Configure system settings

Settings allows you to configure system settings for your ActiveServer instance. **Settings** has 3 tabs:

- System
- Security
- ActiveMerchant Migration

System

The **System** tab has 3 sections:

Server URLs

- **External URL** - externally accessible URL, used for authentication callbacks and product activation. The URL can be populated with the form of `https://"your ActiveServer domain name":"server port number"`, e.g. `https://paymentgateway.com:8443`. The `server port number` in the URL pattern is the `as.server.http.port` or `as.server.https.port` value (depending on the protocol being used) set in the **ActiveServer** configuration file.

> **Warning**
>
> Updating the **External URL** will also initiate an update of the 3DS Server URL in the Directory Server settings for each card scheme. If the **3DS Server URL** value is empty for any card scheme, it will be updated to use the new **External URL** value, with the HTTPS listening port value also being appended. If the **3DS Server URL** value is already set, no changes will be made.
>
> This is to assist with the setup process as these URLs are generally the same. If your architecture setup has a separate URL assigned for the **3DS Server URL**, this setting should be updated before performing a transaction.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

> **Tip**
>
> For a load-balanced setup, this URL may be different to the URL pattern described above and there may be a separate admin UI interface URL that has been configured. Please make sure that the load-balancer for the **External URL** forwards the requests to the server ports mentioned above.
>
> E.g. If the URL `https://paymentgateway.com` has been configured for server callbacks and `https://admin.paymentgateway.com` has been configured for admin UI interface requests, then `https://paymentgateway.com` should be used for the **External URL**.

- **API URL** - Optional URL used to receive authentication and administration API calls. The domain name of this URL will also be used to generate client certificates for the authentication of APIs (x.509). If it is not provided, by default **ActiveServer** will use the domain name in the External URL for client certificate generation. Note this URL does not have to be publicly accessible. The form of the URL is the same as the **External URL**, with the port number being the API port.
- **Admin URL** - Optional URL that is used for user email activation and reset password procedures. This value can only be entered if the Admin port in the **ActiveServer** configuration file is enabled. If the admin port is enabled and this value is empty, a localhost domain will be used with the admin port specified, however this will cause issues accessing the domain from a remote host. If the admin port is disabled, the domain name in the **External URL** will be used. Note this URL does not have to be publicly accessible.

> **Important**
>
> For the URLS above, URL validation is performed to ensure that the system functions will perform correctly. The validation checks to ensure no **paths** or **query strings** are included in the URL.
>
> E.g. `https://domainname<:port>` is allowed, whereas `https://domainname<:port>/path?queryString` would be rejected.

Logging

- **Log level** - verbosity of the console output and system logs. Possible values in least verbose to most verbose order: **ERROR** > **INFO** > **DEBUG**.
- **Enable message content logs** - when enabled, ActiveServer will log 3DS message contents.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

API configuration

The API configuration section allows system management of the API versions for the instance. Currently it displays the supported API versions, along with providing functionality to disable APIV1.

Disable APIv1

Support for APIV1 has now reached its sunset date, so functionality to disable it has been provided to update the system to only use APIV2. APIV2 has many improvements, including:

- Full PANs are no longer stored, potentially reducing PCI security audit requirements
- Encryption keys are no longer required per merchant, improving performance for transaction processing and database/HSM access
- Improved data structure for transaction storage

Migrating to APIV2 is a **one way** process to disable Authentication APIV1 and convert all transactions to APIV2 and cannot be reversed. **We strongly suggest upgrading your 3DS Requestor to only use APIV2 transactions and confirming full operations before migrating.**

Once you select the ***Disable API V1*** button the following process will be executed:

1. All Authentication APIV1 requests sent will now return the error code `1027 Unsupported API version`. Therefore, the 3DS Requestor will no longer be able to send APIV1 requests.
2. The data key used for encrypting transactions performed by a merchant will no longer be created when a new merchant is created. Authentication APIV2 does not use a per merchant key but rather uses envelope encryption using the master key and data key for encrypting transaction data.
3. A background migration process will be started to truncate the PANs stored from API v1 and change the data format to APIV2 (including removing no longer used tables from the database). The number of transactions to be migrated will be shown on the Admin UI. Once the **Number of API v1 transactions** counter reaches `0`, the migration process has completed.

