One Identity Manager 8.1.1

Data Archiving Administration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Data Archiving Administration Guide
Updated - August 2019
Version - 8.1.1

Contents

Change management **4**
Implementing a One Identity Manager History Database 4
Permissions for the One Identity Manager History Database on an SQL Server 5
Advanced configuration for transferring data 9
Tips for using more than one SQL Server 12
Tips for using integrated Windows authentication 14
Setting up an Administrative Workstation 14
Installing and updating a One Identity Manager History Database 15
Declaring the database source in the One Identity Manager History Database 16
Archiving procedure setup 18
Selecting an archiving procedure in the One Identity Manager database 19
Specifying data retention periods 20
Configuring the databases for direct archiving 22
Direct deletion of records in the One Identity Manager database 23

About us **25**
Contacting us 25
Technical support resources 25

Index **26**

1

Change management

Initially, all changes made to data in the One Identity Manager are saved in the One Identity Manager database. One Identity Manager historical data is transferred at regular intervals into a One Identity Manager History Database. Therefore, the One Identity Manager History Database provides an archive of change information. Statistical analyzes are carried out in the One Identity Manager History Database that simplify how trends and flows are presented. Historical data is evaluated using the TimeTrace function or using reports.

Implementing a One Identity Manager History Database

When you implement the History Database, you should consider the effects it will have on performance. It might be necessary to create more One Identity Managers at certain intervals (for example, yearly, quarterly or monthly) depending on the amount of data in the One Identity Manager History Database database, the data to be logged and how often changes are made.

The following steps are required for setting up a working environment for the One Identity Manager History Database:

- Setting up an Administrative Workstation
- Creating and migrating the One Identity Manager History Database
- Installing and configuring the One Identity Manager Service for the One Identity Manager History Database
- Declaring the Source Database
- Archiving procedure setup

Detailed information about this topic

- Setting up an Administrative Workstation on page 14
- Permissions for the One Identity Manager History Database on an SQL Server on page 5
- Tips for using more than one SQL Server on page 12
- Tips for using integrated Windows authentication on page 14
- Installing and updating a One Identity Manager History Database on page 15
- Declaring the database source in the One Identity Manager History Database on page 16
- Archiving procedure setup on page 18

Permissions for the One Identity Manager History Database on an SQL Server

The following users are identified for using a One Identity Manager History Database on an SQL Server with the granular permissions concept. User permissions at server and database level are matched to their tasks.

NOTE: If you want to switch to granular permissions when you update from 8.1.x at a later date, contact support. To access the Support Portal, go to https://support.oneidentity.com/identity-manager/.

- Installation user

  The installation user is needed for the initial installation of a One Identity Manager History Database using the Configuration Wizard.

  NOTE: If you want to change to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.1, you will also require an installation user.

- Administrative user

  The administrative user is used by One Identity Manager components that require permissions at server and database level, including for example the Configuration Wizard, DBQueue Processor or the One Identity Manager Service.

- Configuration user

  The configuration user can execute configuration tasks within the One Identity Manager, for example, creating working with the Designer. Configuration users need permissions at the server and database levels.

- End user

  End users are only assigned permissions at database level in order, for example, to complete tasks with the HistoryDB Manager.

Permissions for installation users

An SQL Server login and a database user with the following permissions must be provided for the installation user.

SQL Server:

- Member of **dbcreator** server role

  This server role is required if the database is created by the Configuration Wizard and if you are updating from version 7.0.x, 7.1.x or 8.0.x to version 8.1.1.

- Member of **securityadmin** server role

  This server role is required to create the SQL Server logins.

- Permission **view server state** and permission **alter any connection** with the option **with grant option**

  These permissions are required to check connections and close these if necessary.

- **alter any server role** permission

  This permission is required to create the server role for the administrative user.

msdb database:

- **Select** permission with the option **with grant option** for the `dbo.sysjobs`, `dbo.sysjobschedules`, `dbo.sysjobactivity` and `dbo.sysschedules` tables

  The permissions are required to execute and monitor database schedules.

