FEATURE GUIDE
DATA PRIVACY
Product version 5.0.12

Vista Entertainment Solutions
2023-05-11

for the ❤ of cinema

Copyright notice

Vista Entertainment Solutions Limited

PO Box 90551, Victoria Street West, Auckland 1124, New Zealand

P: +64 9 984 4570 www.vista.co

Contents

About this document

The *Data Privacy Feature Guide* describes the areas in Vista software that allow you to anonymise or delete stored personal data so that you can comply with data privacy laws.

This guide assumes you're familiar with Vista databases and scheduled tasks.

About Data Privacy

Protecting people's personal data is an increasing global concern. Companies that collect, store, and use personal information are required by data privacy laws to protect an individual's privacy. Vista provides data privacy tools and features to help you comply with these laws.

The PCI DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation) are examples of data protection efforts.

The types of personal data stored by Vista software processes are **patron data**, **business contact data** and **Vista user data**.

Locating personal data using the Privacy Control cabinet

The **Privacy Control** cabinet displays which fields in your Vista product databases capture personal data and how this data is being anonymised. This data could be about patrons (both Loyalty and non-Loyalty members), business contacts (for corporate sales), or Vista users (employees at your company that use Vista software).

The cabinet is intended for IT staff who need to manually locate and anonymise personal data, or staff who have to report its location.

You'll find the **Privacy Control** cabinet in Vista desktop applications that use cabinets.

1. Open the **Privacy Control** cabinet.

2. Sort the data as you require.

   For example: If you need to find information that isn't being anonymised, set the **Anonymisation Method** filter to **Not Implemented**.

3. Record the location of data that needs anonymising but isn't being anonymised currently.

   Warning! *If you've added any of your own tables and columns to your Vista databases, these won't be detected or shown in the Privacy Control cabinet. Any personal-data values in them* ***will not*** *be anonymised. Add your own anonymised values (to replace personal data in any tables and columns you've added) to the* ***tblPrivacyControl_Fields*** *table in the relevant database. Contact your Vista Services representative if you need help doing this.*

   Tip! *Click* ***Export to Excel*** *to quickly create a file containing the records visible in the cabinet. This is handy if you need to report where personal data is located in your databases.*

4. If a column has the data subject **Patron Data** and no anonymisation method, ensure you've followed all the steps to anonymise personal data (page 8).

   All patron data is anonymised by the **Database Purge Monitor** and the **Purge Historical Data** task.

5. Inside the relevant database, manually anonymise any records or update replacement values as required.

   Contact your Vista Services representative if you or your IT staff require assistance.

SEE ALSO

Privacy Control cabinet column descriptions............................27

Vista system monitors and data purging

Database Purge Monitor

The data stored in your Vista databases is categorised by data type. Regularly purging data that you don't need any more helps you manage the size of your databases, and anonymising personal data ensures you comply with data privacy laws. The **Database Purge Monitor** in **Back Office** helps you do this.

Use the monitor to see how often the **Purge Historical Data** task anonymises personal data and purges other types of data from products that use cabinets.

Note: *From release 5.0.2, the* ***Purge Historical Data*** *task replaces (and combines the actions of) the following tasks in* ***Vista Cinema****:*

- *Cinema Purge Engine*
- *Purge Bookings*
- *Purge Table Bookings*
- *Purge Data*
- *Purge User Log*

These tasks are no longer supported. We recommend moving to ***Purge Historical Data*** *as soon as possible and removing these old tasks.*

What can I do in each of the monitor's tabs?

In the **Settings** tab, you can see and update how many days each data type needs to be stored before it can be purged. You can also set whether it needs to be manually purged, is scheduled to be purged by the **Purge Historical Data** task, or a combination of the two. A blank entry in the **Days to Retain** column indicates that data won't (and shouldn't) be purged.

> **Important!** Setting the **Run Method** to **Scheduled** won't actually schedule the data to be purged. You'll need to set up the **Purge Historical Data** task to do that. The **Run Method** column just shows you and other users **how** the data must be purged.

You can view information about previous purges in the **Purge History** tab. This includes when and how a data type was purged (manually or by a scheduled task). This tab also shows you if the purge task failed and why.

Note: *The purge task could fail if an uncollected booking hasn't been released, or the transaction-table data wasn't summarised because* ***Vista Transaction Summariser*** *didn't run.*

SEE ALSO

Database Purge Monitor data types 27
Purge Historical Data.. 10

Automating database purging

Automating database purging (or anonymising Privacy Data) is done in **Task Scheduler**. The **Database Purge Monitor** reflects which data types are purged, and the manner in which they are purged - whether that be by scheduled tasks, manually, or a mix of both.

