fiserv.

Merchant Care Service

User Guide

Introduction

The Fiserv's Merchant Care Service is the tool used for multiple purposes; to board merchants on the Internet Payment Gateway's (IPG) Virtual Terminal (VT), Hosted Payment Pages (Connect) and APIs on behalf of the distribution channels set up as resellers, updating Merchant master data and deleting existing merchants.

This document is for internal use only for Operational areas to understand the boarding, amending and deletion of Merchants and for Customer Service Support teams to see how they can find information on the Merchant and transactions made.

Merchant Care Service is available in German, English, Portuguese and Spanish.

1   Accessing Merchant Care Service
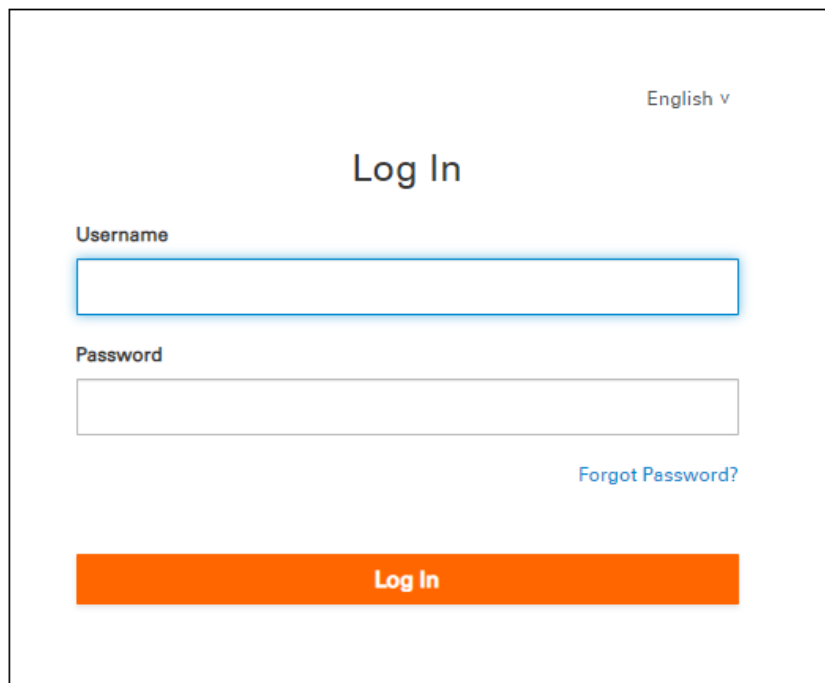
1.1   URL

You should have been issued with logon details for MCS. If not please contact your dedicated MCS administrator to request your logon profile.

To access MCS, click on https://www.ipg-online.com/mcs

1.2   Login

After browsing to your application (and you are not already logged in) you will be redirected to the login screen:

After Pressing the "LOG IN"- button you normally will be redirected to you application.

1.3 Initial password is set for your account after a login

If your account was setup with an initial password you have to reset your password before usage.You can also change your password using the link in the MCS after you have successfully logged in.
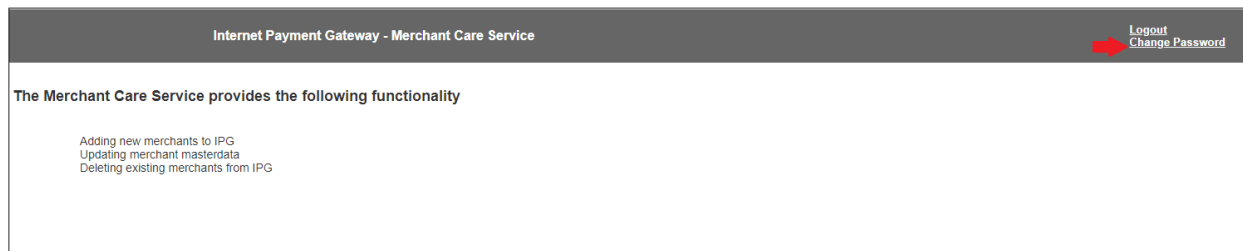
When you signed in you will be taken to the Merchant Care Service menu:
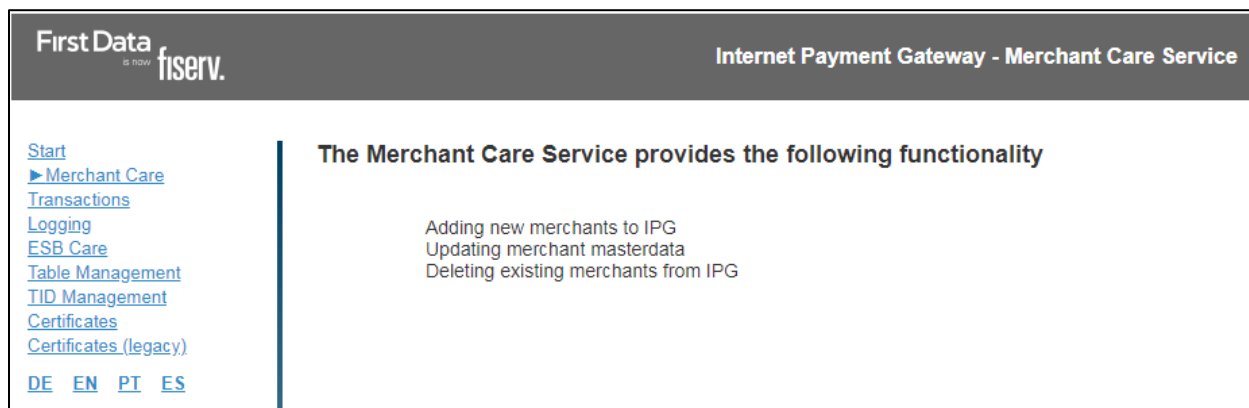
2 Merchant Care

There are 2 options that can be selected under Merchant Care; Search Merchant and New Merchant.

