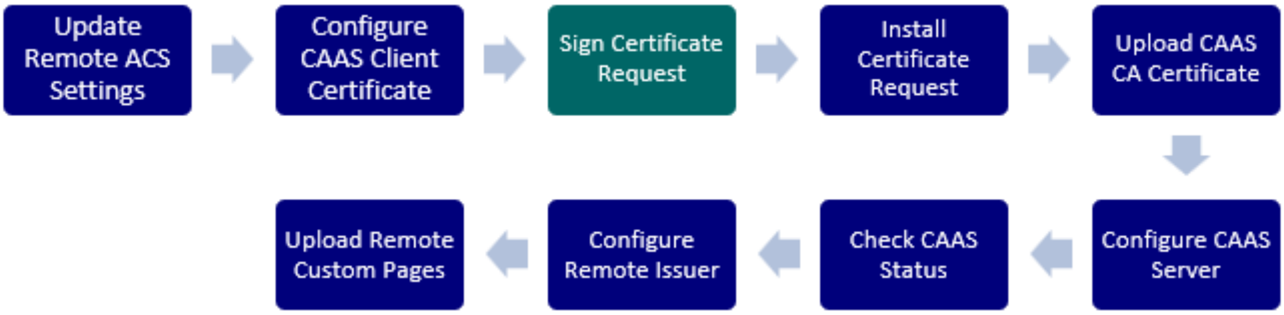
Upload the VASCO File

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


Update Remote ACS Settings
Configure CAAS Client Certificate
Sign Certificate Request
Install Certificate Request
Upload CAAS CA Certificate
Configure CAAS Server
Check CAAS Status
Configure Remote Issuer
Upload Remote Custom Pages

- 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

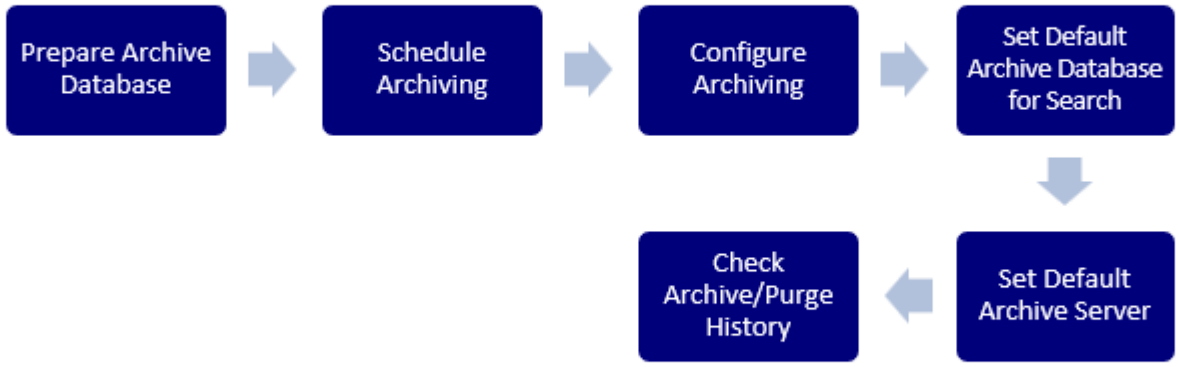
Issuers > Custom Pages

- 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
Schedule Archiving
Configure Archiving
Set Default Archive Database for Search
Set Default Archive Server
Check Archive/Purge History

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 Tomcat_Home\bin\config\acsconfig.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

Error Codes

Server Error Codes

Server Error Codes			
Code	**Message**	**Details**	**Usage**
1	Root element invalid.	Exception message and its cause FourDSecure ThreeDSecure	Yes
2	Message element not a defined message.	Exception message and its cause VVRQ PPRQ Undefined CRReq	Yes
3	Required element missing.	PaReq TermUrl MD Id | VEReq.Extension.Id | PAReq.Extension id VEReq.version | version | PAReq.version Pan | VEReq.Pan PAReq.Merchant.name | name PAReq.Merchant.country | country PAReq.Merchant.url | url PAReq.Purchase.xid | xid PAReq.Purchase.date | date PAReq.Purchase.amount | amount PAReq.Purchase.purchAmount | purchAmount PAReq.Purchase.currency | currency PAReq.Purchase.exponent | exponent PAReq.CH.acctID | acctID PAReq.CH.expiry | expiry Message.Id | Id Message	Yes
4	Critical element not recognized.	Extension | VEReq.Extension | PAReq.Extension	Yes

