Manage merchants

To allow merchants to make authentication requests via the authentication API, a merchant entity needs to be created and the client certificate for its 3DS Requestor downloaded. Details that are included in an authentication request, and do not change very often, are stored in the database to simplify the API functionality. The **create**, **view**, **edit** and **delete** processes for merchant entities are detailed below.

Create a merchant

To create a merchant, first head to the **Merchants** page on the administration interface and select the ***New*** button.

On the **New merchant** screen use the fields described below to create a new merchant.

> **User Access**
>
> A user requires the **Business admin** role to create merchants.

> **Important**
>
> When creating a merchant or editing a merchants details, note that the combination of **Merchant name** and **Merchant ID** must be unique.

Details

These are the general merchant details used for authentication requests:

- **Merchant name** - Merchant name assigned by the Acquirer. This should be the same name used in the authorisation message request. *Required, Maximum 40 characters*
- **Merchant ID** - Merchant identifier assigned by the Acquirer. This should be the same name used in the authorisation message request. *Required, Maximum 35 characters*

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

- **Country** - country that the merchant operates from. As part of an authentication request, ActiveServer will use this entry and convert it to the **Merchant Country Code** and it should match the value used in the authorisation message request. *Required*
- **Default currency** - default currency that will be used in an authentication request. This value can be overwritten in the browser based init API call by specifying the `purchaseCurrency`. *Required*
- **3DS Requestor URL** - fully qualified URL of the 3DS Requestor website or customer care site. This data element provides additional information to the receiving 3-D Secure system, if a problem arises, and should include contact information. *Required*
- **Status** - status to indicate whether the merchant is **enabled** or **disabled**. Disabling a merchant will not allow authentication API requests for that specific merchant. *Required*
- **Notes** - optional section to allow an admin user to access and edit notes for the merchant.

> **User Access**
>
> A user requires the **Business admin** role to view and edit the **Status** and **Notes** fields.

Card Schemes

These are the card scheme specific details used for authentication requests:

- **Acquirer BIN** - acquiring institution identification code as assigned by the DS that is receiving the AReq message. Can be entered manually or pre-filled by choosing an existing acquirer from the **drop down list**. *Maximum 11 characters*
- **Requestor ID** - DS assigned 3DS Requestor identifier. Each DS will provide a unique ID to each 3DS Requestor on an individual basis after 3DS2 merchant on boarding is complete. *Maximum 35 characters*
- **Requestor name** - DS assigned 3DS Requestor name. Each DS will provide a unique name to each 3DS Requestor on an individual basis after 3DS2 merchant on boarding is complete. *Maximum 40 characters*
- **Category code** - DS specific code describing the Merchant's type of business, product or service. *Maximum 4 characters*
- **Merchant ID** - Each card scheme can have an override value for Merchant ID. If this value is provided, it will be used instead of the default Merchant ID value in the merchant details only when that specific card scheme is used. *Optional, Maximum 35 characters*

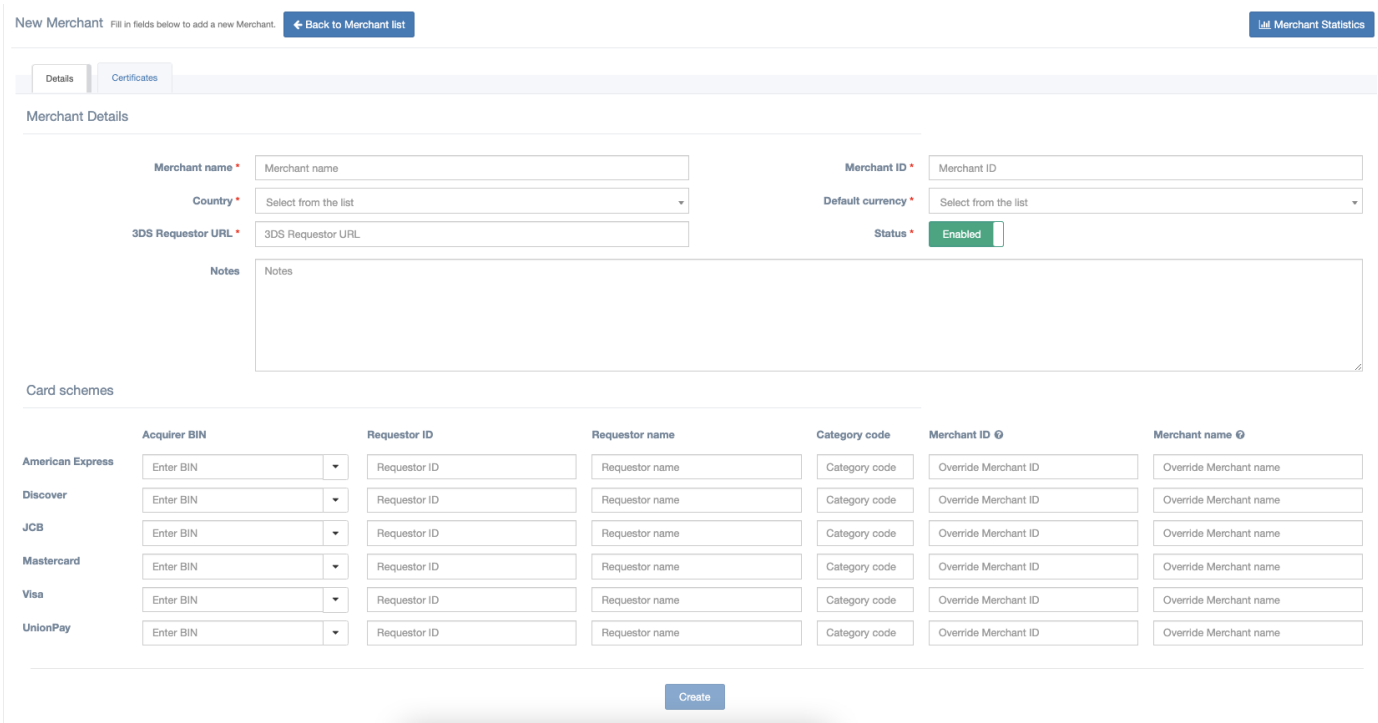
Copyright ©2019 GPayments Pty Ltd. All rights reserved.