1. In **Task Scheduler**, set up the relevant scheduled tasks. See purging long-term data for more information.

   Tip*! We recommend you purge all data types, and use scheduled tasks wherever possible.*

2. In the **Database Purge Monitor**, set the **Run Method** for the relevant data types to **Manual and Scheduled**.

Note: While you could select **Scheduled** only, the **Manual and Scheduled** option gives you the flexibility to run purge data manually in between scheduled purges. That's why we recommend this option.

3. For **Days to Retain**, enter how long the relevant data needs to be stored before it's purged or anonymised.

   For example: if you enter `6`**,** you'll purge or anonymise any records that have been stored for seven days or longer.

   Note: *Enter `0` to purge or anonymise all records each time you perform a purge.*

Manually purging your Vista databases

Important*! Before you manually purge your database, make sure you don't have any urgent tasks to complete in* ***Back Office****. The* ***Database Purge Monitor*** *can't close while it's performing a manual purge. If you're purging data for the first time, or after a long time, this process could take a long time.*

1. Check the **Run Method** for the data types you want to purge is set to **Manual and Scheduled** or **Manual**.

   Note: The monitor won't manually purge any data types set to **Scheduled** only.

   Tip*! If it's set to* ***Manual****, check why a scheduled task wasn't set up for the data type. Set up a scheduled task if possible.*

2. Check the **Run Method** for any data types you don't want to purge is blank.

3. Select **Home** and **Purge Now**.

   The monitor purges the relevant data types from your Vista database.

Anonymising personal data

You can set up **Vista Cinema** so personal data older than a particular date is automatically anonymised. This will help ensure your compliance with laws around the storing and retention of personal data, such as those introduced in Europe by the General Data Protection Regulation (GDPR). If you want to perform a partial anonymisation of data, please contact Vista.

Anonymisation is done by the Purge Historical Data task.

Important! *Data anonymisation is enabled by default. If you don't want data anonymised, you'll need to turn it off. You can do this by leaving the run method for* ***Privacy Data*** *blank.*

Before you begin:

Ensure the Purge Historical Data task has been set up.

1. In **Back Office**, open the **Database Purge Monitor**.

2. Select a **Run Method** (see "**Database Purge Monitor run methods**" page 31) for **Privacy Data**.

3. For **Days to Retain**, enter how long the relevant data needs to stored before it's anonymised.

   For example: if you enter `6`**,** you'll anonymise any records that have been stored for seven days or longer.

   Note: *Enter `0` to anonymise all records each time you perform a purge.*

4. Click **Home > Save**.

Journeys and data purging

Customer journeys are created to link tabs, bookings, and transactions that relate to a single cinema visit. A single journey can include multiple tabs, bookings and transactions as child items. The journey itself will only be purged when all tabs and bookings in that journey are ready to be purged. This is to prevent different parts of a journey being purged at different times. Transactions don't prevent a journey from being purged and will remain in the database until they have reached their own purge date.

For more information, see the *Paperless Ticketing Feature Guide*.

Sales Server Monitor

The **Sale Server Monitor** shows you which in-progress orders have failed. Use the monitor to manually purge personal patron data for failed orders. Set up the **VSS Transaction Cleanup** (page 11) scheduled task to automate the regular purging of failed orders.

Note: *If you open the monitor before VSS Transaction Cleanup has run, you might see patron data because it hasn't been purged yet.*

Scheduled tasks to purge or anonymise personal data

To make sure personal data is only stored as long as it needs to be (and purged regularly from your Vista databases), enable the scheduled tasks below using **Task Scheduler**. Schedule how often each task runs based on regulations about how long data should be kept for your site or organisation.

IN THIS PART

Purge Historical Data

The **Purge Historical Data** scheduled task replaces (and combines the actions of) these **Vista Cinema** scheduled tasks:

- Cinema Purge Engine
- Purge Bookings
- Purge Table Bookings
- Purge Data
- Purge User Log

Set up and enable this task for **Vista Cinema**, **Head Office**, **Vista Connect**, **Vouchers & Gift Cards** and **Loyalty** to purge data you don't need to store, including personal data.

Note: *The task calls on a stored procedure to check the databases for these products and purges data related to the relevant data types. For products that use cabinets, it checks* ***Database Purge Monitor*** *for whether the data has exceeded its required storage time before purging it.*

Cinema Scheduled Tasks

IN THIS PART

Release Bookings

The **Release Bookings** scheduled tasks release bookings so the information related to them can be purged. Releasing bookings also makes seats or tables that were reserved for the booking available again, so another patron can reserve them.