Server Error Codes			
5	Format of one or more elements is invalid according to the specification.	Exception message and its cause version | VEReq.Version | PAReq.Version Pan | VEReq.Pan VEReq.Extension.Id | Extension.Id VEReq.Browser.deviceCategory | devicCategory Extension.Critical PAReq.Merchant.name | name | Merchant.name PAReq.Merchant.country | country | Merchant.country PAReq.Purchase.xid | xid | Purchase.xid PAReq.Purchase.date | date | Purchase.date PAReq.Purchase.amount | amount | Purchase.amount PAReq.Purchase.purchAmount | purchAmount | Purchase.purchAmount PAReq.Purchase.currency | currency | Purchase.currency PAReq.Purchase.exponent | exponent | Purchase.exponent PAReq.Purchase.desc | desc | Purchase.desc PAReq.Purchase.Recur.frequency | frequency | Recur.frequency PAReq.Purchase.Recur.endRecur | endRecur | Purchase.Recur.endRecur PAReq.Purchase.install | install | .Purchase.install PAReq.CH.acctID | acctId | CH.acctID PAReq.CH.expiry | expiry | CH.expiry Message.Id | Id Merchant Merchant.merID	Yes
6	Protocol version too old.	Protocol version too old. Protocol version is not supported by ProtectBuy.	Yes
98	Transient system failure.	Contact your vendor with this 'ACS Session ID': %sessionId%	Yes
99	Permanent system failure.	%s	No

Server Error Codes			
1001	Invalid http request	Invalid HTTP request: PAHndler.run() Invalid HTTP request:	Yes
1002	Process timed out	Process timed out	Yes
1003	Invalid xml request	Invalid XML request process.	No
1004	Error in ThreeDS.service(): %s	Error in ThreeDS.service(): %s	No
1005	Permission denied	Permission denied	Yes
1006	An extension is not currently associated with this request	An extension is not currently associated with this request	Yes
1007	ACS failed to start successfully.	ACS failed to start successfully	Yes
1008	Error in inflating PAReq	Error in inflating PAReq ver 1.0.1	Yes
1009	Error in deflating PARes	Error in deflating PARes ver 1.0.1	No
1010	This session is invalid. Please try again.	This session is invalid. Please try again.	Yes
1011	Your session has now expired. Please try again.	Your session has expired. Please try again.	Yes
1012	Internal error: Unable to save session.	Internal error: Unable to save session.	No
1013	Invalid authentication result in ThreeDS.service(): %s	Invalid authentication result in ThreeDS.service(): %s	No
1014	'%s' request length is too large	'HTTP' request length is too large 'XML' request length is too large	Yes
1015	Invalid cardholder name for PARes 10X in ThreeDS.service()	Invalid cardholder name for PARes 10X in ThreeDS.service()	No

Server Error Codes			
1016	The process has been successfully completed. One or more required parameters were not specified.	The process has been successfully completed. One or more required parameters were not specified.	Yes
1017	Cannot find any authentication data.	Authentication data not found.	Yes
1018	Issuer's BIN does not support device authentication over 3-D Secure.	This issuer BIN range does not support device authentication for 3-D Secure.	No
1019	Issuer does not support any devices.	Issuer does not support any devices.	Yes
1020	Invalid request.	ACS records show the card type is MasterCard but the request was received as on Visa VE server. ACS records show the card type Visa but the request was received as on MasterCard VE server. ...	Yes
1021	There is no assigned device.	There is no device assigned.	Yes
1022	Different card types.	Cards belong to different card schemes.	Yes
1023	Invalid character	There is an invalid character in parameter (%s)	No
1024	Invalid card in authentication process	Card is pre-registered and cannot be used in the authentication process.	Yes
1025	Illegal process	Illegal process 'Authorization'	Yes
1026	Server is in reinitializing state	Server is in reinitializing state.	Yes
1027	Invalid authentication URL	'Url' is invalid	Yes
1028	Cannot find all the required parameters for PA processing	Cannot find all the required parameters for PA processing 'URI'.	Yes

Server Error Codes			
1029	Page and process do not match	The 'page name' page cannot be displayed while in the duplicate cardholder process.	Yes
1030	Invalid parameter value		No
1031	Email Device Param not initialized		Yes

User Error Codes

User Error Codes			
Code	**Message**	**Details**	**Usage**
1	Root element invalid.	Device	Yes
2	Message element not a defined message.	Name of undefined element	Yes
3	Required element missing.	Name of missing element	Yes
4	Critical element not recognized.	Extension	Yes
5	Format of one or more elements is invalid according to the specification.	Name of invalid element	Yes
50	Issuer %s does not participate in device authentication.	%s	Yes
55	Transaction data not valid.	%s	Yes
56	Signature verification failed.	%S	Yes
70	Invalid request	%S	Yes
71	Session is invalid.	%S	Yes

User Error Codes			
72	Session is expired.	%S	Yes
98	Transient system failure	%S	Yes
99	Permanent system failure.	%S	Yes
1001	Invalid HTTP request	Invalid request	No
1002	Process timed out	Process timed out	No
1003	Invalid XML request	Invalid XML request	No
1004		%s does not exist or has an incorrect format	No
1005	Permission denied	Permission denied	No
1006	An extension is not currently associated with this request	An extension is not currently associated with this request	No
1007	Server has not started correctly	Server has not started correctly	No
1008		Error in serializing the %s XML Document	No
1009		Session '%s' has expired	No
1010	Invalid request length	'%s' request length is too large	No
1011		The process has been successfully completed. One or more required parameters were not specified	No
1012		Error in inflating UAReq ver 1.0.1	No
1013		Error in deflating UARes ver 1.0.1	No
2001	User not registered		No