2.1   New Merchant

To board a new merchant you need to access 'New Merchant' from this menu. You will then be presented with the Merchant Masterdata screen.

Note, that you can also search for an existing store by using 'Search Merchant' option first. After doing so, you can select an existing store and use it as a template, by selecting a button 'Use as Template', what allows you to re-use some of the settings and finalize a new store setup relatively quickly.

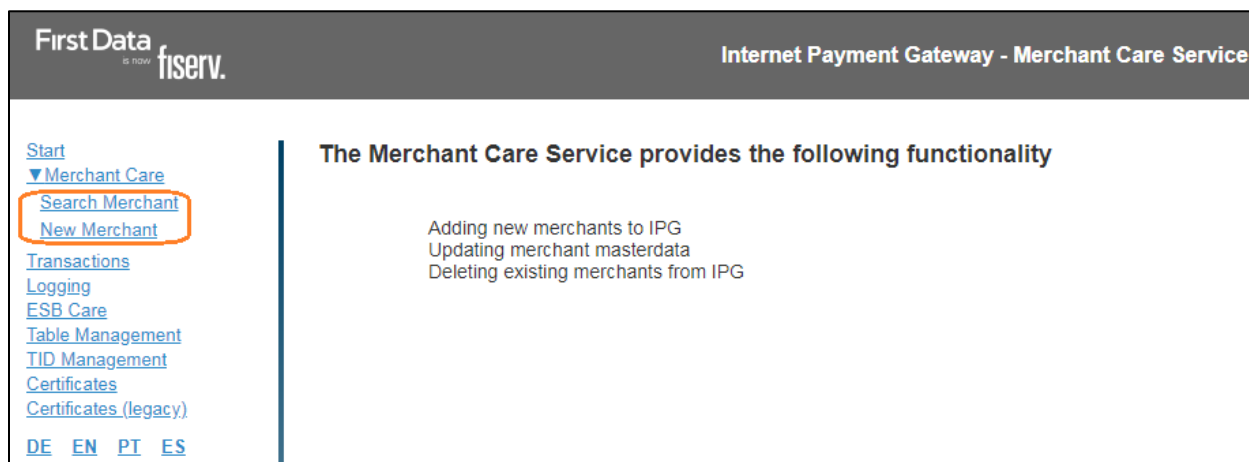### 2.1.1   Merchant Masterdata

Complete the relevant fields, using drop boxes where available. The fields marked with a red dot are mandatory, and the URL and MCC fields are mandatory if the merchant requires a 3-D Secure service.

Master | Address | Contact | Service | Terminal | Purchase Limits | Fraud | Connect Logos

Merchant Masterdata

● Reseller	CBD	⌄
● Store Id	8125	09950006
MCC	1234	
● Legal Name	CBD Demo Store	
ISP eMail		
URL	https://www.test.com	
● Default Ccy Code	AED ⌄	
Timezone	Asia/Dubai ⌄	
Status	OPEN ⌄	
Open Date	12.05.2022	
Close Date		
National Tax ID		
Individual Tax ID		
● DBA	CBD Demo	
● Acquirer	Dummy-3DS2 ⌄	
Country of Governmental Control	⌄	
Sender Account Number		
Sender Account Type	⌄	

Next

Save All

- **Store Id** - consists of 2-4 digits reseller prefix (provided by IPG) and a sequence number, no characters are allowed. Store Id has a 13 character limitation.
- **MCC (Merchant category code)** - This is not a mandatory field if the merchant is not using 3DS 2.0 authentication. If you are entering the MCC for a store, please ensure it is correct. Entry of the invalid MCC results in clearings transactions being rejected. Should you be boarding a

merchant to support a specific MCC driven addendum this field will become mandatory and an error message will be shown if you are missing this information upon completion.

- **Legal Name** - Merchant's official name as written in a legal documents
- **Reseller** - reseller name setup in the Gateway; automatically populated
- **URL** - this field needs to be populated with the merchant's official URL in case 3-D Secure service is being used
- **Default Ccy Code** - represents the default currency of the reseller, it is populated automatically during manual boarding process
- **Timezone** - represents the time zone, where merchant operates
- **Status** - When this is set to CLOSED, the Store cannot process transactions anymore. Users of this Store will however still be able to log in to the Virtual Terminal to see Reports of historical transactions (what they can't if the Store gets completely deleted).
- **National Tax ID** and **Individual Tax ID** are only required for the stores located in Brazil.
- **DBA** - The merchant's "Doing Business As" name (which can differ from the officially registered company name).
- **Acquirer** - This is related to the 3-D Secure functionality. Choose the correct acquirer as applicable for your store from the dropdown values.
- **Country of Governmental Control** - required for merchants falling into governmental control category, the country to be selected from dropdown list
- **Sender Account Number** - Required for VISA OCT transactions. If entered, account type must be chosen as well.
- **Sender Account Type** - Required for VISA OCT transactions. Defines the type of the entered account number.