Task name	Data type	What this task does
Release Bookings	Patron data	Releases bookings that weren't paid for by the session start time.
Release Table Bookings	Patron data	Releases table bookings that weren't marked as seated by the booking start time.
Release Unpaid Advance Bookings	Patron data	Releases bookings that weren't paid for by the set number of days before the session start time.

VSS Transaction Cleanup

This task purges transactions from failed in-progress orders.

Data subject type

- Patron Data

Configuring the task to remove expired bookings made through Facebook

The Sales Server Transaction Cleanup job must be configured to remove expired bookings made through Facebook.

1. Open **Task Scheduler**.

   VISTA > Task Scheduler

2. In the **Tasks** panel, select the menu item **Cinema > Scheduled Tasks > Processes**.

3. Right-click on the task **VSS Transaction Cleanup**, and choose **Edit Task Details**.

4. In the **Settings** tab, add the parameters `/FACEBOOKEXPIREFROMSESSION` and `/FACEBOOKEXPIREFROMCREATION` (with appropriate values) to the **Parameters** field.

   Choose the same values for the parameters as the corresponding settings (`TimeToExpireFromSession` and `TimeToExpireFromCreation`) in your web server's `Userweb.config` file.

   For example:

   ```
   /MINUTELAGCANCEL 10 /FACEBOOKEXPIREFROMSESSION 120 /FACEBOOKEXPIREFROMCREATION 1440
   ```

5. Click **OK**.

Head Office Upload Export File Cleanup

This task deletes old XML and zipped **Head Office** export files in the `uploads` folder.

Data subject type

- Patron data

Head Office Scheduled Tasks

IN THIS PART

Head Office Upload Cleanup

This task purges all summarised transaction and real-time admit data.

Data subject type

- Patron data
- Vista user data

HO Refresh Token Cleanup

This task purges temporary tokens (API keys) and application-initialisation data (related to a security mechanism) from the **Head Office** database.

Data subject type

- Vista user data

Purge Group Sales User Log

This task purges the **Group Sales** user log. The user log contains the interaction history between a business contact and a Vista user.

Data subject type

- Business contact data
- Vista user data

Connect Scheduled Tasks

IN THIS PART

Transient Object Cleanup Task

This task purges temporary historical tokens (API keys) and temporary order-completion data older than the scheduled number of minutes from the **Vista Connect** database.

Data subject type

- Patron data

Delete Orders in History Tables

This task purges order-completion data older than the scheduled number of minutes from the **Vista Connect** database.

Data subject type

- Patron data

Clean up Expired in Progress Orders

Purges abandoned in-progress order-completion data older than the scheduled number of minutes from the **Vista Connect** database.

Data subject type

- Patron data

Vouchers and Gift Cards Scheduled Tasks

IN THIS PART

VM Refresh Token Cleanup

Purges temporary historical tokens (API keys) and temporary application-initialisation data (security mechanism) from the **Vouchers & Gift Cards** database.

Data subject type

- Vista user data

Loyalty Scheduled Tasks

IN THIS PART

Database Cleanup

Purges processed message data and a log of when users enter and exit groups from the **Loyalty** database.

Data subject type

- Patron data
- Vista user data

Sending databases to Vista

To ensure compliance with data privacy laws, and to meet your obligations under them, you must send any requested databases to Vista using the DB Tool (page 16). We will *only* request and accept databases sent to us through the tool.

The DB Tool

We created the **DB Tool** to help you comply with data privacy regulations.

The tool creates a temporary copy of a database, from a backup, and anonymises or removes any personal data from the copy before sending it to us. It then deletes the temporary files.

Warning! If you've added any custom tables and/or columns to the database, the DB Tool cannot detect these or anonymise the data in them. See Custom tables and columns (page *16*) for instructions in this situation.

Note: *The DB Tool uses HTTP and HTTPS to upload a `.bak` file in chunked blocks to* ***Microsoft Azure****. It requires an internet connection to do this.*
Note: *The DB Tool will remove all locks within your database. If you're experiencing issues related to locked data and need to send us a copy of your database, ask your Vista Services consultant for instructions on how to do this.*

Custom tables and columns

If you've added custom tables to the Vista database you're sending us, the **DB Tool** cannot detect them to anonymise or remove personal data. If the data in your custom tables is confidential and needs to be anonymised (page 16) or removed (page 17), add the table and column names to the **tblPrivacyControl** table in the same database. This makes sure the tool can anonymise or remove data in your custom tables.

Important! *Let your Vista Services representative know if your database has custom tables.*

Allowing the DB Tool to anonymise data in custom tables

1. In **SQL Server Management Studio**, find the reference table **tblPrivacyControl_Fields**.
2. Enter the names of any custom tables you've created in the column **PrivacyControl_strTableName**.
3. Enter the names of any columns within a custom table in the column **PrivacyControl_strField**.