- **alter any user** permission

  This permission is required to create the necessary database users for the administrative user.

- Permission **alter any role**

  This permission is required to create the necessary database role for the administrative user.

- Member of the **SQLAgentUserRole** database role

  This database role is required for managing database schedules during an update from version 7.0.x, 7.1.x or 8.0.x to version 8.1.1.

master database:

- **alter any user** permission

  This permission is required to create the necessary database users for the administrative user.

- Permission **alter any role**

  This permission is required to create the necessary database role for the administrative user.

- Permission **Execute** with the option **with grant option** for the procedure `xp_readerrorlog`

  This permission is required to find out information about the database server's system status.

One Identity Manager History Database:

- Member of the **db_owner** database role

  This database role is only required if you wish to use an existing database or a schema update is performed when installing the schema with the Configuration Wizard.

Permissions for administrative users

The following principal elements with the permissions are created for the administrative user during the installation of the One Identity Manager History Database with the Configuration Wizard:

SQL Server:

- **OneIMAdminRole_<DatabaseName>** server role
  - **alter any server role** permission

    This permission is required to create the server role for the configuration user.
  - **view any definition** permission

    The permission is required to link the SQL Server logins for the configuration user and the end user with the corresponding database users.
- **<DatabaseName>_Admin** SQL server login
  - Member of the **OneIMAdminRole_<DatabaseName>** server role
  - Permission **view server state** and permission **alter any connection** with the option **with grant option**

    These permissions are required to check connections and close these if necessary.

msdb database:

- **OneIMRole_<DatabaseName>** database role
  - Member of the **SQLAgentUserRole** database role

    The database role is required to execute database schedules.
  - **Select** permission for the `dbo.sysjobs`, `dbo.sysjobschedules`, `dbo.sysjobactivity` and `dbo.sysschedules` tables

    The permissions are required to execute and monitor database schedules.
- **OneIM_<DatabaseName>** database user
  - Member of the **OneIMRole_<DatabaseName>** database role
  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

master database:

- **OneIMRole_<DatabaseName>** database role
  - Permission **Execute** for the procedure `xp_readerrorlog`

    This permission is required to find out information about the database server's system status.
- **OneIM_<DatabaseName>** database user
  - Member of the **OneIMRole_<DatabaseName>** database role
  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

One Identity Manager History Database:

- **Admin** database user
  - Member in **db_owner** database role

    The database role is required to update a database with the Configuration Wizard.
  - The database user is assigned to the **<DatabaseName>_Admin** SQL server login.

Permissions for configuration users

The following principal elements with the permissions are created for configuration users during the installation of the One Identity Manager History Database with the Configuration Wizard:

SQL Server:

- **OneIMConfigRole_<DatabaseName>** server role
  - Permission **view server state** and permission **alter any connection**

    These permissions are required to check connections and close these if necessary.
- **<DatabaseName>_Config** SQL login
  - Member of the **OneIMConfigRole_<DatabaseName>** server role

One Identity Manager History Database:

- **OneIMConfigRoleDB** database role
  - **Create Procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create View**, **Insert**, **Execute**, **Create function** permissions for the database
- **Config** database user
  - Member of the **OneIMConfigRoleDB** database role
  - The database user is connected with the **<DatabaseName>_Config**SQL Server login.

Permissions for end users

The following principals are created with the permissions for end users during the installation of the One Identity Manager History Database with the Configuration Wizard:

SQL Server:

- **<DatabaseName>_User** SQL login

One Identity Manager History Database:

- **OneIMUserRoleDB** database role
  - **Insert**, **Update**, **Select**, **Delete** permissions for selected tables in the database
  - **View Definition** permission for the database
  - Permissions **Execute** and **References** for individual function, procedures and types
- **User** database user
  - Member of the **OneIMUserRoleDB** database role
  - The database user is connected with the **<DatabaseName>_User** SQL Server login.

Tips for using integrated Windows authentication

Integrated Windows authentication can be used without restriction for the One Identity Manager Service and the web applications. Integrated Windows authentication can be used for FAT clients. Use of Windows groups for logging in is supported. To ensure functionality it is strongly recommended you use SQL Server login.