When you have completed all fields click 'Next' to save the data and proceed to the next page.

2.1.2 Address

Enter the address that the merchant wishes to appear on their receipts should they opt to provide them. If the merchant has an Irish address without a zip/postcode, please enter IE into the ZIP field. If the merchant is outside of US, please keep the field **"State"** blank.

The country code field dictates which language the Virtual Terminal will be set for the merchant. When you have completed all fields click 'Next' to save the data and proceed to the next page.

Master | Address | Contact | Service | Terminal | Purchase Limits | Fraud | Connect Logos

Address

Store Id: 812509950006

🔴 Address Type	MainAddress ▾
🔴 Address 1	Street 1
Address 2	
🔴 City	Dubai
State	
🔴 ZIP	12345
🔴 Country Code	Unit.Arab Emir. ▾

[Previous] [Next]

[Save All]

2.1.3   Contact

Enter the details for the merchant's principal contact, the red dot signifying mandatory fields.

Master | Address | Contact | Service | Terminal | Purchase Limits | Fraud | Connect Logos

Contact

Store Id: 812509950006

🔴 Contact Type	Principal ▾
🔴 Name	Name Surname
🔴 Email	name.surname@merchant.com
🔴 Phone	12354657
Fax	

[Previous] [Next]

[Save All]

When you have completed all fields click 'Next' to save the data and proceed to the next page.

2.1.4 Service

Under the service tab is a drop-down menu of services that can be added to that merchant:

Highlight the relevant services for the merchant one at a time and click on add. Once you have added all relevant services, complete the fields for each of the services before clicking on Next.

2.1.4.1 3-D Secure (MCSC / VbV)

Remove	Service Type	Configuration	
✖	3D Secure (MCSC / VbV)		Previous Show All 26 ⌄ Next
		TRAGhostCall	☐
		acquirerName	[ ]
		allowAuthenticationRetry	☐
		allowECI1andECI6	true ⌄
		allowECI7onIVRPAResUifInternational	☐
		allowMPIViaAPI	☑
		allowMPIViaRESTAPI	☑
		allowSoftDeclineRetry_Connect	☐
		allowSplitAuthentication	☑
		allowed3dsServerVersionMax	[⌄]
		amex3DSRequestorId	[ ]
		amexMID	[ ]
		declineSameAAV	☐
		declineSameXIDandECI	☐
		dinersMID	[ ]
		excludedCardCountries	[ ]
		iciciOnUsVereq	☐
		integration	Modirum3DSServer ⌄
		jcbMID	[ ]
		jcbPassword	[ ]
		maestroMID	[ ]
		mastercardMID	[ ]
		transactionRiskAnalysis	[⌄]
		visaMID	[ ]
		visaPassword	[ ]
		vmid	[ ]

- **TRAGhostCall** - related to Transaction Risk Analysis product (TRA), if activated the transaction data are shared with TRA Engine without additional risk evaluation with the goal to enhance the machine learning and merchant's transaction processing patterns. Please note that this feature is only available for selected resellers in EMEA region
- **acquirerName** - related to Transaction Risk Analysis product (TRA), where the merchant's acquirer name should be populated, please note that this feature is only available for selected resellers in EMEA region
- **allowAuthenticationRetry** - If this is activated, in case where the 3-D Secure authentication failed, the cardholders will see a hosted page where they can chose to retry the authentication. If the cardholder selects "No", the transaction will be finished as usual. If "Yes" is selected, the cardholder will again be redirected to the issuer's authentication screen.
- **allowECI1andECI6** - select if merchant is to allow Attempted authentications, otherwise they will decline. Please note, that the automatic decline does not apply to the following use cases: zero value authorizations, standing instructions, recurring transactions triggered by the Gateway's scheduler.
- **allowECI7onIVRPAResUifInternational** - for Indian market only - if this is activated, the transactions, that are triggered through IVR, but are with international cards (which cannot be authenticated through IVR) are handled as a standard eCommerce transaction without 3-D Secure (i.e. ECI 7), otherwise authentication fails.
- **allowIVR** - for Indian market only - if this is activated, 3-D Secure authentication via IVR is enabled for the merchant
- **allowMPIviaAPI** - if this is activated, 3-D Secure authentication could be processed via API WS
- **allowMPIViaRESTAPI** - if this is activated, 3-D Secure authentication could be processed via REST API
- **allowSplitAuthentication** - if this is activated, the merchant is allowed to use split authentication functionality
- **allowed3dsServerVersionMax** – represents maximum 3DS protocol version to be processed through Fiserv 3DS Server
- **amexMID** - Acquiring Merchant ID registered with Amex SecureKey program
- **amex3DSRequestorID** - related to merchant's enrollment with Amex SafeKey program 2.x, the ID to be provided by Amex during merchant registration process, until the field will be removed from the service, please use the default value = MER for all merchants
- **declineSameAAV** - If this is activated, transactions with a 3-D Secure Authentication Value (AAV/CAAV) that has already been used in a previous transaction will be declined.
- **declineSameXIDandECI** - If this is activated, transactions with a XID and ECI combination that has already been used in a previous transaction will be declined.
- **dinersMID** - acquiring Merchant ID registered with Diners/Discover ProtectBuy program
- **excludedCardCountries** - It relates to the Dynamic 3-D Secure based on the card issuer's country. You can exclude specific card transactions from the 3-D Secure authentication based on a certain country selection (i.e.: issuing country) e.g.: Germany, Switzerland and Austria, while apply the standard 3-D Secure authentication process for other transactions with card from other countries. The countries, which shall be excluded from 3DS authentication process have to be entered in ISO country code form (comma separated).
- **iciciOnUsVereq** - Alternative 3-D Secure Option for ON-US Transactions. This service has been implemented for cards issued by ICICI, the Fiserv acquiring joint venture partner in India.
- **integration** - used for determine which 3DS protocol version should be supported - select Modirum3DSServer for 3DS2.0, select ModirumLibrary for 3DS 1.0
- **jcbMID** - Merchant ID registered with JCB for J/Secure authentication
- **jcbPassword** - password provided by JCB for a certificate
- **maestroMID** - Merchant ID registered with Mastercard for 3-D Secure authentication with Maestro cards
- **mastercardMID** - Merchant ID registered with Mastercard for 3-D Secure authentication