   Note: Add each column name into its own row.

4. Enter an anonymous value (that will replace and anonymise the data within a column in a custom table) in the column **PrivacyControl_strValue**.

   Example: `@blank`

5. Enter the data type `X` in the column **PrivacyControl_strDataType**.

6. Save your changes.

Allowing the DB Tool to remove confidential data from custom tables

1. In **SQL Server Management Studio**, find the reference table **tblPrivacyControl_Purge**.

2. Enter the names of any custom tables you've created in the column **PrivacyControl_strTableName**.

3. Save your changes.

Note: *The custom table will not be deleted from the copy of your database. The data within it will be removed but the table structure will stay.*

DB Tool fields

Option	Description
Use backup	Select this option when you have a backup of the database.
Use database	Select this option when you don't have a backup of the database. The tool will create a backup from the database you select.
.bak file to cleanse	Browse to the backup file you want the tool to work on.
Temporary database name	Generated automatically by the tool. Click **Regen** to generate a new randomised name.
Database name to perform actions on	If you don't have a backup, select the database you want to send to Vista.
Output .bak file	Location and name of the .bak file the tool will create and send to Vista.
Temporary .bak file	Location and name of the temporary .bak file the tool will create. The tool will delete this when it finishes running.
Temporary db location	Location of the temporary database the tool will create. **Note**: After the tool has finished, it will delete the temporary database.
Keep Transactions From	Select the starting date of the transactions you want to include in the database you send to Vista. Select **All** to include all transactions, regardless of the date. If you don't select a date, the tool will exclude transaction information. **Warning!** If you have a large database and select **All**, the DB Tool may take hours to process the data.
Keep Cinemas	To include specific cinemas in the database you send to Vista, enter their **Cinema** codes. To include all cinemas, select **All**. If you don't select anything, the tool will exclude information from all cinemas in the database.

Keep Members	To include specific **Loyalty** members in the database you send to Vista, enter the primary keys for these members, found in the **person_id** column of the Loyalty database. **For example:** AQ1GM4BYPN. Use a comma to separate the ID strings (PersonID1, PersonID2, PersonID3). To include all members, select **All**. If you don't select anything, the tool will exclude member-related information. **Note:** The tool will anonymise all personal data.
Keep Random Members	Select this to include ten random members from the **Loyalty** database in the database you're sending Vista. The tool will anonymise any personal data. You can use either the **Keep Members** option or this option; you can't use both. Any information you enter for **Keep Members** will override this option.
Anonymise	Determines whether the tool will anonymise the database information. **Leave the checkbox selected.** **Important!** In the rare event we request a non-anonymised database, a Vista services consultant will explain this process. Never send a non-anonymised database if we haven't asked for one or explained how to do it.
Shrink without TRUNCATEONLY	Select this if your database is large and you want the tool to shrink it before sending it to Vista.
SQL Server Connection to use	Enter the **Server Name** and login details of the database server you want to connect to. Alternatively, select **Windows Auth**.

Using the DB Tool

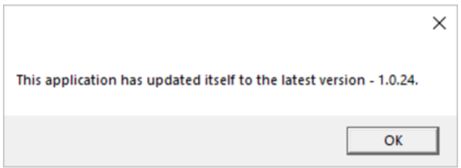
***Note:** When your Vista services consultant requests a database, they will provide clear, case-by-case instructions on how to complete the **Options** section (see "DB Tool fields" page 17) of the tool.*

Before you begin:

- Make sure you've downloaded the tool from the **Software Downloads** page on the Vista Services site. You only need to download it once; the tool updates itself automatically.
- Make sure you have a key from your Vista services consultant.
- Use a server with internet access so the **DB Tool** can successfully send your database to Vista. If your site doesn't have internet access, use a **Head Office** server.
- Read about the DB Tool fields (page 17).

1. Open the tool using the shortcut created on your desktop.

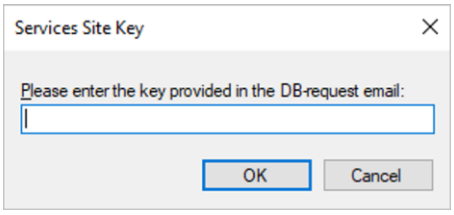
   You might see an update message if the tool has updated itself since you last opened it.

2. Enter the key your Vista services consultant gave you in the dialog that appears.

   The **DBTool** form opens.

Note: Each key can only be used once for one database. Each requested database will need a separate key.