To implement Windows authentication

- Set up an SQL Server login for the user account on the database server.
- Enter **dbo** as the default schema.
- Assign the required permissions SQL server login.

Advanced configuration for transferring data

There are tow scenarios for transferring data:

- Scenario 1: The One Identity Manager History Database and One Identity Manager database are on the same database server.
- Scenario 2: The One Identity Manager History Database and One Identity Manager database are on different database servers. The linked server is created by the One Identity Manager History Database's One Identity Manager Service.
- Scenario 3: The One Identity Manager History Database and One Identity Manager database are on different database servers. There is a linked server available.

Scenario 1:

NOTE: If you work with **sa**, no other steps are required.

If you are working with granular permissions at server and database level, user Designer to create a database user in the One Identity Manager for transferring data.

To set up the database user in the One Identity Manager database

1. In Designer, select the category **Base data | Security settings | Database server permissions | Database server login**.
2. Click and enter the following information:

   Login name: SQL Server The user's login name used for process handling in the History Database (`DialogDatabase.ConnectionString`).

   Database user: Name of the database user.
3. Select the **Database and server roles** tab and assign the role **Database: Data archiving role**.
4. Save the changes.

The DBQueue Processor creates the database role **OneIMHistoryRoleDB** and the database users in the One Identity Manager database. The database user is connected with the SQL Server login and added in the database role.

Scenario 2:

NOTE: If you work with **sa**, no other steps are required.

If you are working with granular permissions at server and database level, additional permissions are required for creating a linked server and for data transfer.

- To create a linked server, the user for process handling in the History Database (`DialogDatabase.ConnectionString`) requires the following permissions at server level:
  - Permission **alter any linked server**

    This permission is required for creating and deleting a linked server. The linked server allows distributed queries to be executed.
  - Permission **alter any login**

    This permission is required for creating and deleting a login name assignment on the local server and a login name on the linked server.
- Create an SQL Server login for data transfer on the database server that hosts the One Identity Manager database.

- In Designer, create a database user in the One Identity Manager database.

  To set up the database user in the One Identity Manager database

  1. In Designer, select the category **Base data | Security settings | Database server permissions | Database server login**.
  2. Click and enter the following information:

     Login name: SQL Server login for data transfer.

     Database user: Database user.
  3. Select the **Database and server roles** tab and assign the role **Database: Data archiving role**.
  4. Save the changes.

  The DBQueue Processor creates the database role **OneIMHistoryRoleDB** and the database users in the One Identity Manager database. The database user is connected with the SQL Server login and added in the database role.

Scenario 3:

- Create an SQL Server login for data transfer on the database server that hosts the One Identity Manager database.
- In Designer, create a database user in the One Identity Manager database.

  To set up the database user in the One Identity Manager database

  1. In Designer, select the category **Base data | Security settings | Database server permissions | Database server login**.
  2. Click and enter the following information:

     Login name: SQL Server login for data transfer.

     Database user: Database user.
  3. Select the **Database and server roles** tab and assign the role **Database: Data archiving role**.
  4. Save the changes.

  The DBQueue Processor creates the database role **OneIMHistoryRoleDB** and the database users in the One Identity Manager database. The database user is connected with the SQL Server login and added in the database role.
- Set up the linked server and reference the SQL Server login for data transfer.

  To provide a linked server, it is recommended to use the SQL procedures `sp_addlinkedserver`, `sp_setNetname` and `sp_addlinkedsrvlogin`.
- Keep the link server names ready. You need them when you declare the source database in the One Identity Manager History Database.
- In the One Identity Manager History Database, enabled the configuration parameter **HDB | UseNamedLinkedServer**.

Tips for using more than one SQL Server

NOTE: If the One Identity Manager History Database database and the One Identity Manager database are on different servers, only matching versions and patches of the operating system and database system are supported.