User Error Codes			
2002	User is locked		Yes
2003	Action cancelled		Yes
2004	User is disabled		Yes
2005	Maximum number of transactions exceeded		Yes
2010	Device not registered		Yes
2011	Cannot find any active devices		Yes
2012	Device type is not supported. Type = %s		Yes
2013	Invalid device extension, %s		Yes
2014	Invalid token		Yes
2015	Invalid password		Yes
2016	One-way authentication is not supported for device type %s		Yes
2017	Maximum number of SMS resend request exceeded		Yes
2050	Issuer %s does not participate in device authentication		Yes
2051	License key does not allow for device authentication, %s		Yes
2052	Invalid password for issuer %s		Yes
2053	Device type %s is not supported for issuer %s		Yes

User Error Codes			
2054	The interface is disabled for issuer %s		Yes
2055	Device type %s is not supported by the device owner (issuer: %s)		Yes
2056	The process has been successfully completed. One or more required parameters were not specified.		Yes
2057	Duplicate UAReq not allowed		Yes

Account Error Messages

Account Error Messages		
Code	**Message**	**Usage**
101	Please re-enter the field(s) highlighted in red	Yes
102	Required field missing	Yes
103	Invalid number	No
104	Invalid password	Yes
105	Invalid activation code	No
106	Data verification error	Yes
107	Field length exceeded	Yes
108	Invalid one time password	Yes
109	Invalid cardholder name	Yes

Account Error Messages		
110	Invalid cardholder	No
111	Invalid password length	No
112	Passwords do not match	Yes
113	Invalid answer	Yes
114	Invalid username	Yes
115	Invalid full name	Yes
116	Invalid personal assurance message (PAM)	Yes
117	Invalid expiry date	Yes
118	Invalid card number	Yes
120	Invalid question	No
121	Invalid device type selected	Yes
122	Resynchronization failed	Yes
123	Invalid cardID	Yes
124	Password must be between [%1] to [%2] characters long	Yes
125	Password must contain at least [?] number(s)	Yes
126	Password must contain at least [?] capital letter(s)	Yes
127	Unicode characters cannot be used	Yes
128	Invalid character	No
129	The parameter ([?]) is required	Yes

Account Error Messages		
130	Invalid PriSec	Yes
131	The Personal Message must not contain your Verified by Visa password or Password Hint	Yes
132	The Password Hint must not contain your Verified by Visa password	Yes
133	The account should have ([?]) authentication data	Yes
134	Invalid Hint	Yes
135	Invalid Data Format	Yes
136	[%1] does not match the confirmation [%2]	Yes

Authentication Device Messages

Authentication Device Messages		
Code	**Message**	**Usage**
101	Please re-enter the field(s) highlighted in red	No
102	Required field missing	Yes
103	Invalid number	No
104	Invalid password	No
105	Invalid Activation Code	No
106	Data verification error	No
107	Field length exceeded	Yes
108	Invalid one time password	Yes

Authentication Device Messages		
301	Current Token:	Yes
302	Please enter the one time password from one of your existing devices here	Yes
303	Invalid one time password	Yes
304	Invalid serial number	Yes
305	Device is lost	Yes
306	Device is damaged	Yes
307	Device is already assigned	Yes
401	Current Token:	No
402	Please enter the one time password from one of your existing devices here	No
403	Invalid one time password	Yes
404	Invalid serial number	Yes
405	Device is lost	Yes
406	Device is damaged	Yes
407	Device is already assigned	Yes
501	SMS Token:	Yes
502	Please enter the one time password which was sent to you via SMS	Yes
503	Invalid SMS one time password	Yes
504	Invalid mobile number	Yes
505	Invalid mobile network provider	Yes

Authentication Device Messages		
506	Invalid country calling code	Yes
507	Please enter the mobile number only, without the country code or prefixes	Yes
508	Mobile number is temporarily disabled	Yes
509	Phone is damaged	Yes
510	Phone is lost	Yes
511	The mobile number entered already exists and has been assigned to a different SMSC	Yes
512	Your mobile number and confirmation do not match. Please re-enter	Yes
513	Phone is already assigned	Yes
601	Current Token:	No
602	Please enter the one time password from one of your existing devices here	No
603	Invalid one time password	Yes
604	Invalid PAN	Yes
605	Device is not active	Yes
606	Device is lost	Yes
607	Device is damaged	Yes
608	Device is already assigned	Yes
701	Email Token:	No
702	Please enter the one time password which was sent to you via Email	No

Authentication Device Messages		
703	Invalid Email one time password	Yes
704	Invalid Email Address	Yes
705	Email is lost	Yes
706	Email is damaged	Yes
707	Your Email and confirmation do not match. Please re-enter	Yes
708	Email is already assigned	Yes
709	Unicode characters are not accepted	Yes