- **Merchant name** - Each card scheme can have an override value for Merchant name. If this value is provided, it will be used instead of the default Merchant name value in the merchant details only when that specific card scheme is used. However, if the `merchantName` field is provided in the Auth API request, the API request field will take precedence. *Optional, Maximum 40 characters*

> **Warning**
>
> All the above card scheme specific details are required to be supplied in an authentication request. If any of them are missing, the authentication request will fail.

View Merchant Details

To view merchant details, search for the merchant on the **Merchants** page of the administration interface. Select the Merchant in the Merchant list and view the **Details** tab.

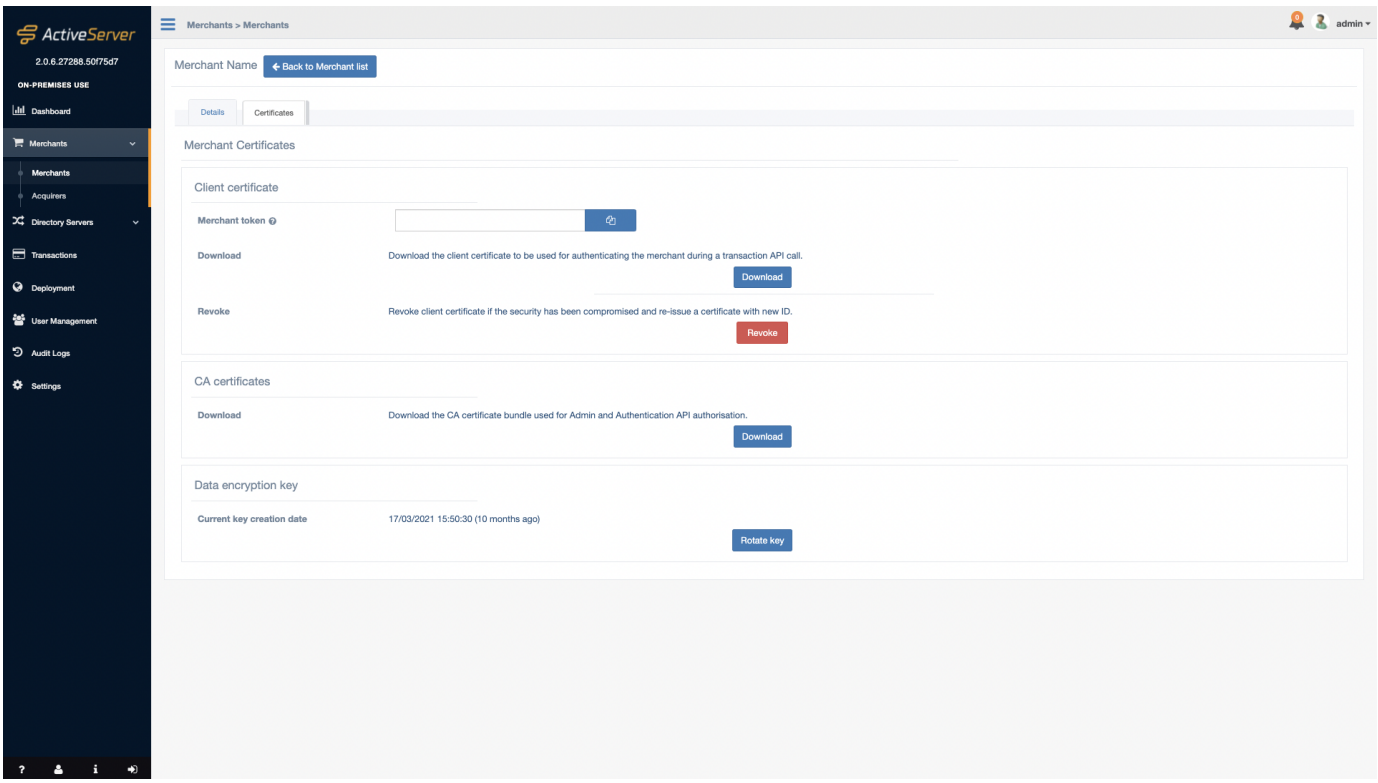


View Merchant Certificates

The Merchant's **Client Certificate** and **Merchant token**, as well as the server CA certificates, can be accessed from the **Certificates** tab. In addition, the user can manage the **Data Encryption Key** for security purposes.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

> **Tip**
>
> Certificate management is only available once the instance has been activated.