If the One Identity Manager History Database and the One Identity Manager database are on different database server, the following prerequisites for data acquisition must be guaranteed on both servers:

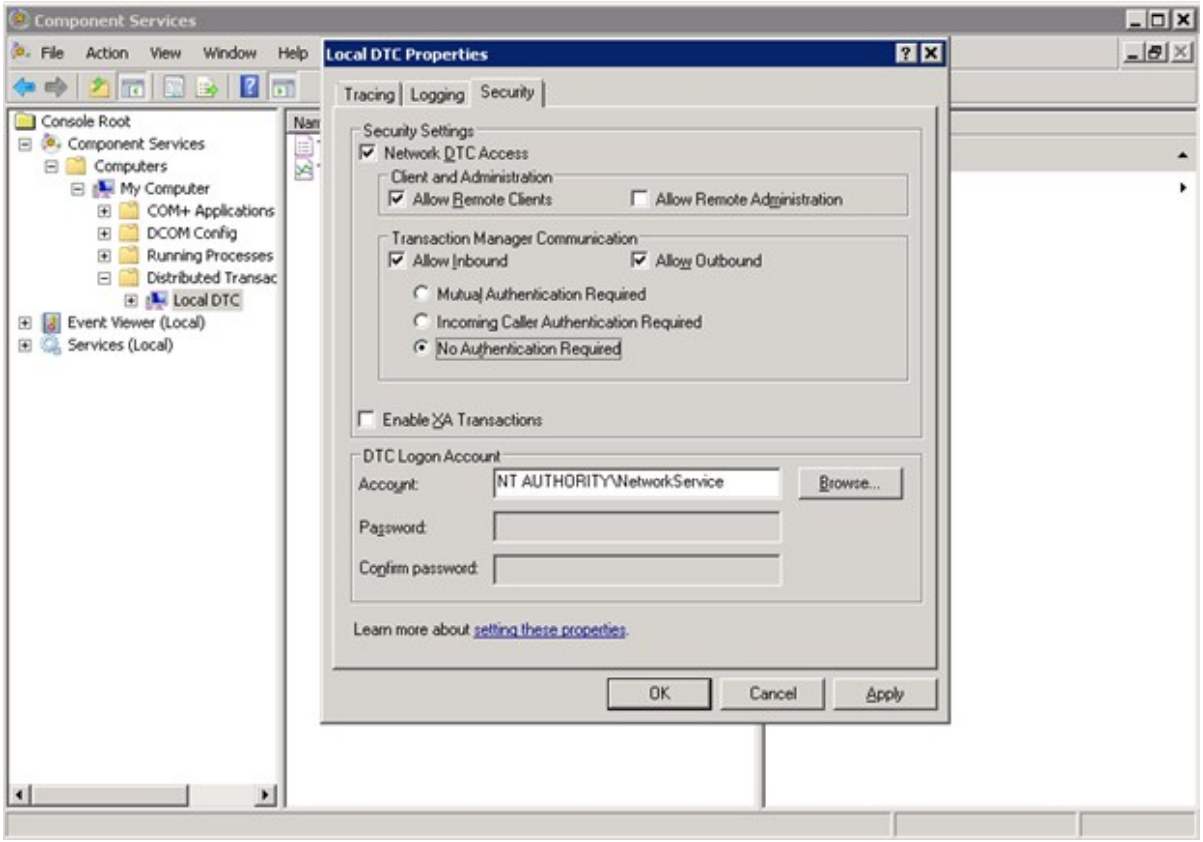
- Start of the services **Microsoft Distributed Transaction Coordinator**(DTC), **RPC Client** and **Security Accounts Manager**
- For network communications between the server, check the firewall settings and, if required, adjust them according to the recommendations of the operating system in use. For more information, refer to the operating system documentation.

Enable the following options in the DTC security settings:

- Network DTC Access
- Allow Remote Clients
- Allow Inbound
- Allow Outbound
- No Authentication Required

Configure the security settings in the Microsoft Management Console with the Component Services snap-in.

