



One Identity Manager 8.1.2

Data Archiving Administration Guide

## Copyright 2020 One Identity LLC.

### ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

### Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

### Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

### 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 - January 2020  
Version - 8.1.2

# Contents

<b>Change management</b> .....	<b>4</b>
<b>Implementing a One Identity Manager History Database</b> .....	<b>5</b>
Permissions for the One Identity Manager History Database on a SQL Server .....	6
One Identity Manager History Database permissions in a managed instance Azure SQL Database .....	10
Advanced configuration for transferring data .....	15
Tips for using more than one SQL Server .....	17
Tips for using integrated Windows authentication .....	19
Setting up an Administrative Workstation .....	19
Installing and configuring a server .....	20
Installing One Identity Manager History Database components .....	21
Installing and updating a One Identity Manager History Database .....	22
The update process for releasing a new version .....	22
<b>Declaring the database source in the One Identity Manager History Database</b> .....	<b>25</b>
<b>Archiving procedure setup</b> .....	<b>28</b>
Selecting an archiving procedure in the One Identity Manager database .....	29
Specifying data retention periods .....	30
Configuring the databases for direct archiving .....	32
Direct deletion of records in the One Identity Manager database .....	32
Optimizing performance by deleting log entries .....	33
<b>About us</b> .....	<b>35</b>
Contacting us .....	35
Technical support resources .....	35
<b>Index</b> .....	<b>36</b>

# 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 19
- [Permissions for the One Identity Manager History Database on a SQL Server](#) on page 6
- [Tips for using more than one SQL Server](#) on page 17
- [Tips for using integrated Windows authentication](#) on page 19
- [Installing and updating a One Identity Manager History Database](#) on page 22
- [Declaring the database source in the One Identity Manager History Database](#) on page 25
- [Archiving procedure setup](#) on page 28

# Permissions for the One Identity Manager History Database on a SQL Server

The following users are identified for using a One Identity Manager History Database on a 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 8.1.2, 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 One Identity Manager, for example, 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

A 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

The server role is only required if the database is created using the Configuration Wizard.

- Member of the **sysadmin** server role

This server role is only required if the database is created by the Configuration Wizard and the directories for the file must be selected in the file browser. If the files are stored in the default database server directories, permissions are not necessary.

- Member of **securityadmin** server role  
This server role is required to create SQL Server logins.
- **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.  
The permissions are required to check connections and close these if necessary.
- **alter any server role** permissions  
The permissions are required to create the server role for the administrative user.

msdb database:

- **Select** permissions with the **with grant option** option for the `dbo.sysjobs`, `dbo.sysjobschedules`, `dbo.sysjobactivity`, and `dbo.syschedules` tables  
The permissions are required to execute and monitor database schedules.
- **alter any user** permissions  
The permissions are required to create the necessary database users for the administrative user.
- **alter any role** permissions  
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 8.1.2.

master database:

- **alter any user** permissions  
The permissions are required to create the necessary database users for the administrative user.
- **alter any role** permissions  
This permission is required to create the necessary database role for the administrative user.
- **Execute** permissions with the **with grant option** option for the `xp_readerrorlog` procedure  
The permissions are 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

During the installation of a One Identity Manager History Database using the Configuration Wizard, the following principal elements and permissions are created for the administrative user:

SQL Server:

- **OneIMAdminRole\_<DatabaseName>** server role
  - **alter any server role** permissions  
The permissions are required to create the server role for the configuration user.
  - **view any definition** permissions  
The permissions are 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
  - **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.  
The 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** permissions 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
  - **Execute** permissions for the `xp_readerrorlog` procedure  
The permissions are 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

During the installation of a One Identity Manager History Database using the Configuration Wizard, the following principal elements and permissions are created for configuration users:

SQL Server:

- **OneIMConfigRole\_<DatabaseName>** server role
  - **view server state** and **alter any connection** permissions  
The 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,** and **Create function** permissions for the database
- **Config** database user
  - Member of the **OneIMConfigRoleDB** database role
  - The database user is connected with the **<DatabaseName>\_ConfigSQL** 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,** and **Delete** permissions for selected tables in the database
  - **View Definition** permissions for the database
  - **Execute** and **References** permissions for individual functions, 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 a SQL Server login for the user account on the database server.
- Enter **dbo** as the default schema.
- Assign the required permissions SQL server login.