- **visaMID** - Merchant ID registered with VerifiedByVisa program
- **visaPassword** - not required anymore. Had been used for a merchant-specific password provided by Visa when every single merchant had to be registered. Obsolete, will be removed.
- **transactionRiskAnalysis** - PSD2 related, the field to be populated with value 'RiskShield' if TRA product is used by a merchant, please note that the service is available only for selected resellers in EMEA region
- **vmid** - 8 characters Visa Merchant Identifier assigned to the merchants enrolled with Visa's Delegated Authentication program required for Trusted Merchant and Delegated Authentication purposes

2.1.4.2 API Webservice

API Webservice		
	allowGetLast	☑
	allowReturn_api	☑
	allowSale_api	☑

Only select if this is required for the merchant being built. This service offers the possibility to selectively enable or disable transaction types for a store per Interface. This functionality only works if the reseller service config "declineUnallowedTransactionType" is activated together with this extension.

2.1.4.3 Connect (Hosted Payment Page)

Connect (Hosted Payment Page)		
	allowExtendedHashCalculationWithoutCardDetails	☐
	allowMOTO	☐
	allowMaestroWithout3DS	☐
	allowVoid	☐
	cardCodeBehaviour	mandatory ▾
	checkoutOptionCombinedPage	☐
	hideCardBrandLogoInCombinedPage	☐
	overwriteURLsAllowed	☑
	responseFailureURL	
	responseSuccessURL	
	reviewURL	
	sharedSecret	sharedsecret / Generate Password
	skipResultPageForFailure	☐
	skipResultPageForSuccess	☐
	transactionNotificationURL	

- **allowExtendedHashCalculationWithoutCardDetails** - is to allow ExtendedHash calculation for Direct Post without PAN/CVV/Expiry Date
- **allowMOTO** – If selected this will allow the Connect merchant to perform MOTO transactions.
- **allowMaestroWithout3DS** - allows the merchant to skip 3DS for Maestro card via Connect
- **allowVoid** - If selected this will allow the merchant to void transactions via hosted payment page.
- **cardCodeBehaviour** – If selected the Connect transactions will check CVC/CV2. In case the service is setup with the value "mandatory" and the service "allowSplitAuthentication" is

activated, the merchants should pass CVC/CV2 value in their Sale/PreAuth API request again, even if shared before in PayerAuth, because the Gateway is not allowed to store CVC due to PCI DSS compliance rules.

- **checkoutOptionCombinedPage** - relevant for merchants not sending a "checkoutoption' parameter in their transaction request via Connect. If you want to make the Connect 'combinedpage' the default checkout option for them w/o a need for these merchants to update their integration, then please set this checkbox to 'true'.
- **hideCardBrandLogoInCombinedPage** - For merchants that let their customers select the payment method within their shop environment and do not want to distinguish between different card brands (but just card vs. alternative payment methods), the "combinedpage"-option now allows to remove the card brand logo from the form for the card details. This can be activated by setting the checkbox 'hideCardBrandLogoInCombinedPage' to 'true'. Then a merchant can send any valid/activated card brand value for the parameter 'paymentMethod' and the cardholder will see a hosted page for the card details entry with no card brand logo shown.
- **overwriteURLsAllowed** – If selected the merchant can manage the URLs using once in production (using Virtual Terminal).
- **responseFailure URL** – Select to customise the transaction page for failed transactions. Leave blank to allow the merchant to manage this (using Virtual Terminal).
- **responseSuccessURL** – Select to customise the transaction page for successful transactions. Leave blank to allow the merchant to manage this (using Virtual Terminal).
- **reviewURL** – Deprecated, formerly used for Masterpass purposes. Masterpass has been sunset in 2021.
- **sharedSecret** – Click on 'Generate Password' to automatically create a SharedSecret for the Merchant to be used in their integration
- **SkipResultPageForFailure** – If selected the Gateway will skip the transaction failure confirmation page. Available only in a design of the Connect 'classic' checkout option.
- **SkipResultPageForSuccess**– If selected the Gateway will skip the transaction success confirmation page. Available only in a design of the Connect 'classic' checkout option.
- **transactionNotificationURL** – The URL the merchant would like to receive transaction notifications. Leave blank to allow the Merchant to manage this (using Virtual Terminal). But make sure that the merchant's Notification URL is entered to the 'transactionNotificationURL' field in case the merchant is going to use the Payment URL.