Figure 1: Configuring DTC Security Settings



The timeout for remote queries should be increased on the database server containing the One Identity Manager database if large amounts of data are transferred from the One Identity Manager History Database database to the One Identity Manager. The default setting is 600 seconds, which corresponds to 10 minutes latency. If the timeout expires, data transfer is aborted. The timeout for remote queries should be orientated on the runtime interval of the data transfer schedule.

You can query the timeout with the following statement:

```
select * from sys.configurations where name like '%remote query timeout%'
```

To change the timeout for remote queries, use the following statement:

```
exec sp_configure 'remote query timeout (s)',<new value>
RECONFIGURE WITH OVERRIDE
```

where:

```
<new value> = new timeout value in seconds
```

Tips for using integrated Windows authentication

If you use Windows integrated authentication, the data transfer takes place with the One Identity Manager History Database's One Identity Manager Service user account.

- Set up an SQL Server login for the user account on the database server. If the One Identity Manager History Database and the One Identity Manager database are on different servers, set up the SQL Server login on both database servers.
- Assign the required permissions for data transfer to the SQL server login. For more information, see Permissions for the One Identity Manager History Database on an SQL Server on page 5.

If the One Identity Manager History Database, One Identity Manager Service and the One Identity Manager database are on different server the following prerequisites have to be fulfilled:

- The One Identity Manager Service user account requires a Service Principal Name (SPN) for authentication. This can be created with the following command line:

  ```
  SetSPN -A HTTP/<Full domain name> <Domain>\<user account>
  ```

- The One Identity Manager Service user account must be available for delegation and use Kerberos for authentication.

  To do this, set the option **Trust this user for delegation to any service (Kerberos only)** on the **Delegations** tab in the Microsoft Management Console for Active Directory users and computers.

- The SQL Server service requires a Service Principal Name for authentication. You can check this with the following command line call:

  ```
  SetSPN -L <name of database>
  ```

Setting up an Administrative Workstation

The system prerequisites for installing the One Identity Manager History Database tools on an administrative workstation and the permissions required are listed in the *One Identity Manager Installation Guide*.

You should install at least the following tools on an administrative workstation:

- HistoryDB Manager
- Job Queue Info
- Configuration Wizard
- Designer

The following prerequisites must be in place on the workstation on which the One Identity Manager History Database schema installation and update is run:

- Installing the Configuration Wizard
- Access to the installation sources

  NOTE: If you copy the installation files to a repository, you must ensure that the relative directory tree remains intact.

Use the installation wizard to install One Identity Manager History Database tools on workstations for the first time.

To install components

1. Launch `autorun.exe` from the root directory of the One Identity Manager installation medium.
2. Go to the **Other products** tab, select **One Identity Manager History Database**, and click **Install**.
3. This starts the installation wizard. Select the language and click **Next**.
4. Specify the data for installation source and target on **Installation settings**.
   - Select the directory with the installation files under **Installation source**.
   - Select the directory into which to install the History Database files under **Installation folder**.
   - Click **Next**.
5. Specify machine roles and installation packages on **Assign machine roles** and click **Next**.

   NOTE: The machine roles appropriate for the One Identity Manager modules are activated. All installation subpackages are selected when you select the machine role. You can deselect individual packages.
6. You can start different programs for further installation on the last page of the install wizard.
   - To perform installation of the One Identity Manager History Database schema, start the Configuration Wizard and follow the instructions of the Configuration Wizard.

     NOTE: Perform this step only on the work station on which you start the installation of the One Identity Manager History Database schema.
7. Click **Finish** to close the installation wizard.
8. Close the autorun program.

Installing and updating a One Identity Manager History Database

The One Identity Manager database and One Identity Manager History Database must have the same version level.

Installation and update of a One Identity Manager History Database is similar to a One Identity Manager database. Use the Configuration Wizard to set up the One Identity Manager History Database. The Configuration Wizard executes the following steps.

1. Installs the One Identity Manager History Database schema in a database.

   The Configuration Wizard can create a new database and install the schema. Alternatively, the schema can be installed in an existing database.
2. Creates the required SQL Server logins and database users permissions for the administrative user, configuration user and end user.
3. Creates administrative system users and permissions groups.
4. Installs and configures the One Identity Manager Service with direct access to the One Identity Manager History Database for handling SQL processes.

