One Identity Manager 9.0

Data Archiving Administration Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

One Identity Manager Data Archiving Administration Guide
Updated - 01 August 2022, 15:50
Version - 9.0

Contents

1

Change management

Initially, all changes made to data in One Identity Manager are saved in the One Identity Manager database. You must ensure that log entries are regularly removed from the One Identity Manager database and archived in a One Identity Manager History Database. In this way, 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.

NOTE: Any number of One Identity Manager History Databases can be used for analyzing historical data in the TimeTrace and in reports. Not only are One Identity Manager History Databases in the current format supported, but older formats in read-only mode also.

Logged data may be subject to further regulations such as statutory retention periods. It is recommended to operate One Identity Manager History Databases that correspond to the report periods. After a specified reporting period has expired, you can set up a new One Identity Manager History Database.

Depending on the volume of the One Identity Manager database data and the frequency at which it is changed, it might be necessary to create further One Identity Manager History Databases at certain intervals (such as yearly, quarterly, or monthly). The proportion of historical data to total volume of a One Identity Manager database should not exceed 25 percent. Otherwise performance problems may arise.

Setting up a One Identity Manager History Database requires the following steps:

- Installing the One Identity Manager History Database
- Declaring a One Identity Manager History Database in the One Identity Manager database
- Archiving procedure setup

Detailed information about this topic

- Installing a One Identity Manager History Database on page 5
- Declaring a One Identity Manager History Database in the One Identity Manager database on page 9
- Archiving procedure setup on page 14

Installing a One Identity Manager History Database

Installation of a One Identity Manager History Database is similar to that of a One Identity Manager database. For more information about the system prerequisites and how to install a database, see the .*One Identity Manager Installation Guide*.

Use the One Identity Manager History Database to set up the Configuration Wizard.

IMPORTANT: Always start the Configuration Wizard on an administrative workstation.

To install a database in the Configuration Wizard

1. Start the Configuration Wizard.
2. On the Configuration Wizard's home page, select the **Create and install database** option and click **Next**.
3. To install a new database, enter the following database connection data on the **Create administrative connection** page.
    - **Server**: Database server.
    - (Optional) **Windows Authentication**: Specifies whether the integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
    - **User**: SQL Server Login name of the installation user.
    - **Password**: Password for the installation user.

    - OR -

    To use an existing empty database, on the **Create administrative connection**page, select the **Use an existing, empty database for installation** option and enter the database connection information.
    - **Server**: Database server.
    - (Optional) **Windows Authentication**: Specifies whether the integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment

supports Windows authentication.

- **User**: SQL Server Login name of the installation user.
- **Password**: Password for the installation user.
- **Database**: Name of the database.

TIP: To configure additional connection settings, enable the **Advanced** option.

4. If you are creating a new database, perform the following tasks on the **Create database** page.
   a. In the **Database properties** view, enter the following information about the database.

Table 1: Database properties

Data	Description
Database name	Name of the database.
Data directory	Directory in which the data file is created. You have the following options: • **<default>**: The database server's default directory. • **<browse>**: Select a directory using the file browser. • **<directory name>**: Directory in which data files are already installed.
Log directory	Directory in which the transaction log file is created. You have the following options: • **<default>**: The database server's default directory. • **<browse>**: Select a directory using the file browser. • **<directory name>**: Directory in which transaction log files are already installed.
Memory tables directory	Directory for data file group and database file for memory-optimized tables. You have the following options: • **<default>**: The database server's default directory. • **<browse>**: Select a directory using the file browser. • **<Directory name>**: Directory in which data files for memory-optimized tables are already installed.
Initial size	Initial size of the database files. You have the following options: • **<Default>**: Default entry for the database server.

Data	Description
	• **<custom>**: User-defined entry. • Different recommended sizes: Depending on the number of employees being administrated.

b. In the **Installation source** pane, select the directory with the installation files.