Local Pages Errors

Local Pages Errors	
Code	**Message**
101	Please re-enter the field(s) highlighted in red
102	Required field missing
103	Invalid number
104	Invalid SecureCode Invalid Verified by Visa Password Invalid JSecure Password Invalid SafeKey Invalid ProtectBuy Password
105	Invalid activation code
106	Data verification error
107	Field length exceeded

Local Pages Errors	
108	Invalid one time password
109	Invalid cardholder name
112	Your SecureCode and confirmation do not match. Please re-enter. Your Verified by Visa Password and confirmation do not match. Please re-enter. Your JSecure and confirmation do not match. Please re-enter Your SafeKey and confirmation do not match. Please re-enter. Your ProtectBuy Password and confirmation do not match. Please re-enter.
113	Invalid answer
114	Invalid username
115	Invalid full name
116	Invalid personal assurance message (PAM)
117	Invalid expiry date
118	Invalid card number
119	Invalid CVC
120	Invalid question
121	Invalid device type selected
122	Resynchronization failed
123	Invalid Password length Your SecureCode must be less "maxPassLen" characters long Your Verified by Visa Password must be less than "maxPassLen" characters long Your SecureCode must be less "maxPassLen" characters long Your Verified by Visa Password must be less than "maxPassLen" characters long Your JSecure Password must be less than "maxPassLen" characters long Your SafeKey must be less than "maxPassLen" characters long Your Password must be less than maxPassLen" characters long

Local Pages Errors	
124	Your SecureCode must be less "maxPassLen" characters long Your Verified by Visa Password must be less than "maxPassLen" characters long
125	Your SecureCode must contain at least "minPassDigit" digit(s) Your Verified by Visa must contain at least "minPassDigit" digit(s) JSecure must contain at least "minPassDigit" digit(s) SafeKey must contain at least "minPassDigit" digit(s) Password must contain at least "minPassDigit" digit(s)
126	Your SecureCode must contain at least "minPassCapital" capital letter(s) Your Verified by Visa must contain at least "minPassCapital" capital letter(s) Your JSecure must contain at least "minPassCapital" capital letter(s) Your SafeKey must contain at least "minPassCapital" capital letter(s) Your Password must contain at least "minPassCapital" capital letter(s)
127	Unicode characters are not accepted
128	Invalid character
129	Device is already assigned
130	Invalid PriSec
131	The Personal Message must not contain your Verified by Visa password or Password Hint
132	The Password Hint must not contain your Verified by Visa password
150	This field cannot be left blank
303	Invalid one time password
304	Invalid serial number
305	Device is lost
306	Device is damaged
307	Device is already assigned

Local Pages Errors	
403	Invalid one time password
404	Invalid serial number
405	Device is lost
406	Device is damaged
407	Device is already assigned
503	Invalid SMS one time password
504	Mobile number does not match the specified mobile restriction pattern
505	Invalid mobile network provider
506	Invalid country phone code
507	Please only enter mobile phone number without country code and prefixes
508	Mobile number has been temporarily disabled
509	Mobile phone for this number has been reported as damaged
510	Mobile phone for this number has been reported as lost
511	There is an already existing mobile number which has been assigned to a different SMSC
512	Your Mobile Number was not correctly confirmed. Please make sure that the Mobile Number and confirmation match
513	Phone is already assigned
603	Invalid one time password
604	Invalid PAN
605	Device is not active

Local Pages Errors	
607	Device is damaged
608	Device is already assigned

Glossary

This page provides a list of terms relating to 3D Secure 1 and 2, some are not used elsewhere in this documentation but are included for completeness of the subject area. Familiarise yourself with them now or refer back to this page when you come across an unfamiliar word, phrase or acronym.

Term	Acronym	Definition
2-F Authentication		A generic functionality, which allows for strong authentication of any transaction, commercial or otherwise, for example, strong authentication of users when they login to an Internet banking site or when they authorise funds transfer to a third party. 2-F authentication requires two independent ways to establish identity and privileges as opposed to traditional password authentication, which requires only one 'factor' (knowledge of a password).
3-D Secure **3D Secure** **3D Secure 1** **3D Secure 2**	**3DS** **3DS1** **3DS2**	A payer authentication standard (3D Secure 1 (3DS1)) introduced by Visa (Verified by Visa) and subsequently adopted by Mastercard (Mastercard SecureCode and Mastercard SecureCode), JCB (JCB J/Secure), American Express (SafeKey) and Diners Club International / Discover (ProtectBuy) designed to reduce online credit card fraud and chargeback. The 3DS standard provides an additional layer of protection in card-not-present credit card transactions for the three domains involved: Issuer domain of the card issuing bank, the Interoperability domain of the card scheme's infrastructure and the Acquirer domain of the merchants. The second version of the standard, 3D Secure 2 (3DS2) (EMV 3-D Secure protocol), is facilitated by EMVCo, a six member consortium comprised of American Express, Discover, JCB, Mastercard, UnionPay and Visa. It creates a frictionless payment experience for cardholders by facilitating a richer cardholder data exchange, allowing risk-based authentication by issuers for low risk transactions, instead of authentication challenges to the cardholder, such that most authentication activity will be invisible to the cardholder. 3DS2 also supports authentication of app-based transactions on mobile and other consumer connected devices, and cardholder verification for non-payment transactions, such as adding a payment card to a digital wallet.