2.1.4.4 Credit Card (Brands and Options)

Credit Card (Brands and Options)	
AVS	☑
Amex	☐
CUP	☐
Diners	☐
IPaddressInAuthRequest	☐
JCB	☐
Mastercard	☑
Visa	☑
allowCredits	☑
allowECI7_API	☑
allowECI7_Connect	☑
allowECI7_EPAS	☑
allowECI7_VT	☑
allowIncrementalPreauth	☑
allowOnlineAuthForRefund	☑
allowPurchaseCards	☐
allowZeroAmount	☑
cardCodeMandatory	☑

- **AVS** – Select to make Address Verification Service mandatory
- **Schemes** – Select which Schemes the Merchant will be supporting
- **IPaddressInAuthRequest** – relevant only for German merchants using authorization host GANS
- **allowCredits** – Select to allow Merchant to support transaction type = credit
- **allowECI7_API** – Select to allow Merchant to support eCommerce transactions with the webservice API
- **allowECI7_Connect** – Select to allow Merchant to support eCommerce transactions with Connect
- **allowECI7_EPAS -** Select to allow transactions with ECI 7 through the EPAS interface
- **allowECI7_VT** – Select to allow Merchant to support eCommerce transactions with the Virtual Terminal
- **allowIncrementalPreauth** - to enable transaction type Incremental preauthorization for the merchant.
- **allowOnlineAuthForRefund –** to enable online authorization for refund
- **allowPurchaseCards -** Select to allow Merchant to support Purchase Cards
- **allowZeroAmount** - leave blank to disable Zero $ Auth / Account authorization for the merchant.
- **cardCodeMandatory** – Select to make the CVV check mandatory in Virtual Terminal. Leave blank to allow the Merchant to manage this.

2.1.4.5 Hosted Data / Data Storage / Data Vault

Hosted Data / Data Storage / Data Vault		
	flagRecurring	☐

Select this to enable the Data Vault for the merchant and only tick the check box for 'flagRecurring' if you have been advised that the merchant needs this enabled, the default is for this not to be selected.

The *flagRecurring* option has been implemented for a special situation where the merchant triggers recurring transactions himself instead of using our scheduler. Nowadays, the appropriate way for this scenario is to submit a Recurring Type in the transaction request so this checkbox should not be ticked for any new merchant. If the check box is ticked, all transactions of the merchant where an existing Data Vault record is being used will be flagged as recurring in the message to the processing platforms. Tick this box only if explicitly advised.

2.1.4.6 Dynamic Currency Conversion

Dynamic Currency Conversion		
	api	☐
	connect	☐
	dynamicPricing	☐
	vt	☐

Select which integration component DCC is required for and/or select 'dynamicPricing' if the merchant would like the dynamic pricing functionality. If you are provided with a merchant commission band amend the zero to the correct band.

2.1.4.7 Maestro / Maestro UK / Laser Setup

Maestro / Maestro UK / Laser Setup		
	International	☑

Select International if the merchant is to support Maestro International. Neither Laser nor UKDM are valid for any future boarded merchants.

2.1.4.8 RESTAPI service

RESTAPI service	
	Nothing to configure here.

Select the service only if RESTful API is required for the merchant. No further configuration is needed.

2.1.4.9 Recurring

Recurring Payments / Periodic Billing		
	allowRecurringType	☐
	dailyFailureThreshold	3
	monthlyFailureThreshold	10
	rcpSharedSecret	[ ] Generate Password
	rcpTransactionNotificationURL	
	weeklyFailureThreshold	5

The fields: 'dailyFailureThreshold', 'monthlyFailureThreshold', 'weeklyFailureThreshold' relate to the number of times when IPG will try to perform a transaction in case the initial transaction has failed. The defaulted number of tries is shown below, however these are amendable.

The 'allowRecurringType' option is for a situation where the merchant triggers recurring transactions himself instead of using the IPG's scheduler. If the check box is ticked, a merchant is allowed to set the RecurringTypes: FIRST or REPEAT in the transaction request via Web Service API. Otherwise, the transaction will be declined. Setting of 'allowRecurringType' to 'true' does not impact the normal recurring processing like install, modify cancel at all. However, if the recurring transaction is started with RecurringType FIRST or REPEAT, it is a transaction which is marked as recurring but cannot be modified, canceled in the meaning of the normal recurring processing.

The fileds 'rcpSharedSecret' and 'rcpTransactionNotificationURL' can be set up for the recurring payments that get automatically triggered by the Gateway (IPG Scheduler). It can be configured to allow a merchant to receive Server-to-Server notifications when the recurring payments transactions get processed. Please note that 'rcpTransactionNotificationURL' can be also set by a merchant himself via VT/Customisation/Define the URLs for the integration with your online store.

