Dell™ One Identity Manager 7.1.3

Data Archiving Administration Guide

Legend

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

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

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

One Identity Manager Data Archiving Administration Guide
Updated - November 2017
Version - 7.1.3

Contents

1

Change Management

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

Installing the HistoryDB Archive System

When you implement the HistoryDB archive system, you should consider the effects it will have on performance. It might be necessary to create more history databases at certain intervals (for example, yearly, quarterly or monthly) depending on the amount of data in the One Identity Manager 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 HistoryDB archive system:

- Setting up an administrative workstation

  For more information, see Setting up an Administrative Workstation on page 4.
- Creating and migrating the history database

  For more information, see Installing and Configuring a History Database on page 10.
- Installing and configuring a One Identity Manager History Service on a server

  For more information, see Installing and Configuring a Server on page 11.

Setting up an Administrative Workstation

The system prerequisites for installing the HistoryDB tools on an administrative workstation and the permissions required are listed in the Dell 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

Use the installation wizard to install HistoryDB tools on workstations for the first time.

To install components

1. Execute the program `autorun.exe` from the root directory on the One Identity Manager installation medium.
2. Go to the **Other products** tab, select "Dell™ One Identity Manager History Database" and click **Install**.
3. The installation wizard is started. Select the language for the installation wizard on the start page and click **Next**.
4. Specify the data for installation source and target on the **Installation settings** page.
    - Select the directory with the installation files under **Installation source**.
    - Select the directory in which to install the One Identity Manager History Database information files in **Installation directory**.
    - Click **Next**.
5. Specify machine roles and installation packages on the **Assign machine roles** page and click **Next**.

    ⓘ **NOTE:** Machine roles which match One Identity Manager modules are already selected. 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 run the HistoryDB installation, start the Configuration Wizard and following the Configuration Wizard instructions.

        ⓘ **NOTE:** Only run this step on the workstation on which you start the HistoryDB installation.
7. Click **Finish** to close the installation wizard.
8. Close the autorun program.

Prerequisites for Maintaining a History Database

When you install a history database for the first time, you need to set up an initial database beforehand. The system prerequisites for this are described in the Dell One Identity Manager Installation Guide.

Tips for Using More than One SQL Server®

ⓘ **NOTE:** If the history 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 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:

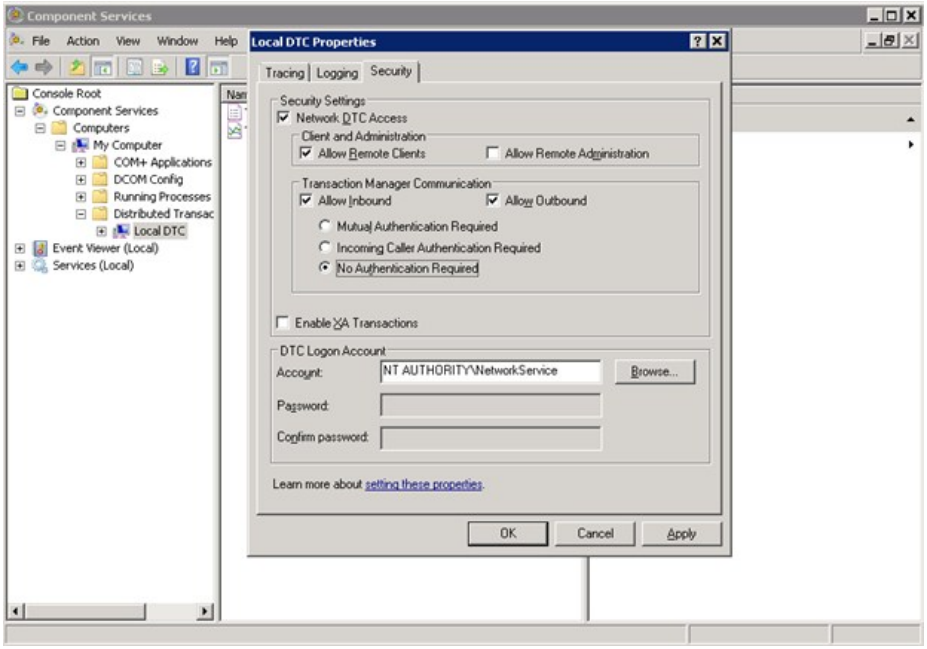
- Start the services "Microsoft Distributed Transaction Coordinator" (DTC), "RPC Client" and "Security Account Manager"
- For network communications between the server, check the Firewall settings and, if required, adjust them according to the recommendations of the operating system in use. For more 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 to the history database. 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
```

Database Users under SQL Server®

ⓘ **NOTE:** Select "English" as default language.

Database user permissions can be divided into two user types:

- End user

  End users that only work with the Web Portal, for example, only have to be members of the database role "basegroup".

- Administrative user

  Administrative users require the permissions listed in below. Here, you can differentiate between permissions for installation and permissions for normal operations.

To use HistoryDB functions to the full, you require the following permissions.

Table 1: Permissions for Database Users under SQL Server®

Permission	For Database	Required for Installation	Required to Operate	Required for
Server role "dbcreator"*		x	-	Creating the database
Server role "processadmin"		-	x	Activities for testing and closing the connection is required.
Database role "db_owner"	History database	x	x	Creating the database Database operations.
Database role "basegroup"**	History database	-	x	Internal permissions roles for database objects.
Permissions "Execute"	Master	x	x	Starting the SQL server agent.
Database role "SQLAgentUserRole"	msdb	-	x	Running database schedules.
Database role "db_Datareader"	msdb	-	x	Reading and changing database schedules.
Database role "SQLAgentOperatorRole"	msdb	x	x	Defining database schedules.
Permissions "Connect"	tempdb	x	x	Checks for single-user mode requirement during start up.

*) The permissions are only required if the database is created using the Configuration Wizard.

**) The database role "basegroup" is added during initial schema installation of the History database by default.

NOTE: If the user account for the database user is changed after migration the new database user must be entered as the owner of the database schedule afterwards. Otherwise errors occur when running the database schedules.

Additional Permissions for Data Transfer

If the history database and the One Identity Manager database are on one database server the data transfer is carried out with the database user that the history database runs under. This database user requires additional access to the One Identity Manager database.

- Database role "db_owner" for the One Identity Manager database

If the history database and the One Identity Manager database are on different database servers a connection is made to the One Identity Manager database with the database user that the history database runs under. The following permissions are also required:

- Server permissions "ALTER ANY LINKED SERVER"

  Creating and deleting a linked server. The linked server allows distributed queries to be executed.

- Server permissions "ALTER ANY LOGIN"

  Creating and deleting login name assignments on the local server and a login name on the connection server.

- Server roles "setupadmin" and "sysadmin"

  Establishing and deleting a connection between database servers.

The subsequent data transfer takes place with a database user that has access to the One Identity Manager database. The following permissions are required:

- Database role "db_owner" for the One Identity Manager database

Tips for Using Integrated Windows® Authentication

Integrated One Identity Manager Service authentication can be used for the Windows® and web applications without restriction. 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 default schema.
- Assign the required permissions SQL server login. For more information, see Table 1 on page 7.

Tips for Using Integrated Windows® Authentication

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

- Set up an SQL Server® login for the user account on the database server. If the 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 Database Users under SQL Server® on page 6.

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

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

Set the option **Trust this user for delegation to any service (Kerberos only)** on the **Delegate** tab for Active Directory® users and computers in the Microsoft Management Console.

- 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>
  ```

Tips for Using More than One Oracle Server

If the history 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.

Database Users under Oracle® Database

You should set up your own database user to use the database. You can create the database user with the Configuration Wizard or manually.

> **NOTE:** The database users involved, must get their permissions directly. When the permissions are assigned through database roles it may lead to Oracle errors when data queries are executed because of permission restrictions.

Permissions for Oracle® Database Installations

The following permissions are required for an Oracle® Database installation to use the HistoryDB functionality in full.