Deleting the data keys

The existing per merchant data keys or keystore files **will not** be automatically deleted by ActiveServer. At any time once the migration process has finished, you may delete the keys in the HSM, local or S3 bucket manually as they are no longer required.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

For those using a HSM, you may delete any key aliases prefixed with `REQ_**`. You **must not** remove any data keys with a key alias prefixed with `AS_**` or `MASTER_**`.

For those using ActiveServer with SunJCE Local or S3 keystore type, you may delete any keystore files in the format `as_<UUID>.jks`. You **must not** remove the `as_sys_<UUID>.jks` or `as_master_key.jks` keystore files.

> **Info**
>
> The APIV1 disabling process does not apply to the KMS keystore type, as APIV1 was disabled by default.

Security

- **Session timeout (read only)** - interval a login session is valid for before expiring and requiring the user to enter their login credentials again. By default, the session timeout value is 900 sec (15 min) and is loaded from an internal setting. To change this setting, add the following line into the `application-prod.properties` file and restart the instance:

  ```
  as.settings.session-timeout={time in seconds}
  ```

  For example, to set the session timeout to 1800 seconds (30 minutes), add `as.settings.session-timeout=1800`.

  > **Important**
  >
  > The value must be a positive integer in the range of 300 ~ 3600 seconds (5 ~ 60 minutes).

- **Session failed attempts** - number of failed login attempts permitted before login is temporarily disabled for the time specified by the session lock time. After the time has elapsed, the session can be re-established by providing the correct credentials (unit: attempts)
- **Session lock time** - interval a user will be locked out for if they exceed the failed login attempts amount (unit: minutes)
- **Password expiry period** - number of days a password is valid for before requiring a new password to be created (unit: days)

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

- **Password history check** - number of unique passwords required to be used before a specific password can be used again (unit: unique passwords)
- **Force two factor login** - **enable** or **disable** two factor authentication for login for **all** users on the server. ActiveServer uses Google Authenticator to provide two factor authentication for users. If this setting is **enabled**, any user who does not have two factor authentication already set up for their account will be forced to set it up on their next login before being able to use any system functionality. Steps to set up the Google Authenticator are provided on screen.

API Security

- **Allow merchant override** - toggle this feature to enable or disable utilising the "merchantOverride" field in the Authentication API to override specific merchant profile fields. ***Disabled*** by default.
- **Skip Enrol API merchant validation** - toggle this feature to enable or disable the merchantId in the Enrol API being required, ***Disabled*** being required, ***Enabled*** being not required. ***Disabled*** by default.

Data encryption key

Shows the current system encryption key's (used to encrypt sensitive system information) creation date and allows the user to rotate the key used by selecting **Rotate key**. New system related data will be encrypted using the new data key.

Rotate master key

Shows the current master cryptographic key's (used to encrypt the Authentication Value for Auth API v2 transactions) creation date and key alias. Allows the user to rotate the key used by selecting **Rotate key**. However, key rotation has no effect on the data that the master key protects. It does not rotate the data keys that the master key generated or re-encrypt any data protected by the master key.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

HSM

This feature allows the user to update the HSM PIN if it has been changed:

- **Full file name and path of PKCS#11 library** - this value is read from the `application-prod.properties` and can only be changed by updating the `application-prod.properties` file and restarting the server.
- **Slot number of HSM** - this value is read from the `application-prod.properties` and can only be changed by updating the `application-prod.properties` file and restarting the server.
- **HSM PIN** - allows the new HSM PIN to be entered.

Selecting the **Test HSM connection** button will attempt to connect to the HSM using the inputted **HSM PIN**. If the test is successful, the system will show "HSM connection successful", otherwise "Invalid HSM Pin" will be shown.

Selecting the **Update** button will update the database with the **HSM PIN** value. **Restarting the server is required after updating**.

Warning

The system will update the HSM PIN regardless of the test result. This is to allow the PIN to be updated in the **ActiveServer** database before the HSM PIN is changed if required. Make sure the right PIN is entered before updating the system, as having the wrong HSM PIN will cause transactions to fail.

Tip

The HSM PIN management will only be shown if a HSM is in use.

Version 1.0.4

This feature was added in the version 1.0.4 release.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

ActiveMerchant migration

The **ActiveMerchant Migration** tab allows a **Business Admin** user to import merchants and acquirers from GPayments **ActiveMerchant** (3DS1 MPI) to assist with the transition from 3DS1 to 3DS2.

For information on how to use the migration feature, refer to the ActiveMerchant migration guide.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.