2.1.4.10 Riskshield

Riskshield	Nothing to configure here.

Select the service only if Riskshiled is required for the merchant. No further configuration is needed.

2.1.4.10 Virtual Terminal

Virtual Terminal		
	allowCredits_vt	☑
	allowReturn_vt	☑

Only select if this is required for the merchant being built. This service offers the possibility to selectively enable or disable transaction types for a store per Interface.

2.1.5 Terminal

A terminal entry needs to be created per MID/TID so often multiple terminals are required for one merchant (e.g: American Express MIDs need to be added to the MID and therefore built separately to the MID created for Visa and Mastercard). A separate terminal would also need to be built if schemes are to point to a different endpoint.

- **Endpoint** – Select from the dropdown box where the transaction for that MID/TID/Scheme will be sent to
- **Terminal ID** - TID number
- **Merchant ID** – MID number
- **Brand Bitmap** – Select which schemes are to be included on the TID being created
- **Trx Origin Bitmap** – Select the type of transaction the merchant will be supporting for this Terminal being created
- **Payer Sec Level Bitmap** -
- **Trx Submission Bitmap** – Select the IPG components for this Terminal
- **Currencies** – Select which currencies the merchant can transact for this Terminal
- **Selected** – This field will show which currencies have been selected
- **Locked** – Only change the drop down to Yes if you wish the Merchant to be locked out. The "locked" setting in MCS is only relevant is a few special cases. In normal day-to-day operations, there is no need to set this to "Y".
- **Active** – Only change the drop down to No if you do not wish the Merchant to be active. If the "active" parameter for a specific Terminal ID is set to "N" , transactions would be declined if no alternative active Terminal ID is available for the Store. In normal day-to-day operations, there is no need to set this to "N".

At the end of each terminal configuration, click on Add/Update for the detail to save. You will then see the details shown in a line under the Store ID and the fields are then ready to complete again for another terminal if necessary.

To the left of the table next to each terminal built are a red cross and a pencil. You can delete the terminal by clicking on the red cross or edit the build by clicking on the pencil. Always remember to Add/Update to save any changes.

Once all the terminals are saved and shown in the table under the Store ID, click on 'Next' to move on.

2.1.6   Purchase Limits

For each currency chosen the default maximum order amount is 9999.0. However, these are amendable. Choose each currency maximum you wish to amend individually from the Currency dropdown box, add the new Maximum Order Amount in the box below then select Add/Update.

Master | Address | Contact | Service | Terminal | Purchase Limits | Fraud | Connect Logos

Purchase Limits

Store Id: 812509950006

		Minimum required currencies: [784]			
Remove	Edit	Currency ISO Code	Currency ISO Alpha Code	Max Order Amount	TxnValueExemption ⓘ
✖	✎	978	EUR	9999	
✖	✎	784	AED	9999	

Currency   [AED ▾]
● Max Order Amount   [0]
TxnValueExemption   [   ]

[Add / Update] [Reset]

[Previous] [Next]

[Save All]

Repeat this process for each currency you wish to amend then click on Next once all amendments are completed.

2.1.7 Fraud Settings

The defaulted settings are shown above to enable the Merchant to use these facilities, however these can be amended by using either the dropdown boxes or amending the number of seconds for Dup Lockout time and/or Auto Lockout Time.

Master | Address | Contact | Service | Terminal | Purchase Limits | Fraud | Connect Logos

Fraudsettings

Store Id: 812509950006

Check Card Number	Yes
Check Blocked IP	Yes
Check Blocked Class C	Yes
Check Blocked Name	Yes
Check Blocked Card	Yes
● Dup Lockout Time (Seconds)	60
● Auto Lockout Time (Seconds)	30
BIN Block Profile	99
Allow merchant to change country profile in VT	☐
Credit BIN Block Countries Whitelist	Yes
Credit BIN Block Countries	ABW AFG AGO AIA ALA
Credit BIN Block Countries Selected	
Debit BIN Block Countries Whitelist	Yes
Debit BIN Block Countries Whitelist	ABW AFG AGO AIA ALA
Debit BIN Block Countries Selected	

Previous Next

Save All

Select 'Allow merchant to change country profile in VT' check box if merchant should not be allowed to change the Country Profile via the Virtual Terminal' Administration section.

- **Auto Lockout Time (Seconds**) - You can choose how long any automatically blocked transaction will continue to be blocked. No orders from that blocked name (or card, Domain, IP, or Class C address) will be approved until the lock out time has expired.
- **Dup Lockout Time (Seconds)** - You can choose how long a duplicate transaction will continue to be blocked. No duplicate orders will be approved until the lock out time has expired.Auto Lockout Time (Seconds)
- **Credit BIN Block Countries Whitelist** - you can configure to "Yes" and select only the issuer countries to be allowed for transactions on this Store; you can configure to "No" and select the issuer countries to be blocked for the store (restriction applied to card type=CREDIT)
- **Debit BIN Block Countries Whitelist** - you can configure to "Yes" and select only the issuer countries to be allowed for transactions on this Store; you can configure to "No" and select the issuer countries to be blocked for the store (restriction applied to card type=DEBIT)

2.1.8 Connect Logos

If the merchant wishes to add their own company logos to the hosted payment page they need to email the logos so they are virus checked, then the logos can be uploaded.