Term	Acronym	Definition
3DS Client		The consumer-facing component, such as a browser-based or mobile app online shopping site, which facilitates consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.
3DS Integrator		An EMV 3-D Secure participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer.
3-D Secure Provider		An entity such as American Express, Diners Club International, Discover, JCB, Mastercard or Visa, which provides interoperability services for issuers and merchants who participate in the authentication process. The 3-D Secure provider is normally in charge of managing the directory server, managing the authentication history server and issuing the digital certificates required for participation in the authentication scheme.
3DS Requestor		The initiator of the EMV 3-D Secure Authentication Request, known as the AReq message. For example, this may be a merchant or a digital wallet requesting authentication within a purchase flow.
3DS Requestor App		An App on a Consumer Device that can process a 3-D Secure transaction through the use of a 3DS SDK. The 3DS Requestor App is enabled through integration with the 3DS SDK.
3DS Requestor Environment		This describes the 3DS Requestor controlled components of the Merchant / Acquirer domain, which are typically facilitated by the 3DS Integrator. These components include the 3DS Requestor App, 3DS SDK, and 3DS Server. Implementation of the 3DS Requestor Environment will vary as defined by the 3DS Integrator.
Three Domain Secure Software Development Kit	**3DS SDK**	3-D Secure Software Development Kit. A component that is incorporated into the 3DS Requestor App. The 3DS SDK performs functions related to 3-D Secure on behalf of the 3DS Server.
3DS Requestor Initiated	**3RI**	3-D Secure transaction initiated by the 3DS Requestor for the purpose of confirming an account is still valid. The main use case being recurrent transactions (TV subscriptions, utility bill payments, etc.) where the merchant wants perform a Non-Payment transaction to verify that a subscription user still has a valid form of payment.
3DS Server		Refers to the 3DS Integrator's server or systems that handle online transactions and facilitate communication between the 3DS Requestor and the Directory Server.

Term	Acronym	Definition
3-D Secure	**3DS**	**Three Domain Secure**. An eCommerce authentication protocol that for version 2 onwards enables the secure processing of payment, non-payment and account confirmation card transactions.
Access Control Server	**ACS**	A component that operates in the Issuer Domain, which verifies whether authentication is available for a card number and device type, and authenticates specific Cardholders.
Accountholder Authentication Value	**AAV**	A value providing proof of cardholder authentication, which is generated by the issuer's access control server for each transaction. The AAV is passed by the merchant to the acquirer and then by the acquirer to the issuer through the UCAF field.
Acquirer		A financial institution that has a relationship with a merchant and processes payment transactions for that merchant.
ActiveAccess		GPayments' access control server for card issuers and service providers.
ActiveDevice		GPayments' device agnostic two-factor authentication component.
ActiveMerchant		GPayments' payment authentication platform (merchant plug-in) for merchants.
ActiveServer		GPayments' 3DS Server for payment processors and merchants (see *3DS Server*).
Attempts		Used in the EMV 3DS specification to indicate the process by which proof of an authentication attempt is generated when payment authentication is not available. Support for Attempts is determined by each DS.
Authentication		In the context of 3-D Secure, the process of confirming that the person making an eCcommerce transaction is entitled to use the payment card.
Authentication Device		A physical device capable of generating a token to be used in the verification of a user's identity.
Authentication Request Message	**AReq**	An EMV 3-D Secure message sent by the 3DS Server, via the DS, to the ACS to initiate the authentication process.

Term	Acronym	Definition
Authentication Response Message	**ARes**	An EMV 3-D Secure message returned by the ACS, via the DS, in response to an Authentication Request message.
Authentication Token		An unpredictable piece of information generated by an authentication device, which is used to verify the identity of a user. The term token may sometimes be used to refer to the physical device that generated the token as well.
Authentication Value	**AV**	A cryptographic value generated by the ACS to provide a way, during authorisation processing, for the authorisation system to validate the integrity of the authentication result. The AV algorithm is defined by each Payment System.
Authorisation		A process by which an Issuer, or a processor on the Issuer's behalf, approves a transaction for payment.
Authorisation System		The systems and services through which a Payment System delivers online financial processing, authorisation, clearing, and settlement services to Issuers and Acquirers.
Bank Identification Number	**BIN**	The first six digits of a payment card account number that uniquely identifies the issuing financial institution. Also referred to as an Issuer Identification Number (IIN) in ISO 7812.
BankNet		Mastercard's proprietary payment network.
Base64		Encoding applied to the Authentication Value data element as defined in RFC 2045.
Base64 URL		Encoding applied to the 3DS Method Data, Device Information and the CReq/CRes messages as defined in RFC 7515.
Card		Card is synonymous with the account of a payment card, in the *EMV 3-D Secure Protocol and Core Functions Specification*.
Certificate Authority	**CA**	
Cardholder		An individual to whom a card is issued or who is authorised to use that card.