Example: `12A34567-8B91-2C3D-4567-891E2F3GH456`

3. Select **Use backup** or **Use database**, depending on the database source.

4. If you're using a backup, browse to the location of the **.bak file to cleanse**.

   Note: If you chose the **Use database** option, this field isn't applicable and will be greyed out.

5. To log into the database server, enter the **Server Name** and login details, or select **Windows Auth**.

   Note: This doesn't have to be a production instance of SQL (for example, it can be a developer, test, or UAT environment, or a temporary SQL Express instance).

6. If you chose the **Use database** option, select the **Database name to perform actions on**.

   Warning! *If you're using a backup, the **Temporary database name** will be populated automatically. **Don't change this name!** If you change the name to an existing database, the tool will delete that database.*

7. Browse to the location where you want the **Output .bak file** to be generated, and type a name for the generated file with the `.bak` file extension.

   Example: `D:\Data\test.bak`

   Warning! *Make sure there isn't a `.bak` file in the same location with the same name already. If there is, the tool will send this file without anonymising or deleting private data in it.*

   If you're using a backup, the **Output .bak file** location and name is populated automatically based on the location and name of the **.bak file to cleanse** you selected earlier.

   The **Temporary .bak file** and **Temporary db location** are populated automatically.

8. Using the relevant **Options**, select the database information you want to anonymise and send to Vista.

9. Run the tool.

   If the tool runs successfully, you can close it. Your Vista services consultant is notified when your database arrives.

   If the tool fails, try to troubleshoot (page 19) the failure.

Troubleshooting the DB Tool

If the **DB Tool** fails, troubleshoot the error using the details in the "Failed**"** message.

Note: *If you cannot troubleshoot the error, contact your Vista services representative and send a copy of all the text from the **Summary** section in the DB Tool.*

Not enough disk space

If the DB Tool fails because there is not enough disk space, browse to a new output location in a drive with more space.

Example message: "Failed. Not enough disk space at `D:\.` (7.97 GB required)"

1. Note from the message the amount of space required.

2. Browse to a new **Output. bak file** location with the required amount of space.

   Note: This disk space can be on another server, external disk, or removable drive.

SQL compatibility issue

If the **DB Tool** fails because of a SQL compatibility issue, make sure the selected backup file and SQL server are compatible.

1. Browse to the Microsoft article outlining database compatibility levels.

2. Make sure the selected backup is created in a version of SQL Server compatible with the SQL Server used in the connection.

Firewall preventing tool from sending the database

If your firewall is preventing the **DB Tool** from sending the database, set it to allow connection with the Vista Azure URLs.

1. Allow the following URLs for port 443:

   `https://support.vista.co/API/V2`

   `https://vistastormaster.azurewebsites.net`

   `https://vistastornode1.azurewebsites.net`

   `https://vistastornode2.azurewebsites.net`

   `https://vistastornode3.azurewebsites.net`

   `https://vistastornode4.chinacloudsites.cn`

2. If your firewall allows wild cards, allow the URL `https://vistastornodeXX.azurewebsites.net`.

No internet connection

Sites might not have internet access (so the tool can't be downloaded or run), but your head office often will.

Move the backup file (of the database you've been asked to send to Vista) to a server at your head office with internet access. Run the **DB Tool** from there.

Transaction log full

If the **DB Tool** doesn't run successfully because the transaction log of the relevant database is full, clear the log and run the tool again.

Can't check backup file compatibility or restore database

If the **DB Tool** can't confirm your backup file is compatible with SQL Server, or restore the database, it could be for one of the following reasons:

- The backup file isn't accessible (due to permissions or the file location).
- The backup file is incomplete or corrupted.
- The wrong backup file was selected.
- The SQL connection is incorrect.
- There is a SQL compatibility issue (page 20).
- Your user account doesn't have the right permissions.

Use the error details to troubleshoot, and try running the tool again. If it still doesn't work, contact your Vista Services representative and send them a copy of all the text from the **Summary** section in the DB Tool.

Task cancelled

A "task cancelled" error appears if you cancel the **DB Tool** or a background task fails.

- If you've cancelled the tool, ignore this error.
- If you haven't cancelled the tool but see this error, contact your Vista services representative and send them a copy of all the text from the **Summary** section in the DB Tool.

Person records in Loyalty

IN THIS PART

Viewing anonymisation details of Loyalty data

To view personal data fields and their anonymisation details in **Loyalty**, generate a SQL view.

1. Open **Microsoft SQL Server Management Studio**.

2. Execute this query against your **Loyalty** database:

   ```
   SELECT * FROM vwPrivacyControl
   ```

   For every field in your Loyalty database that holds personal data, the results display anonymisation details equivalent to those in the Privacy Control cabinet (page 6).