# One Identity Manager History Database permissions in a managed instance Azure SQL Database

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

- **Installation user**  
The installation user is needed for the initial installation of a One Identity Manager History Database using the Configuration Wizard.
- **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 One Identity Manager, for example, 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

A 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  
The server role is only required if the database is created using the Configuration Wizard.
- Member of **securityadmin** server role  
This server role is required to create SQL Server logins.
- **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.  
The permissions are required to check connections and close these if necessary.
- **alter any server role** permissions  
The permissions are required to create the server role for the administrative user.

msdb database:

- **Select** permissions with the **with grant option** option for the `dbo.sysjobs`, `sysjobsteps`, `dbo.sysjobschedules`, `dbo.sysjobactivity`, and `dbo.sysschedules` tables  
The permissions are required to execute and monitor database schedules.
- **alter any user** permissions  
The permissions are required to create the necessary database users for the administrative user.
- **alter any role** permissions  
This permission is required to create the necessary database role for the administrative user.

master database:

- **alter any user** permissions

The permissions are required to create the necessary database users for the administrative user.

- **alter any role** permissions

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

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

The permissions are required to find out information about the database server's system status.

- **Execute** permissions with the option **with grant option** for the `xp_sqlagent_is_starting`, `xp_sqlagent_notify`, and `xp_sqlagent_enum_jobs` procedures

The permissions are required to execute and monitor database schedules.

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

During the installation of a One Identity Manager History Database using the Configuration Wizard, the following principal elements and permissions are created for the administrative user:

SQL Server:

- **OneIMAdminRole\_<DatabaseName>** server role

- **alter any server role** permissions

The permissions are required to create the server role for the configuration user.

- **view any definition** permissions

The permissions are 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

- **view server state** permissions with the **with grant option** option and **alter any connection** permissions with the **with grant option** option.

The 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** permissions for the `dbo.sysjobs`, `sysjobsteps`, `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
  - **Execute** permissions for the `xp_readerrorlog` procedure  
The permissions are required to find out information about the database server's system status.
  - **Execute** permissions for the `xp_sqlagent_is_starting`, `xp_sqlagent_notify`, and `xp_sqlagent_enum_jobs` procedures  
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.

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

During the installation of a One Identity Manager History Database using the Configuration Wizard, the following principal elements and permissions are created for configuration users:

SQL Server:

- **OneIMConfigRole\_<DatabaseName>** server role
  - **view server state** and **alter any connection** permissions  
The 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,** and **Create function** permissions for the database
- **Config** database user
  - Member of the **OneIMConfigRoleDB** database role
  - The database user is connected with the **<DatabaseName>\_ConfigSQL** 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,** and **Delete** permissions for selected tables in the database
  - **View Definition** permissions for the database
  - **Execute** and **References** permissions for individual functions, procedures, and types
- **User** database user
  - Member of the **OneIMUserRoleDB** database role
  - The database user is connected with the **<DatabaseName>\_User** SQL Server login.

# Advanced configuration for transferring data

There are two 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:

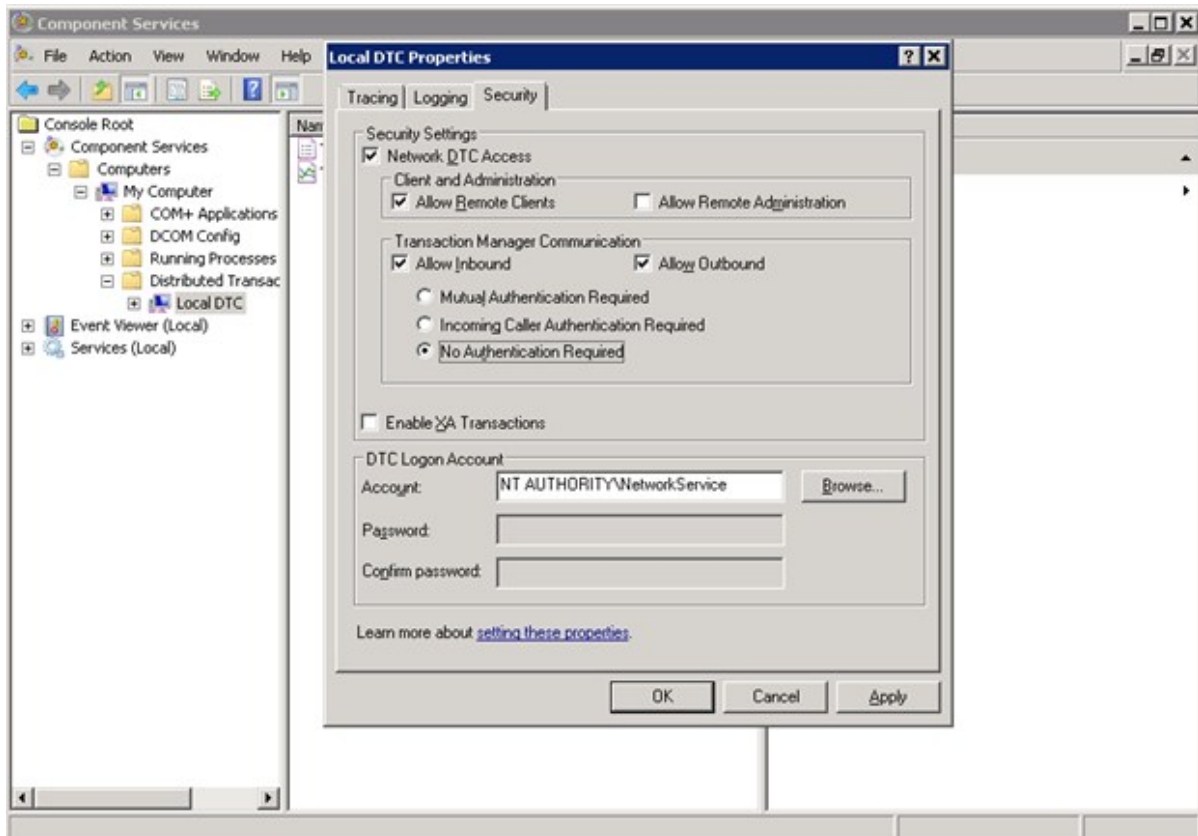
- Start of the services **Microsoft Distributed Transaction Coordinator(DTC)**, **RPC Client** and **Security Accounts Manager**
- For network communications between the server, check the firewall settings and, if required, adjust them according to the recommendations of the operating system in use. 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 a SQL Server](#) on page 6.

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 configuring a server**

The One Identity Manager History Service service ensures data transfer from the One Identity Manager database to the One Identity Manager History Database.

The system prerequisites for installing the One Identity Manager History Service on a server and the permissions required are described in the *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 *One Identity Manager Installation Guide*.

## Installing One Identity Manager History Database components

### 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. Confirm the conditions of the license.
5. On the **Installation settings** page, enter the following information.
  - **Installation source:** Select the directory containing the installation files.
  - **Installation directory:** Select the directory in which you want to install the files for One Identity Manager History Database.

**NOTE:** To make further configuration settings, click on the arrow button next to the input field. Here, you can specify whether you are installing on a 64-bit or a 32-bit operating system.

For a standard installation, no further configuration settings are necessary.
6. On the **Assign machine roles** page, define the machine roles.

**NOTE:** All installation subpackages are selected when you select the machine role. You can deselect individual packages.
7. On the **Change service properties** page, you can change the name, display name and the description for installing the One Identity Manager Service.

**NOTE:** This page is only shown if you have selected the **Server | Job Server** machine role.
8. 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:** Only perform this step on the workstation that you use to start

| installing the One Identity Manager History Database schema.

9. Click **Finish** to close the installation wizard.
10. Close the autorun program.

The One Identity Manager is installed for all user accounts on the workstation or server. In the default installation the One Identity Manager is installed under:

- %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)
- %ProgramFiles%\One Identity (on 64-bit operating systems)

## 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*.


## The update process for releasing a new version

**IMPORTANT:** The One Identity Manager database and the One Identity Manager History Database must have the same version number.

**NOTE:** Read the release notes for possible differing or additional steps for updating One Identity Manager.

For detailed information about updating a database, see the *One Identity Manager Installation Guide*.