Term	Acronym	Definition
Cardholder Activation During Shopping		A 3D-Secure 1 process by which cardholders can enrol with the authentication system at the time of making a purchase at a participating merchant eCommerce website.
Centralised Authentication and Authorisation Service	**CAAS**	A remote ACS, see *Access Control Server*.
Challenge		The process where the ACS is in communication with the 3DS Client to obtain additional information through Cardholder interaction.
Challenge Flow		A 3-D Secure flow that involves Cardholder interaction as defined in the *EMV 3-D Secure Protocol and Core Functions Specification*.
Challenge Request Message	**CReq**	An EMV 3-D Secure message sent by the 3DS SDK or 3DS Server where additional information is sent from the Cardholder to the ACS to support the authentication process.
Challenge Response Message	**CRes**	The ACS response to the CReq message. It can indicate the result of the Cardholder authentication or, in the case of an App-based model, also signal that further Cardholder interaction is required to complete the authentication.
Chip Card		A card with an on-board integrated circuit chip.
Consumer Device		Device used by a Cardholder such as a smartphone, laptop, or tablet that the Cardholder uses to conduct payment activities including authentication and purchase.
Cryptography		A process that encrypts information for the purpose of protecting it. Information is decrypted when required.
Device		see *Authentication Device*.
Device Channel		Indicates the channel from which the transaction originated. Either: • App-based (01-APP) • Browser-based (02-BRW) • 3DS Requestor Initiated (03-3RI)
Device Information		Data provided by the Consumer Device that is used in the authentication process.

Term	Acronym	Definition
Directory Server	**DS**	A server component operated in the Interoperability Domain; it performs a number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Directory Server Certificate Authority	**DS CA** or **CA DS**	A component that operates in the Interoperability Domain; generates and Certificate Authority (DS distributes selected digital certificates to components participating in 3-D Secure. Typically, the Payment System to which the DS is connected operates the CA.
Directory Server ID (directoryServerID)		Registered Application Provider Identifier (RID) that is unique to the Payment System. RIDs are defined by the ISO 7816-5 standard.
Electronic Commerce Indicator	**ECI**	Payment System-specific value provided by the ACS to indicate the results of the attempt to authenticate the Cardholder.
Digital Signature		Equivalent of the physical signature in the digital world. Digital signatures can verify the identity of owner of a piece of information or a document in the digital world.
Enrolment		A cardholder must pass an initial online authentication procedure in 3D-Secure 1, which is verified by the Issuer prior to gaining eligibility for participation in American Express SafeKey, Diners Club International ProtectBuy, JCB J/Secure, Mastercard SecureCode or Verified by Visa authentication.
Frictionless		Used to describe the authentication process when it is achieved without Cardholder interaction.
Frictionless Flow		A 3-D Secure flow that does not involve Cardholder interaction as defined in EMVCo Core Spec Section 2.5.1.
Issuer		A financial institution that provides cardholders with credit cards.
J/Secure		JCB's standard for cardholder authentication, based on 3-D Secure.
Message Authentication Code	**MAC**	

Term	Acronym	Definition
Mastercard SecureCode / Identity Check		Mastercard's payer authentication brand, which includes SPA Algorithm for the Mastercard Implementation of 3-D Secure, SPA and chip card authentication program (CAP).
Mastercard 3-D Secure		The SPA Algorithm for the Mastercard Implementation of 3-D Secure that provides a browser authentication experience to the cardholder (see also *3-D Secure)*.
Mastercard Identity Check		see *Mastercard SecureCode / Identity Check*.
Merchant		Entity that contracts with an Acquirer to accept payments made using payment cards. Merchants manage the Cardholder online shopping experience by obtaining the card number and then transfers control to the 3DS Server, which conducts payment authentication.
Merchant Plug-in (MPI)		A software module which can be integrated into a merchant's eCommerce website or run as a managed service on behalf of a number of merchants to provide 3-D Secure authentication.
Non-Payment Authentication	**NPA**	.
One-Time Passcode	**OTP**	A passcode that is valid for one login session or transaction only, on a computer system or other digital device.
Out-of-Band	**OOB**	A Challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed. ACS authentication methods or implementations are not defined by the 3-D Secure specification.
Payer Authentication Request	**PAReq**	Message sent from the MPI to the Access Control Server at the cardholder's issuer via the cardholder browser.
Payer Authentication Response	**PARes**	A digitally signed message sent from the Access Control Server to the Merchant Plug-in which communicates whether the cardholder authentication was successful or not.