Anonymising previously-deleted Person records

In releases of **Loyalty** earlier than 5.0.2, the data for deleted **Member**, **Administrator**, **User**, and **Customer Service** Person records wasn't completely anonymised in the Loyalty database. If you need to completely anonymise Person records deleted in the past to comply with local data privacy laws, follow these steps:

1. In the **Loyalty website**, enable the system setting ClearPersonOnDeletion.

2. In the **Privacy Update Pack** installation package, find the AnonymisePreviouslyDeletedPersonDetails folder.

   For example:
   PrivacyUpdatePackage\Loyalty\<version>_Install_Customisation\General\AnonymisePreviouslyDeletedPersonDetails\

3. Open the SQL script sp_AnonymisePreviouslyDeletedPersonDetails.sql in **SQL Server Management Studio**.

4. Run the script against your Loyalty database.

5. Run the command EXEC anonymisePreviouslyDeletedPersonDetails to execute the stored procedure.

   The stored procedure updates the database fields for all previously-deleted Person records.

Confirmation of successful anonymisation

Successful completion of the anonymisation procedure (page 22) updates the relevant fields in your database. Nullable fields are set to **NULL**, and non-nullable fields are set to their default values.

Fields that are updated for non-member Person Types:

- The majority of fields in the **cognetic_core_person** table

Fields that are updated for **Loyalty** members:

- The majority of fields in the **cognetic_core_person** table
- Any card numbers in the **cognetic_core_userLog** table
- The new and old values in the **cognetic_core_userUpdateDetail** table (this table is present in release 4.5.8 onward)
- Some fields in the **cognetic_members_card** table

Note: *Card codes, barcodes, and card numbers stay in the cognetic_members_card table. This avoids card numbers being reassigned to new members. To make sure no personally identifiable data is accessible in these values, the membership IDs are replaced with* ***DELETED****, and names are replaced with* ***NULL****.*

You can automate Person records to be anonymised and deleted when the **Night Batch** scheduled task runs. You can do this if you've installed the **Loyalty** component of the **Privacy Update Pack**.

1. Enable the `ClearPersonOnDeletion` **Loyalty** system setting.

   Data for newly-deleted Loyalty members is anonymised during the **Night Batch** scheduled task.

   Data for newly-deleted records of all other Person Types is cleared if they were deleted through the **Loyalty website**.

Vista Connect *records Persons that have requested to be deleted from your* ***Loyalty*** *system. If you're restoring your Loyalty database to an earlier version you'll need to delete these Person records again. Run the Connect "Redo Loyalty member deletion" PowerShell script to delete these records. You can find the script in the folder* `VistaInstall\_Install_Customisation\DataPrivacy\RedoLoyaltyMemberDeletion`*, along with instructions on how to use it.*

Anonymising personally identifiable non-member data

Use the **Night Batch** scheduled task to anonymise the personal details and transaction records of non-members captured in **Loyalty**.

Important! *Any non-member who performs a transaction in* ***Vista Mobile*** *is recorded in* ***Loyalty*** *as an "anonymous member". They're called "anonymous" because they're unknown to Loyalty, but from a data privacy perspective, their personal data isn't anonymised until the Night Batch task runs.*

1. In **Task Scheduler**, go to **Loyalty > Scheduled Tasks > General Tasks > Night Batch**

   Note: If you don't see the task, go to **File > Add/Remove Task** and add **Night Batch** from the list of tasks.

2. Right-click on **Night Batch**, and select **Edit Task Details**.

3. Configure the task parameter `AnonMembersToProcess` with a value greater than 0 (default).

   Note: Anonymous members are processed in batches. Set how many anonymous members the task will process on each run to a value that is suitable for your environment. As a guideline, we recommend a value of 5000, to balance efficiency and speed.

Loyalty PII and member personal data

For **Loyalty** 5.0.9 and later releases, auditing is automatically enabled for PII and member personal data interactions.

Every read and write access of personal data is recorded in a JSON file on your Loyalty server. The audit logs detail the acting person, the requesting source, the time of access, and the action being performed. Any identifying information of the acting person is obfuscated before being written to the audit log.

Impact of your Connect version

If you're using **Connect** 5.0.11 or higher, when a client calls Connect then Connect calls Loyalty, the original client will be logged as the requesting source. If you're using a lower version of Connect, Connect will be logged as the requesting source.

We recommend upgrading to Connect 5.0.11 or higher. This will allow you to differentiate between the various clients that are calling Connect.

Logged services and audited actions

Audit logs are created for the following services:

- visLoyalty web service (<Vista_install_folder>\Log\Audit\Loyalty.PersonalDataAuditLog.json).
- Vista Loyalty Member service (<Vista_install_folder>\Log\ServiceFramework\Audit\Vista.Service.Loyalty.Members.PersonalDataAuditLog.json).