Table 2: Permissions for Database Users

Permission	Required For
GRANT ALTER SESSION TO <user>	Changing own user session settings.
GRANT ANALYZE ANY TO <user>	The permissions are used to execute the procedure `DBMS_STATS.FLUSH_DATABASE_MONITORING_INFO` while calculating statistics , These permissions are not required if no statistics are being determined.
GRANT CONNECT TO <user>	Connecting database.
GRANT CREATE JOB TO <user>	Creating database schedules.
GRANT CREATE PROCEDURE TO <user>	Creating schema objects.
GRANT CREATE SEQUENCE TO <user>	Creating schema objects.

Permission	Required For
GRANT CREATE SYNONYM TO <user>	Creating schema objects.
GRANT CREATE TABLE TO <user>	Creating schema objects.
GRANT CREATE TRIGGER TO <user>	Creating schema objects.
GRANT CREATE TYPE TO <user>	Creating schema objects.
GRANT CREATE VIEW TO <user>	Creating schema objects.
GRANT EXCEUTE ON DBMS_PIPE TO <user>	Communication of single processing steps concurrently with the DBQueue Processor main routine.
GRANT EXECUTE ON DBMS_CRYPTO TO <user>	Access to package for general encryption routines.
GRANT EXECUTE ON DBMS_LOCK TO <user>	Uses the sleep method for relaying processing in the DBQueue Processor, for example, to wait for single processing steps to end.
GRANT SELECT ON GV_$OSSTAT TO <user>	Loading information about the current server version.
GRANT SELECT ON GV_$SESSION TO <user>	Loading data from the current session. These permissions are also required to switch the database into single-user mode.

Additional Permissions for Data Transfer

Use the database user under which the history database runs to carry out the data transfer. This database user requires additional access to the One Identity Manager database through a database link. The database link should be made available by a database administrator. The database link has to be created uniquely.

Installing and Configuring a History Database

Installation and configuration of the database is carried out by the Configuration Wizard. The sequence is described in the Dell One Identity Manager Installation Guide.

The following prerequisites have to be implemented on the workstation, from which the schema installation starts:

- Installation of the "Configuration Wizard" program

  Use the install wizard to install the program. To do this, select the installation type "Workstation" and the installation package "Configuration" in the install wizard.

- Access the installation source

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

NOTE: Update the HistoryDB tools on this workstation with the installation wizard and not by automatic software update.

Installing and Configuring a Server

The "One Identity Manager History Service" ensures data transfer from the One Identity Manager database in the history database.

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

Use the installation wizards to install the One Identity Manager History Service on the server for the first time. Installation and configuration of the One Identity Manager History Service is analog to One Identity Manager Service. The sequence is described in the Dell One Identity Manager Installation Guide.

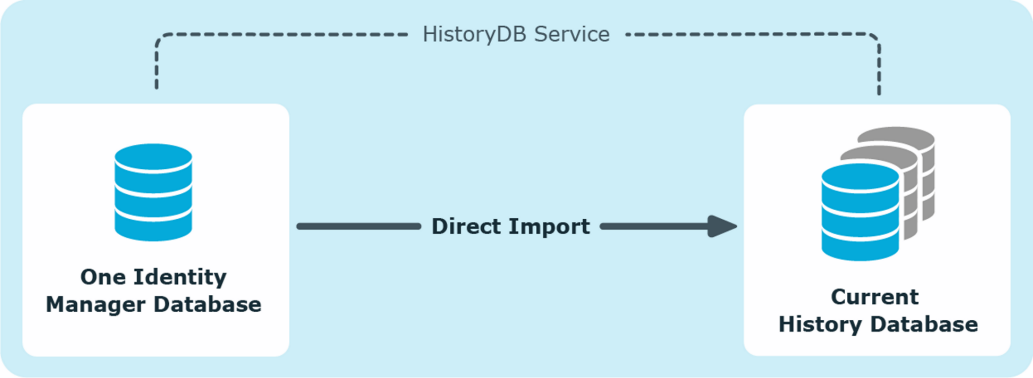
Archiving Procedure Setup

There are different methods in the One Identity Manager for tracking changes. These include recording data changes, recording process information and recording messages in the process history. The proportion of historical data to total volume of a One Identity Manager database should not exceed 25%. Otherwise performance problems may arise.