For detailed information about system prerequisites for installing and updating a database, see the *One Identity Manager Installation Guide*.

Declaring the database source in the One Identity Manager History Database

Declare the One Identity Manager database to be used for transferring data to the One Identity Manager History Database. Use the HistoryDB Manager to set up access to the source databases.

To declare the source database

1. Start the HistoryDB Manager and enter the connection data.
2. Select **History | Base Data | Source databases**.

3. Select the source database in the result list and edit the master data.

Table 1: Data for Source Database

Property	Meaning

Server	Name of the database server where the One Identity Manager database is installed.
	The server name can be queried in the One Identity Manager database using the following statement:
	`select @@SERVERNAME`
	If the server can be reached through a specific port, enter the port as follows.
	`Server name, port`
	NOTE: If you are providing a linked server, enter its name here. For more information, see Advanced configuration for transferring data on page 9.

Database	Name of the One Identity Manager database.
Database ID	Database ID of the One Identity Manager database. This ID corresponds to the UID of the database entry in the One Identity Manager database. NOTE: Using the Object Browser, connect to the One Identity Manager database and copy from the table `DialogDatabase` and the value of the `UID_Database` column. Insert the value in **Database ID**.
Use integrated Windows authentication	If you use integrated Windows authentication, the data transfer takes place with the One Identity Manager Service user account. You need to take certain installation prerequisites into account in order to use this authentication procedure. For more information, see Installing and updating a One Identity Manager History Database on page 15.
Database user	SQL Server login user for data transfer. This data is only required if the One Identity Manager History Database and One Identity Manager database are on different servers and there is not linked server. For more information, see Advanced configuration for transferring data on page 9.
Password	Password for the SQL Server login. This data is only required if the One Identity Manager History Database and One Identity Manager database are on different

Property	Meaning
	servers and there is not linked server. For more information, see Advanced configuration for transferring data on page 9.
Start and end of the recordings	These date specifications are automatically set and updated when the recordings are imported.

4. Save the changes.

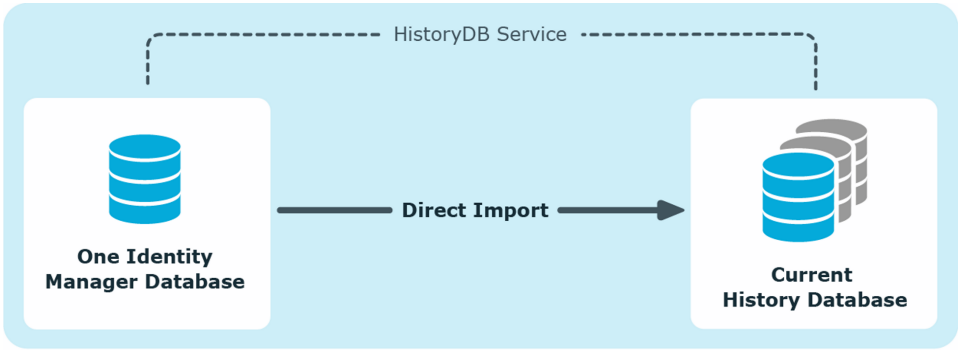
Archiving procedure setup

All records logged in One Identity Manager are initially saved in the One Identity Manager database. The proportion of historical data to total volume of a One Identity Manager database should not exceed 25 percent. Otherwise performance problems may arise. Records should be regularly removed from the One Identity Manager database and archived.

The following methods are provided for regularly removing data recorded from the One Identity Manager database:

- The data can be transferred directly form the One Identity Manager database into a One Identity Manager History Database. This is the default procedure for data archiving. Select this method if the servers on which the One Identity Manager database and the One Identity Manager History Database are located have network connectivity.
- The data is deleted from the One Identity Manager database after a certain amount of time without being archived.

Figure 2: Transferring Records to the One Identity Manager History Database



All records in the History Database database that are triggered by an action are grouped together into a process group based on an ID number, the GenProcID, for direct transfer to a One Identity Manager. The exported process groups along with the associated records are delete from the One Identity Manager database once the export has been successfully completed.