Read and write actions to the following data are audited:

- Bulk cards
- Cards
- Clubs
- Contact details
- Genres
- Film history
- Linked cards and members
- Loyalty Admin pages
- Manual recognitions and transactions
- Member details for current and pending members
- Messages and responses
- Passwords
- Payment methods
- Payment records
- Points
- Preferences
- Preferred sites
- Recognitions
- Redemptions
- Subscriber profile photos
- Subscription status
- Transactions
- User logs
- Watchlists

Detailed Member History report

The **Privacy Update Pack** adds the **Detailed Member History** report to the available reports on the **Loyalty website**.

Generate a **Detailed Member History** report for any Loyalty member who asks to be provided with the information you hold about their membership. The data provided spans their entire history as a member. It includes personal and membership details, points balances, transactions, activity involving points and recognitions, and an audit of any changes made to their Member record.

***Note**: You can't run this report for deleted members.*

Report Prompts

Prompt	Description
Member ID	Enter the **Person ID** of the member you want to generate the report for. **Note**: You can filter by either **Member ID** or **Card number**.

Card number	Enter the **Card Number** of the member you want to generate the report for. **Note**: Filter by **Member ID** or **Card number**. If the member has multiple cards, enter any one of their card numbers. The report will include data for all their memberships.

Terms Used

Term	Description
Personal details	All details entered on the **Loyalty website**'s **Add/Modify Person** page for the member.
Membership details	All details entered in the **Club Details** section of the **Loyalty website**'s **Add/Modify Member** page for the member. **Note**: These details are included for every club they are currently a member of.
Points balance details	Lists the member's points balances (grouped by Balance Type) and the expiry dates of their points.
Sales transactions	Displays the details of every transaction made by the member. Details include: Date, Transaction Number, Site, Item, Quantity, Sales value, Redemption value, Discount value, Movie, and Recognition.
Recognition redemptions	Displays the details of every recognition redeemed by the member. Details include: Date, Transaction Number, Site, Recognition, Quantity taken, Points cost, and Note.
Points transactions	Displays the details of activites in which the member earned or redeemed points. Details include: Date, Transaction Number, Site, Sequence, Sales value, Balance type, Points earned, Points redeemed, Description, Reason, and User.
Audit history	Displays a history of all changes made to the member's account, such as PIN changes, card replacements, and points adjustments. Details include: Date, Action, Site, User, Old value, and New value.

Reference information

IN THIS PART

Privacy Control cabinet column descriptions

Column	Description
Table	The name of a database table that contains personal data.
Personal Data Column	The name of a database column that contains personal data.
Data Subject	The category of the personal data. The **Patron Data**, **Business Contact**, and **Vista User** data subjects relate to a person. The **Vista End Point** data subject relates to the location of a web service.
Anonymisation Method	Describes how the relevant personal data will be anonymised. For example, by the **Database Purge Monitor** (page 7). **Note: Not Implemented** means you'll need to manually remove or anonymise the personally identifiable data for the relevant table column.
Replacement Value	The value that will overwrite personal data to anonymise it. Replacement values can replace an individual's personal data with a generic identifier. This lets you identify the transaction without identifying an individual. **For example:** The email address a patron entered to make a booking (**jane.doe@email.com**) will be replaced with the booking number and a generic email suffix (**364578.noreply@vista.co**). This tells you a personal email address was anonymised. You can still find the transaction using the booking number. Similarly, phone numbers will be anonymised with **123 456 789**. **Note:** If this column is blank, the personal data values are replaced by an empty string.
Anonymisation Base Date Column	The name of a database column which stores the date that will be used to calculate when data will be anonymised.

Database Purge Monitor data types

The data stored in your Vista databases (including personal data) is categorised as one of these data types. The **Database Purge Monitor** (page 7) deletes or anonymises information depending on what data type it is.