The following methods are provided for regularly removing data recorded in specific areas, from the One Identity Manager database.

- The data can be transferred directly form the One Identity Manager database into a 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 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 HistoryDB Archive System



All records in the One Identity Manager 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 history database. 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 must be fulfilled for direct transfer to a 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 - the One Identity Manager database and the history database - have to be configured.

Selecting an Archiving Procedure in the One Identity Manager Database

Select the basic procedure by setting the configuration parameter "Common\ProcessState\ExportPolicy". 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 3: Permitted Values for the Configuration Parameter "Common\ProcessState\ExportPolicy"

Value	Meaning
HDB	The files are transferred directly to the 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 4: Configuration Parameter for Handling Process Information

Configuration parameter	Meaning
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\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.

Table 5: Configuration Parameter for Handling Process History

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

Table 6: Configuration Parameter for Handling Change Data

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\PropertyLog\IsToExport	Exports the data changes. 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 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 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 history database and then deleted from the One Identity Manager database

Example 2

Records are transferred directly to the 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 history database and then deleted from the One Identity Manager database

Declaring the Source Database in the History Database

Declare the One Identity Manager database to be used for transferring data to the history database. Use the HistoryDB Manager to setup access to the source databases.

To declare the source database

- Start the HistoryDB Manager and enter the connection data.
- Select the category **History | Base Data | Source databases**.
- Select the source database in the result list.

- Edit the master data.

Table 7: 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`
	Enter the port as follows if the server can be reached through a specific port.
	`Server name, Port`

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:** Connect to the One Identity Manager database with the Object Browser and copy the value from the column `UID_Database` in the table `DialogDatabase`. Insert the value in the input field **Database ID**.
Use integrated Windows® authentication	If you use Windows® integrated authentication the data transfer takes place with the One Identity Manager History Service user account. You need to take certain installation prerequisites into account in order to use this authentication procedure. For more information refer to Prerequisites for Maintaining a History Database on page 5.
Database user	Database user used to access the source database. If the history database and the One Identity Manager database are on the same server this input is not required. The database user under which the history database runs is used to access the databases. If the history database and the One Identity Manager database are not on the same server enter the One Identity Manager database user to be used to execute the data transfer. Note the permissions described in Database Users under SQL Server® on page 6.
Password	Database user password.
Start and end dates for logging	These dates are automatically set and updated when records are imported.

- Save the changes.

Configuring Databases for Direct Archiving

One Identity Manager database:

- Enable the configuration parameter "Common\ProcessState\ExportPolicy" in the Designer and enter the value `HDB`.
- Configure the subsections for export and define a retention period. For more information, see Selecting an Archiving Procedure in the One Identity Manager Database on page 12.

- Check the value of the configuration parameter "Common\ProcessState\PackageSizeHDB". This parameter specifies the maximum number of process groups transferred to the database. The default value is 10000.

History database:

- Declare the One Identity Manager database as source database in the history database. For more information, see Declaring the Source Database in the History Database on page 14.
- Importing is carried out at regular intervals by the One Identity Manager History Service. Configure and enable the system schedule "Import process information directly" in the Designer.

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 however, then you have the following options:

- To exclude subsection from archiving do not configure it for export, but only specify a retention period. For more information, see Selecting an Archiving Procedure in the One Identity Manager Database on page 12.
- To delete all subsections with archiving, specify the retention period. Enable the configuration parameter "Common\ProcessState\ExportPolicy" in the Designer and enter the value `NONE`.

The records are deleted from the DBQueue Processor database by the One Identity Manager 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.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.quest.com.

Contacting Dell

For sales or other inquiries, visit http://quest.com/company/contact-us.aspx or call +1 949 754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.quest.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. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to http://quest.com/trials.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

Index

D

H

O

P