The following conditions have to be met for direct transfer to a One Identity Manager History Database:

- The subsection of records is configured for export.
- The retention period for all records that belong to a process group has ended, not taking into account whether the section of record is labeled for export or not.
- There are no processes enabled with the process group GenProcID in the DBQueue, Job queue or as planned operations.
- There is at least one record in the subsection of records for the triggered action that should exported.

Both databases for archiving records in a One Identity Manager History Database - the One Identity Manager database and the One Identity Manager History Database - have to be configured.

Selecting an archiving procedure in the One Identity Manager database

Select the basic procedure by setting the **Common | ProcessState | ExportPolicy** configuration parameter. If the configuration parameter is disabled, the data remains in the One Identity Manager database. If the configuration parameter is enabled, the selected procedure is applied.

Table 2: Permitted values for the Common | ProcessState | ExportPolicy configuration parameter

Value	Meaning
HDB	The files are transferred directly to the One Identity Manager History Database after a specified time period has expired.
NONE	The data is deleted in the One Identity Manager database after the specified time period has expired.

After selecting the basic procedure, you can specify whether data is exported or deleted for each subsection of records individually. You use configuration parameters to make the choice for each subsection.

Table 3: Configuration Parameter for Handling Change Data

Configuration parameter	Meaning
Common | ProcessState | PropertyLog | IsToExport	Exports the data changes. If this configuration parameter is not set the information is deleted once the retention period has expired.

Configuration parameter	Meaning
Common | ProcessState | PropertyLog | LifeTime	This configuration parameter specifies the maximum retention period in the database for log entries from change tracking.

Table 4: Configuration Parameter for Handling Process Information

Configuration parameter	Meaning
Common | ProcessState | ProgressView | IsToExport	Exports the data in the process information. If this configuration parameter is not set the information is deleted once the retention period has expired.
Common | ProcessState | ProgressView | LifeTime	This configuration parameter specifies the maximum length of time that log data from process information can be kept in the database.

Table 5: Configuration Parameter for Handling Process History

Configuration parameter	Meaning
Common | ProcessState | JobHistory | IsToExport	Exports the information in the process history. If this configuration parameter is not set the information is deleted once the retention period has expired.
Common | ProcessState | JobHistory | LifeTime	This configuration parameter specifies the maximum retention period in the database for log entries from process history.

Specifying data retention periods

Once the retention period has ended, the recorded data is either exported or deleted from the One Identity Manager database depending on which archiving method has been chosen. A longer retention period should be selected for subsections whose records will be exported than for those that will be deleted.

NOTE: If you do not specify a retention period, the records for this subsection will be deleted daily from the One Identity Manager database within the DBQueue Processor daily maintenance tasks.

The recordings are not exported until the retention period for all subsections has expired and no other active processes for the process group (GenProcID) exist in the DBQueue, process history or as planned operation.

Example 1

Records are transferred directly to the One Identity Manager History Database. The following configurations are selected for each subsection:

Configuration	Process Information	Process history	Data Changes
Export data	No	No	Yes
Retention period	3 days	4 days	5 days

This results in the following sequence:

Time	Process Information	Process history	Data Changes
Day 3	Data is deleted from the One Identity Manager database	No action	No action
Day 4	-	Data is deleted from the One Identity Manager database	No action
Day 5	-	-	Data is transferred to the One Identity Manager History Database and then deleted from the One Identity Manager database

Example 2

Records are transferred directly to the One Identity Manager History Database. The following configurations are selected for each subsection:

Configuration	Process Information	Process history	Data Changes
Export data	Yes	No	Yes
Retention period	3 days	4 days	5 days

This results in the following sequence:

Time	Process Information	Process history	Data Changes
Day 3	No action because the retention period has not ended for all subsections	No action	No action
Day 4	No action because the retention period has not ended for all subsections	Data is deleted from the One Identity Manager database	No action
Day 5	Data is exported and then deleted	-	Data is transferred to the One Identity Manager History Database and then deleted from the One Identity Manager database

Configuring the databases for direct archiving

One Identity Manager database:

- Enable the **Common | ProcessState | ExportPolicy** configuration parameter in Designer and enter the value **HDB**.
- Configure the subsections for export and define a retention period.
- In Designer, check the value of the **Common | ProcessState | PackageSizeHDB** configuration parameter. This parameter specifies the maximum number of process groups to be transferred to the History Database. The default value is **10000**.