Data type	Personal data captured	What the monitor does with this data type

Privacy data	Patron	References the **Privacy Control** cabinet (page 6) to anonymise personal identifiers in patron data in Vista database tables. Replaces a patron's personal data with the anonymised value supplied by the **Replacement Value** column in the Privacy Control cabinet (page 6). The number of days that this data is kept (before it is anonymised) is calculated from the **Anonymisation Base Date**. **Note: Privacy data** is the only data type available across multiple Vista products. Other data types are only available in **Vista Cinema**.
Transaction data	Patron and Vista user	Purges transaction data (if this data hasn't already been purged manually or by the Purge Historical Data (page 10) task) from the transaction tables after the number of days specified in the monitor. **Important!** Ensure the Summariser in **Task Scheduler** is enabled. If it isn't, this data can't be purged until it becomes older than the stored summarised data.
Bookings	Patron	Purges patron data connected to a booking. This includes regular bookings and table bookings. The number of days that this data is kept is calculated from the date the booking was collected. **Important!** Ensure the **Release Bookings** scheduled task is enabled so uncollected bookings are captured and purged also.
Kitchen prepare and pickup	Patron	Purges patron data related to food and drink orders. This includes patron seat details and information about food and drink orders. The number of days that this data is kept is calculated from the date the kitchen prepared the order. **Important!** The number of days that this data is kept must be less than for **Bookings** data. This is because Bookings data can't be purged unless kitchen prepare and pickup data has been purged.
Alert history	Vista user	Purges historical data for alerts if you have them configured and running. **For example:** the details of a **POS** operator who triggered a risk profile by having too much cash in their till.
Key logs and error logs	Vista user	Purges user data captured by key presses, **POS** button presses, audit logging (the audit domain log can contain business data), and **Head Office** download logs. The number of days that this data is kept is calculated from the date the log was generated.
User log	Vista user	Purges user-log information. This could include user names and important actions users completed. **For example:** any properties users have edited.
Scheduler process history	Unrelated to personal data or data subjects	Ensures scheduled tasks run quickly and efficiently.

Seating data	Unrelated to personal data or data subjects	Purges information related to a session's seat allocation. The number of days that this data is kept is calculated from the day the session is completed. **For example:** where seats are and whether they have been booked in relation to a session.
Summarised data	Unrelated to personal data or data subjects	Purges records from summarised transaction table data that was uploaded to **Head Office**. ***Note:*** *This data type includes summarised session and film programming data from the 5.0.2.28 release of the Privacy Update Pack and the 5.0.2.28, 5.0.3.33, and 5.0.4.11 releases of Cinema.* **Tip!** This data takes less database space and can be kept for a greater number of days. The default is 400.
Time and attendance data	Vista user	Purges summarised data related to your staff's work hours, such as clock-in times, breaks, and shift comments. ***Note:*** *This data type was added in the 5.0.2.28 release of the Privacy Update Pack and the 5.0.2.28, 5.0.3.33, and 5.0.4.11 releases of Cinema.*
Closed checks	Patron	Purges data for closed checks, and debtors who have no open checks. The number of days that this data is kept is calculated from the date the check was opened. ***Note:*** *The transactions for a closed check are transaction data. The debtors and checks data type will not purge a closed check's transactions.* ***Note:*** *This data type was added in the 5.0.2.28 release of the Privacy Update Pack and the 5.0.2.28, 5.0.3.33, and 5.0.4.11 releases of Cinema.*
Point of sale sessions	Vista user	Purges data for summarised **POS Sessions**. The number of days that this data is kept is calculated from the date the POS Session was closed. ***Note:*** *This data type was added in the 5.0.2.28 release of the Privacy Update Pack and the 5.0.2.28, 5.0.3.33, and 5.0.4.11 releases of Cinema.*

SEE ALSO

Database Purge Monitor 7
Database Purge Monitor data types 27
Manually purging your Vista databases 8

Database Purge Monitor columns

Settings tab

Column	Description
Purge	Indicates whether the data type will be purged. Checkboxes are automatically selected when a **Run Method** is set.

Data Type	The data type (see "Database Purge Monitor data types" page 27) that will be affected by your purge settings.
Run Method	Describes how each data type will be purged. Options: • **Blank**: Data type isn't purged • **Manual**: Data type is manually purged • **Scheduled**: Data type is purged by a scheduled task • **Manual and Scheduled**: Data type is purged by a scheduled task, *and* you can manually purge it
Days to Retain	The number of days each data type will be kept before it is purged.
Last Run Date	Timestamp of when the data type was last purged.

Database Purge Monitor run methods

Run Method	Description
Blank/no run method selected	This data type won't be purged (or anonymised, in the case of **Privacy Data**).
Manual	Purge (or anonymise, in the case of **Privacy Data**) this data type by clicking **Home > Purge Now** in **Database Purge Monitor**. **Warning!** Database Purge Monitor can't be closed while performing a manual purge. If this is your first time performing a purge, or if you will potentially purge a large amount of data, we recommend using a scheduled purge.
Scheduled	Purge (or anonymise, in the case of **Privacy Data**) this data type using the **Purge Historical Data** task.
Manual and Scheduled	Purge (or anonymise, in the case of **Privacy Data**) this data type by doing either of the following: • Clicking **Home > Purge Now** in **Database Purge Monitor**. • Using the **Purge Historical Data** task.

Index