- OR -

If you are using an existing database, on the **Create database** page, **Installation source** view, select the directory containing the installation files.

5. On the **Select configuration modules** page, select the **Data archiving** configuration module.
6. The installation steps are shown on the **Processing database** page.

   Installation and configuration of the database are automatically carried out by the Configuration Wizard. This procedure may take some time depending on system performance. Once processing is complete, click **Next**.

   TIP: Set **Advanced** to obtain detailed information about processing steps and the migration log.
7. On the last page of the Configuration Wizard, click **Finish**.

Additional configuration steps are required after the schema installation:

- Declare the One Identity Manager History Database in the One Identity Manager database.
- Set up the archiving procedure in the One Identity Manager database.

TIP: Alternatively, you can create the One Identity Manager History Database using the `Quantum.MigratorCmd.exe` command line program.

Calling example:

```
quantum.migratorcmd.exe
    /connection="Data Source=<Database server>;Initial Catalog=<Database>;User ID=<Database user>;Password=<Password>"
    --Install
    /Module="HDB"
    /System=MSSQL
    /LogLevel= Info
    /Destination=<source folder>
```

For more information about the `Quantum.MigratorCmd.exe` command line program, see the *One Identity Manager Operational Guide*.

Related topics

- Declaring a One Identity Manager History Database in the One Identity Manager database on page 9
- Archiving procedure setup on page 14

3

Declaring a One Identity Manager History Database in the One Identity Manager database

The One Identity Manager Service service ensures data transfer from the One Identity Manager database to the One Identity Manager History Database. Declare the One Identity Manager History Database to be used for transferring data to the One Identity Manager in the TimeTrace. Use the Designer to set up access to the One Identity Manager History Database.

NOTE: Any number of One Identity Manager History Databases can be used for analyzing historical data in the TimeTrace and in reports. Not only are One Identity Manager History Databases in the current format supported, but older formats in read-only mode also.

NOTE: Only one One Identity Manager History Database can be used as a destination for data transfer at a time, all other databases are read-only.

There are different ways to establish a connection to a One Identity Manager History Database:

- Method 1: Establish a connection to the One Identity Manager History Database through an application server.

  This is the recommended method. Use this method for accessing the One Identity Manager History Database over an encrypted connection. For more information, see Connecting a One Identity Manager History Database through an application server on page 10.

- Method 2: Establish a direct connection to the One Identity Manager History Database.

  This method uses an unencrypted connection to access the One Identity Manager History Database. For more information, see Establishing a direct connection to a One Identity Manager History Database on page 12.

Connecting a One Identity Manager History Database through an application server

Declare the One Identity Manager History Database to be used for transferring data to the One Identity Manager in the TimeTrace. Use the Designer to set up access to the One Identity Manager History Database.

Prerequisites for connecting a One Identity Manager History Database through an application server

- Declaring the One Identity Manager History Database in the TimeTrace, requires an ID.
- An ID for the One Identity Manager History Database connection is entered in the application server's configuration file (`web.config`).
    - Enter a unique ID for each One Identity Manager History Database.
    - The ID must be entered in all application servers that can be used by users to log in to the Manager.
    - The ID must be entered for the application server that the One Identity Manager Service uses to connect.
- The Manager and the Web Portal use the application server to log in. Otherwise the evaluation of the data changes in TimeTrace or in reports is not possible.
- To generate and send report subscriptions and reports by email that show changes to data, there must be a Job server set up over an application server.

  For more information about setting up a Job server and about configuring the One Identity Manager Service, see the *One Identity Manager Configuration Guide*.

To link a One Identity Manager History Database into a TimeTrace

1. Use the Designer to log in to the One Identity Manager database.
2. In the Designer, select the **Base Data > General > TimeTrace databases** category.
3. Select the **Object > New** menu item.
4. Ensure that the **Use ID from application server** option is set.
5. In **History database name**, enter the name of the One Identity Manager History Database.
6. In the **Connection parameter (read)** field, enter the ID for connecting to the One Identity Manager History Database.