Master | Address | Contact | Service | Terminal | Purchase Limits | Fraud | Connect Logos

Connect Logos

Store Id: 812509950006
for checkout option 'classic'

Image Top Left   [Choose File] No file chosen
[Upload] [Delete]

Image Top Right   [Choose File] No file chosen
[Upload] [Delete]

Image Bottom   [Choose File] No file chosen
[Upload] [Delete]

for checkout option 'combinedpage'

Image Top   [Choose File] No file chosen
[Upload] [Delete]

Image Bottom   [Choose File] No file chosen
[Upload] [Delete]

[Previous]

[Save All]

There are no mandatory fields in this tab so if no logos are provided this screen can be bypassed.

The Connect solution's checkout option 'combinedpage'

The logos uploaded to the 'combinedpage' allows merchants to use the Virtual Terminal and to customize the hosted page with their own logo and further graphical element at the top and bottom of the page, where the reseller branded logo is shown.

Once logos have been uploaded (if required) select Save All to save the merchant details you have entered which will prompt relevant certificates to be generated.

2.1.9 Merchant build completed

Once completed and 'Save All' has been selected, you will see the following screen informing you the Merchant Data has been saved successfully.

There is an option to view the merchant's details by selecting *Show Details* should you wish to check what has been boarded, or to *Create Hierarchy Entries*.

2.2 Search Merchant

If you need to view an existing merchant on the IPG, select 'Search Merchant' from the menu on the right under Merchant Care and you will be presented with the options by which you can search.

Once you have clicked on 'Search' the merchants that match your search information will be shown in a table.

Merchant Search Result

			Store Id	Legal Name	Reseller	Acquirer	MCC	Timezone	Default Ccy Code	Status	Open Date	Close Date	DBA	User Id	
🔍	Σ	⊖ 🏭 👤	812509950006	CBD Demo Store	CBD	Dummy-3DS2	1234	Asia/Dubai	784	OPEN	May 12, 2022		CBD Demo	812509950006	

To the left of the high-level merchant information there are 5 symbols which will lead you to specific information for that Store.

2.2.1   Merchant Details

When the magnifying glass is selected you will see the full details of the merchant. You will also be offered the options of deleting or editing the merchant details or using the merchant details as a template for a new build.

Merchant Details

Delete   Edit   Use As Template

Merchant Masterdata

		Store Id	Legal Name	Reseller	Acquirer	MCC	Timezone	Default Ccy Code	Status	Open Date	Close Date	DBA	User Id
		812509950006	CBD Demo Store	CBD	Dummy-3DS2	1234	Asia/Dubai	784	OPEN	May 12, 2022		CBD Demo	812509950006

Address

Address Type	Address 1	Address 2	City	State	ZIP	Country Code
MainAddress	Street 1		Dubai		12345	ARE

Contact

Contact Type	Email	Name	Phone	Fax
Principal	adriana.vas@fiserv.com	Adriana Vas	12354657	

Services

Service Type	Configuration	
3D Secure (MCSC / VbV)	TRAGhostCall	false
	acquirerName	
	allowAuthenticationRetry	false
	allowECI1andECI6	true
	allowECI7onIVRPAResUifInternational	false
	allowMPIViaAPI	true
	allowMPIViaRESTAPI	true
	allowSoftDeclineRetry_Connect	false
	allowSplitAuthentication	true
	allowed3dsServerVersionMax	
	amex3DSRequestorId	

2.2.2   Summary Information

Selecting the "Sum" symbol will take you to the Summary information for the Store's login and password details.

Summary Information

Store / Admin

Store Id	812509950006
Login	812509950006
Password	*Password changed by user*
Sharedsecret	sharedsecret
Admin Login	T41583441844
Admin Password	Not possible to display

API

Login	WS812509950006._.1
Password	*Not possible to display*
Key Name	WS812509950006._.1.key
Key Password	*Not possible to display*
JKS Name	WS812509950006._.1.ks
JKS Password	*Not possible to display*

Note: The passwords are only visible during the session where they have been created and only for the current/last created/edited API User.

- Instead of the passwords (displayed as plain text), you will see a label 'Not possible to display' on the 'Summary Information' page as well as on the 'API Users Overview' page.

2.2.3   View Blocked BIN Ranges

Selecting the 'Stop' symbol will allow you to view and modify the blocked BIN ranges.

Merchant Search Result

			Store Id	Legal Name	Reseller	Acquirer	MCC	Timezone	Default Ccy Code	Status	Open Date	Close Date	DBA
🔍 Σ ⊝ ⛭ 👤			812509950006	CBD Demo Store	CBD	Dummy-3DS2	1234	Asia/Dubai	784	OPEN	May 12, 2022		CBD Demo

View and modify blocked BIN ranges

- from [　　　　　　　　　　　　　　]
- to [　　　　　　　　　　　　　　]

[Add / Update] [Reset]

2.2.4   Hierarchy Details

Merchant Search Result

					Store Id	Legal Name	Reseller	Acquirer	MCC	Timezone	Default Ccy Code	Status	Open Date	Close Date	DBA
🔍	Σ	⊘	▦	👤	812509950006	CBD Demo Store	CBD	Dummy-3DS2	1234	Asia/Dubai	784	OPEN	May 12, 2022		CBD Demo

Selecting the hierarchy symbol allows you to see that Store's hierarchy details. Selecting '*Save*' from this page will save the settings. You are also able to *Assign store to other existing merchant in hierarchy* from here.