Term	Acronym	Definition
Payment Gateway		A software system provided by an acquirer or a third party which accepts transactions from the Internet and transfers them to a payment network such as BankNet or VisaNet.
Preparation Request Message	**PReq**	3-D Secure message sent from the 3DS Server to the DS to request the ACS and DS Protocol Versions that correspond to the DS card ranges as well as an optional 3DS Method URL to update the 3DS Server's internal storage information.
Preparation Response Message	**PRes**	Response to the PReq message that contains the DS Card Ranges, active Protocol Versions for the ACS and DS and 3DS Method URL so that updates can be made to the 3DS Server's internal storage.
Proof or authentication attempt		Refer to Attempts.
ProtectBuy		Diners Club International and Discover standard for cardholder authentication, based on 3-D Secure.
Registered Application Provider Identifier	**RID**	Registered Application Provider Identifier (RID) is unique to a Payment System. RIDs are defined by the ISO 7816-5 Standard and are issued by the ISO/IEC 7816-5 Registration Authority. RIDs are 5 bytes.
Results Request Message	**RReq**	Message sent by the ACS via the DS to transmit the results of the authentication transaction to the 3DS Server.
Results Response Message	**RRes**	Message sent by the 3DS Server to the ACS via the DS to acknowledge receipt of the Results Request message.
Risk-Based Authentication	**RBA**	During risk-based authentication, the rich cardholder data exchanged in AReq is taken into account to determine the risk profile associated with that transaction. The complexity of the challenge is then decided based on the risk profile.
SafeKey		American Express standard for cardholder authentication, based on 3-D Secure.

Term	Acronym	Definition
Secure Payment Application (SPA)		Mastercard's payer authentication standard designed to reduce online credit card fraud and chargeback using a client-side applet. Also known as Mastercard's PC Authentication Program, Mastercard SecureCode, Mastercard SPA and SPA.
Secure Sockets Layer (SSL)		A protocol designed to maintain the integrity and confidentiality of communication over the Internet.
SecureCode		see *Mastercard SecureCode / Identity Check*.
Token:		see *Authentication Token*.
Two Factor Authentication		see *2-F Authentication*
Uniform Resource Locator (URL)		Address system for locating unique sites on the Internet.
Universal Cardholder Authentication Field (UCAF)		Data element 48 sub element 43 as defined in Mastercard BankNet to carry authentication data. Mastercard SecureCode uses this element to transport AAV from the acquirer to the issuer.
Verified by Visa	**VbV**	A payer authentication standard introduced by Visa (see *3-D Secure*).
VisaNet		Visa's proprietary payment network.
Visa Secure		A program developed by Visa to make online payments more secure through 3-D Secure 2.

Document Control

+ new item Δ item changed X item removed 🟦 no change to item

Date	AA Ver	Doc Ver	Change Details
[06/11/2019]	8.0.3	8.0.3:1	**Risk Engine Adapter** (Specifications) Δ Change made to AdapterInfo Data Elements: Removed round brackets fr **Token** Sample Value. Δ Change made to AssessmentResult Data Elements: Change the descript `whatToDoNext` + Add `range` field into ConditionValue Data Elements
09/10/2019	8.0.2	8.0.2:2	**Remote Messaging** (Specifications) Δ 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 valu
			Risk Engine Adapter (Specifications) Δ **Risk chain setup diagram** updated.
02/10/2019	8.0.2	8.0.2:1	**Installation** (Installation Guide) Δ 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) + **Response code = 3** added.
			Transaction Status Codes + New Transaction Status Codes page added.
05/09/2019	8.0.1	8.0.1:1	**Product Architecture** (Installation Guide) Δ Disaster Recovery and Clustering diagrams added.

Date	AA Ver	Doc Ver	Change Details
			Installation (Installation Guide) Δ Changes made to Upgrades to v8.0.x and New installations.
			Security (Admin UI) + Create Certificate Request: New **Key type** field added.
			Risk Engine Adapter (Specifications) Δ **ParameterDataElements**: **Validator** field description updated Δ **RemoteAssessmentRequest Data Elements**: **PreviousData** field format u + **AReqWithTransStatusDataElements** added Δ **AReq Data Elements**: **ThreeDSCompInd** and **ThreeDSRequestorAuthenticationInd** field updated.
			Remote Messaging (Specifications) Δ **InitAuthReq** table: Usage of **oobInfo** changed.
			Out of Band (OOB) Authentication Adapter (Specifications) Δ Change the URL in **Restful API version of OOB Adapter** Δ Change `NOT__AUTHENTICATED` to `NOT_AUTHENTICATED` Δ Update MobilePhone Data Elements, HomePhone Data Elements, and W Data Elements.
15/08/2019	8.0.0	8.0.0:1	**Product Architecture** (Installation Guide) Δ Components labelled with (3DS1) or (3DS2) as relevant + Challenge Server (3DS2) added. + Risk Engine Adapter added + Out of Band (OOB) Authentication Adapter added Δ Logical view of ActiveAccess diagram updated Δ Hardware and Software Requirements updated X Removed references to **RuPay** components.
			External Components (Installation Guide) Δ Application Server dependency removed, supports compatible Java Appl Servers.
			Installation (Installation Guide) Δ ActiveAccess installation and setup process simplified.