One Identity Manager History Database:

- Declare the One Identity Manager database as source database in the One Identity Manager History Database.
- Importing is carried out at regular intervals by the One Identity Manager History Database's One Identity Manager Service. Configure and enable the system schedule **Import process information directly** in Designer.

Related topics

- Selecting an archiving procedure in the One Identity Manager database on page 19
- Declaring the database source in the One Identity Manager History Database on page 16

Direct deletion of records in the One Identity Manager database

If records from a subsection should be kept in the One Identity Manager database for a certain amount of time but are not archived later, you then have the following options:

- To exclude subsection from archiving do not configure it for export, but only specify a retention period.
- To delete all subsections with archiving, specify the retention period. Enable the **Common | ProcessState | ExportPolicy** configuration parameter in Designer and enter the value **NONE**.

The records are deleted from the One Identity Manager database by the DBQueue Processor when the retention period has ended. In addition, all entries for triggered actions that have no corresponding records in the subsections are deleted.

NOTE: If you do not specify a retention period, the records from the subsection are deleted from the One Identity Manager database during DBQueue Processor daily maintenance tasks.

If there is a large amount of data, you can specify the number of objects to delete per DBQueue Processor operation and run in order to improve performance. You use configuration parameters to make the choice for each subsection.

Table 6: Configuration Parameters for Deleting logged Data Changes

Configuration parameter	Meaning
Common | ProcessState | PropertyLog | Delete	This configuration parameter allows configuration of deletion behavior for logged data changes.
Common | ProcessState | PropertyLog | Delete | BulkCount	This configuration parameter contains the number of entries to be deleted in an operation.
Common | ProcessState | PropertyLog | Delete | TotalCount	This configuration parameter contains the total number of entries to be deleted in any processing run.

Table 7: Configuration parameters for deleting process information

Configuration parameter	Meaning
Common | ProcessState | ProgressView | Delete	This configuration parameter allows configuration of deletion behavior for process information.
Common | ProcessState | ProgressView | Delete | BulkCount	This configuration parameter contains the number of entries to be deleted in an operation.

Configuration parameter	Meaning
Common | ProcessState | ProgressView | Delete | TotalCount	This configuration parameter contains the total number of entries to be deleted in any processing run.

Table 8: Configuration Parameters for Deleting Process History

Configuration parameter	Meaning
Common | ProcessState | JobHistory | Delete	This configuration parameter allows configuration of deletion behavior for the process history.
Common | ProcessState | JobHistory | Delete | BulkCount	This configuration parameter contains the number of entries to be deleted in an operation.
Common | ProcessState | JobHistory | Delete | TotalCount	This configuration parameter contains the total number of entries to be deleted in any processing run.

Table 9: Configuration Parameters for Deleting Process Status Entries

Configuration parameter	Meaning
Common | ProcessState | Delete	This configuration parameter allows configuration of deletion behavior for process status entries.
Common | ProcessState | Delete | BulkCount	This configuration parameter contains the number of entries to be deleted in an operation.
Common | ProcessState | Delete | TotalCount	This configuration parameter contains the total number of entries to be deleted in any processing run.

Related topics

- Selecting an archiving procedure in the One Identity Manager database on page 19

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

D

data change
- retention period 20

O

One Identity Manager History Database
- archiving method 18-19
- data archiving 4, 18-19
  - configure 22
- database user
  - Microsoft SQL Server 15
- install 4
- source database 16

P

process history
- retention period 20

process information
- archive 19
- delete 23
- export 22
- import 22
- retention period 20

process monitoring
- archive 18
- retention period 20