   The ID must match the ID in the application server's configuration file.

7. On the One Identity Manager History Database, where the data from the One Identity Manager database will be archived:
    a. Enable the **Current transport target** option.
    b. In the **Connection parameter (transport)** field, enter the connection parameters for connecting to the One Identity Manager History Database.
8. Select the **Database > Save to database** and click **Save**.

NOTE: Set the **Disabled** option to disable the connection at a later time. If a One Identity Manager History Database is disabled, it is not taken into account when determining change data in the TimeTrace.

To configure an ID in the application server for connecting to the One Identity Manager History Database

- During installation of the application server, enter the ID for connecting to the One Identity Manager History Database.
- To connect a One Identity Manager History Database at a later date, enter the ID for connection in the application server's configuration file (`web.config`) in the `<connectionStrings>` section.

Example:

```
<connectionStrings>
    ...
    <add name="<History Database ID>" connectionString="Data
    Source=<database server>;Initial Catalog=<database name>;User
    ID=<database user>;Password=<password>"/>
    ...
</connectionStrings>
```

NOTE:

The connection credentials in the application server's configuration file are encrypted with the default Microsoft ASP.NET encryption. If you want to change the connection credentials later, you must decrypt them first and then encrypt them again afterward. Use ASP.NET IIS registration tool to decrypt and encrypt (`Aspnet_regiis.exe`).

Example call:

Decrypt: `aspnet_regiis.exe -pdf connectionStrings <path to web application in IIS>`

Encrypting: `aspnet_regiis.exe -pef connectionStrings <path to web application in IIS>`

Related topics

- Establishing a direct connection to a One Identity Manager History Database on page 12

Establishing a direct connection to a One Identity Manager History Database

Declare the One Identity Manager History Database to be used for transferring data to the One Identity Manager in the TimeTrace. Use the Designer to set up access to the One Identity Manager History Database.

To link a One Identity Manager History Database into a TimeTrace

1. Use the Designer to log in to the One Identity Manager database.
2. In the Designer, select the **Base Data > General > TimeTrace databases** category.
3. Select the **Object > New** menu item.
4. Ensure that the **Use ID from application server** option is not set.
5. In **History database name**, enter the name of the One Identity Manager History Database.
6. Declare the **Connection parameters (read)**.
    a. Click the [**...**] button next to the input field to open the input dialog for connection data.
    b. Enter the connection data for the One Identity Manager History Database.
        - **Server**: Database server.
        - (Optional) **Windows Authentication**: Specifies whether the integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
        - **User**: The user's SQL Server login name.
        - **Password**: Password for the user's SQL Server login.
        - **Database**: Select the database.
7. On the One Identity Manager History Database, where the data from the One Identity Manager database will be archived:
    a. Enable the **Current transport target** option.
    b. In the **Connection parameter (transport)** field, enter the connection parameters for connecting to the One Identity Manager History Database.
8. Select the **Database > Save to database** and click **Save**.

NOTE: Set **Disabled** to disable the connection at a later time. If a One Identity Manager History Database is disabled, it is not taken into account when determining change data in the TimeTrace.

Related topics

- Connecting a One Identity Manager History Database through an application server on page 10

Archiving procedure setup

All entries 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. You must ensure that log entries are regularly removed from the One Identity Manager database and archived.

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

- Data can be transferred directly from 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.

All records in the One Identity Manager 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 deleted 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:

- This section of the 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 is labeled for export or not.
- There are no processes enabled with the process group GenProcID in the DBQueue, Job queue, or as scheduled operations.
- For the triggered action, there is at least one record in the section to be exported.

Selecting an archiving procedure in the One Identity Manager database

Select the basic procedure by setting the **Common | ProcessState | ExportPolicy** configuration parameter. In the Designer, modify the 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.
  - **HDH**: 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 section of records individually. You use configuration parameters to make the choice for each section. In the Designer, modify the configuration parameters.