Hierarchy Details

Store

Store Id	812509950006
Node Id	41583441842
User Id	[812509950006]
Email address for password reset	adriana.vas@fiserv.com
Password	*Password changed by user* [Reset store password]

[Edit Store API Users]

Merchant

Merchant Name	[CBD Demo Store]
Node Id	41583441844
Password	*Not possible to display* [Generate Password]

[Edit Merchant API Users]

[Save]   [Assign store to other existing merchant in hierarchy]

2.2.5 API Users Overview

Selecting the little person icon will show the API Users Overview for the Store. It will also provide you with an option to create a new API User.

Merchant Search Result

					Store Id	Legal Name	Reseller	Acquirer	MCC	Timezone	Default Ccy Code	Status	Open Date	Close Date	DBA
🔍	Σ	⊖	⊞	👤	812509950006	CBD Demo Store	CBD	Dummy-3DS2	1234	Asia/Dubai	784	OPEN	May 12, 2022		CBD Demo

If you opt to create a new API user the following screen will show with the Store ID already selected and greyed, the option to amend the User ID and to select Generate Password for both the Store and the Certificate.

Note: During your login session in MCS <u>work only with one/single store/API User</u> when creating/generating a new API User/Client Certificate.
When contacting your API merchants <u>put emphasis on the need to confidently store the API Client Certificate password</u> on their side since there will be no possibility for you to retrieve it via MCS in the future and provide it again to your merchants.

Note: The passwords are only visible during the session where they have been created and only for the current/last created/edited API User.

- Instead of the passwords (displayed as plain text), you will see a label 'Not possible to display' on the 'API Users Overview' page as well as on the 'Summary Information' page.

API Users Overview for Store 812509950006

			Store Id	User Id	Comment	Create Date
🖊	✖	🔒	812509950006	WS812509950006._.1		5/13/2022

Create new API User

Store API User Edit

- Store Id   812509950006
- User Id   WS812509950006._.1
- Password   *Not possible to display*   Reset Password
- Certificate password   *Not possible to display*
- Comment   [   ]

Cancel   Save

2.2.6 Resending Certificates

When working in the same login session as the latest API Client Certificate was generated you will be able to resend the certificate.

When not working in the original login session as the latest API certificate was generated you will see:

Instead of resending the API Client Certificate for a selected API User, you will have to generate it by using the new button 'Generate Certificate' on the 'API Users Overview' page.

3 Transactions

Multi Alliance real time transactions can be seen when selecting Transactions in Merchant Care Service.

These can be filtered by date, Store ID, Order ID, User ID, Total Amount range, Currency code (numerical), TID, Approval, Transaction ID, Type of Transaction and/or State of transaction by completing the fields shown in the initial screen.

Once the relevant fields have been entered select Search and the list of transactions matching your search criteria are shown.

There is an option to the left to 'Show'. If selected a further line of information is shown. This line can be hidden again by selecting 'Hide'.

There is also the option to select the Store ID from the table of transactions. This will take you to the Merchant Details of the Store so the set-up details can be reviewed and amended if necessary.

4 Logging

Logging is information used by the 2nd level support as it shows more technical details in regard to the real live transactions which have taken place in the previous 4 hours.

The logging entries can be filtered by Store ID (which is a mandatory field) and OrderID as shown on the example below:

Search Logging Entries

Search Logging Entries

▼Hide Form

- Time Range `19.05.2022 08:16:57`   `19.05.2022 12:16:57`
- Store Id
- Order Id

Search

Once the filters have been entered and Search has been selected an app log is shown:

Search Logging Entries

Search Logging Entries

▶ Show Form

```
[2022-05-18 10:50:00.607[CEST/+0200] null [null] null - (uuid=YoSzOJ19TYkUgXexnDxS
TRANSACTION_START=2022-05-18T10:50:00.607+02:00;SUBMISSION_COMPONENT=VT;SERVLET_ST
, 2022-05-18 10:50:00.607[CEST/+0200] null [null] null - (uuid=YoSzOJ19TYkUgXexnDx
POST /vt/view/pos/confirmOrder.faces - 302
, 2022-05-18 10:50:00.679[CEST/+0200] INFO [IPG.Transaction.CORE.in] de.firstdata.

amount: 126.00 AED, VAT: 21.00, shipping: 5.00
billingInformation:
billingAddress1: "Street 21"
billingCity: "Frankfurt"
billingCountry: "DEU"
billingName: '
billingZip: "12345"
brandType: MASTERCARD
capture
clientLocale: en_GB
consumerCheckInformation: ConsumerCheckInformation [result=null, score=0]
contactInformation:
contactBillingEmail: "adriana.vas@fiserv.com"
creditCard: 554433...0011 2022-12 - CCV(3) MASTERCARD TWN (MASTERCARD) SUNNY BANK
dccApplied: false
dynamicPricing: false
installment
ipgReceiptTimestamp: Wed May 18 10:50:00 CEST 2022
notes
orderID: "V1652863800627995059"
```