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

Date	AA Ver	Doc Ver	Change Details
			Local Messaging (Specifications) Δ Final Registration Request: updated with OOB device registration request
			Remote Messaging (Specifications) Δ **Transaction** table: **issuerName** and **theeDSProtocolVersion** added + **HeaderParams** table added + **AdditionalParams** table added + **PreAuthResp** table: **AuthType** added + **InitAuthReq** table: new OTP types for **AuthType** and **oobInfo** added Δ Sample Request Response: changed **CVD** to NULL.
			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. Δ **See Documentation change details** for full details of the changes in the documentation moving from PDF to online format.
26/02/2019	**7.4.6**	**7.4.6.1**	**Remote Messaging** Δ **initAuthReq** table: added AuthType Δ **CardInfo** table: RegToken definition updated.
06/07/2018	**7.4.0**	**7.4.0:1**	+ Addition of options in **System Management > Settings** to allow administr specified access levels to view Card Number (plaintext) and AAV/CAVV/AEV Δ Updated description of Soft Launch List + Addition of ActiveAccess Error Codes in Appendix A.

Documentation change details

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
Introduction		
Installation Guide >		A11-Install_Maint_TechRef.pdf
	Product Architecture	
	External Components	
	Installation	
Administration UI >		AA12-ActiveAccess Administration.pdf
	About the Issuer Administration Server	AA12 / Added support for two-factor authentication for logging into the Administration UI
	System Management >	AA12
	About System Management	AA12
	Settings	AA12
	ACS Settings	AA12
	Issuer Management	AA12
	- Group Management	AA12
	- *Authentication Mgmt >*	+ **New Subsection**
	- About Authentication Management	+ **New**

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	- Devices	Δ AA12, previously Device Management
	- Risk	➕ **New**
	- OOB	➕ **New**
	Public & Encryption Key Management	AA12
	Exchange Configuration	AA12
	Archive Management	AA12
	Security	AA12
	- Issuer Certificate	AA12
	- AHS Certificate	AA12
	- CAAS Certificate	AA12
	- Directory Server Certificate	➕ **New**
	- OOB Certificate	➕ **New**
	- Risk Certificate	➕ **New**
	- CA Certificate	AA12
	Servers	AA12
	- MIA Servers	AA12
	- Access Control Servers (ACS)	AA12
	- Authentication History Servers (AHS)	AA12

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	- Centralised Authentication and Authorisation Servers (CAAS	AA12
	- Out of Band Authentication Servers (OOB)	AA12
	- Risk Servers	AA12
	Utilities >	
	Utilities	AA12
	Key Retiring Utility	AA12
	Issuers	AA12
	- Settings	AA12
	- Upload Registration Files	AA12
	- Custom Pages	AA12
	- Key Management	AA12
	Rules	
	- Registration -- Amount Threshold -- Merchant Blacklist	AA12
	- Authentication -- Soft Launch List Rule -- Merchant Whitelist Rule -- Merchant Watchlist -- Location Watchlist - Location Watchlist Search Results -- Domestic & International Transaction Amount Threshold -- Stand-In Transaction Threshold	AA12

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	- Settings	AA12
	Admin Users	AA12
	Cards	AA12 Δ **Users** renamed to **Cards**
	Transactions	AA12
	Reporting	AA12
	Audit Log	AA12
	Profile Management_	AA12
Specifications		
	Local Messaging >	
	Local Messaging	AA61-Messaging Specification.pdf
	Card Loader	AA32-GPayments Card Loader.pdf
	Remote Messaging >	
	Remote Messaging	AA71-Remote System Messaging Specification.pdf
	Country and Currency Codes	AA71-Remote System Messaging Specification.pdf Appendix A
	Sample Card	AA71-Remote System Messaging Specification.pdf Appendix B
	Sample Request Response	AA71-Remote System Messaging Specification.pdf Appendix C
	SMS via JMS	AA83-ActiveAccess - SMS via JMS Library.pdf
	Out of Band Authentication Adapter	➕ **New**

Online Main Menu	Sub Menus	Previous PDF Document / Latest Changes
	Risk Engine Adapter	➕ **New**
Error Codes		AA12 - Appendix A
Glossary		AA12
Document Control>		
	Document Control	AA12
	Documentation Changes (*this page*)	➕ **New**
Release Notes		Δ Previously included in the ActiveAccess package
Legal Notices		AA12

Release Notes

ActiveAccess v8.0.4

[06/11/2019]

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

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

Type	Issue Number	Description	Components
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

This work is Copyright © 2003-2019 by GPayments Pty Ltd. All Rights Reserved. No permission to reproduce or use GPayments Pty Ltd copyright material is to be implied by the availability of that material in this or any other document.

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.