Client Certificate

The 3DS Requestor client certificate is required for a merchant to include in the authentication API requests for SSL authentication:

- **Certificate Algorithm** - AES256 provides stronger security using modern encryption standards. LEGACY provides broader compatibility using older encryption standards.
- **Tracker** - When enabled, the expiry date is tracked each time a certificate is downloaded. Business Admins and System Admins will receive an email notification when the certificate is 90 days or less away from expiring.
- **Merchant token** - token to be added in HTTP header of an authentication API request. Only required if using a Master Auth API client certificate to authenticate on behalf of a merchant. This field will only be visible to a user with a **Business admin** role, as this is the only role with access to the Master Auth API client certificate. For information on using the master certificate with the merchant token, refer here.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

- **Download** - Allows the user to download a `zip` file containing the 3DS Requestor client certificate in a **.p12** format, which is used for authentication API requests, and a `metadata.txt` file. The `.p12` file is protected by a generated secure random password (16 characters):
  - **Administration UI v2** - the password is **not** included in the zip file. After selecting **Download**, the **Save your merchant client certificate password** dialog shows the password once. Copy it or select **Show password**, store it securely, then select **Download certificate bundle**. Select **I have saved it** to close the dialog. The password cannot be shown again; if it is lost, download a new certificate.
  - **Classic Administration UI** - the password is included in `metadata.txt` as `P12-Password`.

  `metadata.txt` contains the following information:
  - `Owner` - The merchant name.
  - `Type` - The certificate type, `AuthAPI`.
  - `P12-Filename` - The filename of the P12 file. Example: cert-b1cdf956-a4f4-4ce4-ade6-cd84d68e59f2.p12
  - `P12-Password` - The password of the P12 file. Classic Administration UI only.
  - `Created-Date` - The date and time in UTC which the P12 file was generated. Format: `yyyy-MM-dd'T'HH:mm:ss` Example: 2023-12-12T10:01:15
  - `Expiry-Date` - The date and time in UTC which the client certificate file will be expired. The client certificate file will be invalid after the expiry date, please re-download a new one before the expiry date. Format: `yyyy-MM-dd'T'HH:mm:ss` Example: 2025-12-12T10:01:15
  - `Description` - The encryption used for the P12 file, based on the selected **Certificate Algorithm**.

    > **Client certificate expiry**
    >
    > Downloaded client certificates have a **2 year expiry** from date of download for security reasons. Ensure that all certificates are renewed before this expiry date, **otherwise API requests will be rejected due to an expired certificate error**.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

For more information on this functionality, see the API document overview.

- **Revoke** - disables the current 3DS Requestor client certificate if there has been a security breach or lost certificate, then re-issues a new certificate which can be downloaded and provided to the merchant.

> **Warning**
>
> **Revoking** a client certificate will invalidate all instances of the certificate, and the merchant will not be able to initiate API requests until the replacement certificate can be installed.

CA Certificates

- **Download** - allows the download of the servers CA certificates, to be used in authentication API requests. For more information on this functionality, see the API document overview.

> **Version 1.0.5**
>
> CA certificate download was added in the version 1.0.5 release.

> **User Access**
>
> A user requires the **Business admin**, **Merchant admin** or **Merchant** role to download a certificate.
> A user requires the **Business admin** or **Merchant admin** role to revoke a certificate.

Data encryption key

There is a key assigned for every merchant which **ActiveServer** uses to encrypt the requests and responses for all authentications prior to saving them in the database. This key is also used to decrypt the account number used for the transaction when searching for transactions.

- **Rotate key** - used for changing the current data encryption key, in use, if required, e.g. for internal or external policies requiring the rotation of encryption keys. Old key will still be available to be used for decrypting/encrypting the old transactions. New key will be used for transactions performed after the rotation.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

User Access

A user requires the **Business admin** or **Merchant admin** role to rotate a key.

Edit merchant details

To edit a merchant, view its profile and edit its available fields.

The merchant profile details available are specific to user roles:

- **Status** - the enabled status is only available to users with the **Business admin** role.
- **Notes** - the notes section is only available to users with the **Business admin** role.

User Access

A user requires the **Business admin**, **Merchant admin** or **Merchant** role to view merchant details.
A user requires the **Business admin** or **Merchant admin** role to edit merchant details.

Delete a merchant

To delete a merchant, first head to the **Merchants** page on the administration interface, search for the merchant and select the **delete check box** adjacent to the Merchant name, in the search result table. Select the ***Delete*** button and confirm on the dialogue box.

Important

The default **Test Merchant** cannot be deleted, as it is used for testing purposes.

User Access

A user requires the **Business admin** role to delete merchants.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.