Table 2: Configuration parameter for handling logged 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.
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 | 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.

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 sections whose records will be exported than for those that will be deleted.

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

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

You use configuration parameters to define the data retention periods for the individual sections. Modify the configuration parameter in the Designer.

Table 3: Configuration parameter for retention periods

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

Example 1:

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

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	No action	No action

Time	Process Information	Process History	Data Changes
	database		
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 section:

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 sections.	No action	No action
Day 4	No action because the retention period has not ended for all	Data is deleted from the One Identity Manager	No action

Time	Process Information	Process History	Data Changes
	sections.	database	
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

Change management in a One Identity Manager History Database

Data can be transferred directly from the One Identity Manager database into a One Identity Manager History Database. This is the default procedure for data archiving.

To use this procedure, make the following configuration settings in the One Identity Manager database:

- Enable the **Common | ProcessState | ExportPolicy** configuration parameter in the Designer and enter the value **HDB**.
- Configure the sections for export and define a retention period.
- In the Designer, check the value of the **Common | ProcessState | PackageSizeHDB** configuration parameter. This parameter specifies the maximum number of progress groups that can be transferred to the One Identity Manager History Database. The default value is **10000**.
- Ensure that the **Transport to history database** schedule is enabled.

  The schedule ensures the transfer of data from the One Identity Manager database to the One Identity Manager History Database. The schedule is run by default every **6** hours. In the Designer, adjust the interval as required.

Related topics

- Selecting an archiving procedure in the One Identity Manager database on page 15
- Specifying data retention periods on page 15
- Declaring a One Identity Manager History Database in the One Identity Manager database on page 9

Deleting log entries without archiving

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

- To exclude a certain section from archiving, do not configure it for export, just specify a retention period.
- To delete all sections without archiving, specify a retention period. In the Designer, set the **Common | ProcessState | ExportPolicy** configuration parameter and enter the value **NONE**.

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

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

Related topics

- Selecting an archiving procedure in the One Identity Manager database on page 15
- Specifying data retention periods on page 15
- Optimizing performance by deleting log entries on page 19

Optimizing performance by deleting log entries

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 section.

Table 4: Configuration parameters for deleting logged data changes

Configuration parameter	Meaning
Common | ProcessState | PropertyLog | Delete	Allows configuration of deletion behavior for logged data changes.
Common | ProcessState | PropertyLog | Delete | BulkCount	Number of entries to be deleted in any operation. The default value is **200**.
Common | ProcessState | PropertyLog | Delete | TotalCount	Total number of entries to be deleted in any processing run. The default value is **10000**.

Table 5: Configuration parameters for deleting process information

Configuration parameter	Meaning
Common | ProcessState | ProgressView | Delete	Allows configuration of deletion behavior for process information.
Common | ProcessState | ProgressView | Delete | BulkCount	Number of entries to be deleted in any operation. The default value is **200**.
Common | ProcessState | ProgressView | Delete | TotalCount	Total number of entries to be deleted in any processing run. The default value is **10000**.

Table 6: Configuration parameters for deleting process history

Configuration parameter	Meaning
Common | ProcessState | JobHistory | Delete	Allows configuration of deletion behavior for the process history.
Common | ProcessState | JobHistory | Delete | BulkCount	Number of entries to be deleted in any operation. The default value is **200**.
Common | ProcessState | JobHistory | Delete | TotalCount	Total number of entries to be deleted in any processing run. The default value is **10000**.

Table 7: Configuration parameters for deleting process status entries

Configuration parameter	Meaning
Common | ProcessState | Delete	Allows configuration of deletion behavior for process status entries.
Common | ProcessState | Delete | BulkCount	Number of entries to be deleted in any operation. The default value is **500**.
Common | ProcessState | Delete | TotalCount	Total number of entries to be deleted in any processing run. The default value is **10000**.

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

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