## To update the One Identity Manager History Database to a new version

1. In the Designer, carry out all consistency checks in the **Database** section.
  - a. In the Designer, start the Consistency Editor by selecting the **Database | Check data consistency** menu item.
  - b. In the **Test options** dialog click the icon .
  - c. Activate all tests in the **Database** view and click **OK**.
  - d. To start the check, select the **Consistency check | Run** menu item.

All the database tests must be successful. Correct the errors. Some consistency checks offer repair methods for correcting errors.
2. Update the administrative workstation on which the One Identity Manager History Database database schema update will start.
  - a. Execute the autorun.exe program from the root directory on the One Identity Manager installation medium.
  - b. Switch to the **Other products** tab and select the **One Identity Manager History Database** entry.
  - c. Click **Install**.

This starts the installation wizard.
  - d. Follow the installation instructions.

**IMPORTANT:** On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.
3. (From version 7.0.x or version 7.1.x) End the One Identity Manager Service on the server that processes direct database queries.

(From version 8.0.x or version 8.1.x). End the One Identity Manager Service on the update server.
4. Create a back up of the One Identity Manager History Database.
5. Check whether the database's compatibility level is set the **130** and change it if necessary.
6. Run a schema update of the One Identity Manager History Database.
  - Start the Configuration Wizard on the administrative workstation.

Select a user who has at least administrative permissions for the One Identity Manager database to update the One Identity Manager schema with the Configuration Wizard.

    - Use the same user that you used to initially install the schema.
    - If you created an administrative user during schema installation, use that one.

- If you selected a user with Windows authentication to install the schema, you must use the same one for updating.

**NOTE:** If you want to switch to the granular permissions concept when you upgrade from version 7.0.x, 7.1.x or 8.0.x to 8.1.2, you will also require an installation user in accordance with [Permissions for the One Identity Manager History Database on a SQL Server](#) on page 6.

After updating One Identity Manager, change the connection parameters. This affects the connection credentials for the database (DialogDatabase), for example, the One Identity Manager Service, the application server, administration, and configuration tools, web applications and web services, and the connection credentials in synchronization projects.

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

7. (From version 7.0.x or version 7.1.x) Update the One Identity Manager Service on the server that processes direct database queries.

(From version 8.0.x or version 8.1.x). Update the One Identity Manager Service on the update server.

- a. Execute the program autorun.exe from the root directory on the One Identity Manager installation medium.
- b. Change to the **Other products** tab and select the **One Identity Manager History Database** entry.
- c. Click **Install**.

This starts the installation wizard.

- d. Follow the installation instructions.

**IMPORTANT:** On the **Installation Settings** page, select the directory for your current installation as the installation directory. Otherwise the components are not updated and a new installation is created in the second directory instead.

8. Check the One Identity Manager Service's login information. Revert to the original settings if the One Identity Manager Service did not initially use the local system account for logging in. Specify the service account to use.
9. Start the One Identity Manager Service on the update server.



## 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	<p>Name of the database server where the One Identity Manager database is installed.</p> <p>The server name can be queried in the One Identity Manager database using the following statement:</p> <pre>select @@SERVERNAME</pre> <p>If the server can be reached through a specific port, enter the port as follows.</p> <p>Server name, port</p> <p><b>NOTE:</b> If you are providing a linked server, enter its name here. For more information, see <a href="#">Advanced configuration for transferring data</a> on page 15.</p>
Database	Name of the One Identity Manager database.
Database ID	<p>Database ID of the One Identity Manager database. This ID corresponds to the UID of the database entry in the One Identity Manager database.</p> <p><b>NOTE:</b> 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 <b>Database ID</b>.</p>
Use integrated Windows authentication	<p>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 <a href="#">Installing and updating a One Identity Manager History Database</a> on page 22.</p>
Database user	<p>SQL Server login user for data transfer.</p> <p>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 <a href="#">Advanced configuration for transferring data</a> on page 15.</p>
Password	<p>Password for the SQL Server login.</p> <p>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 <a href="#">Advanced configuration for transferring data</a> on page 15.</p>

<b>Property</b>	<b>Meaning</b>
Start and end of the recordings	These date specifications are automatically set and updated when the recordings are imported.

4. Save the changes.

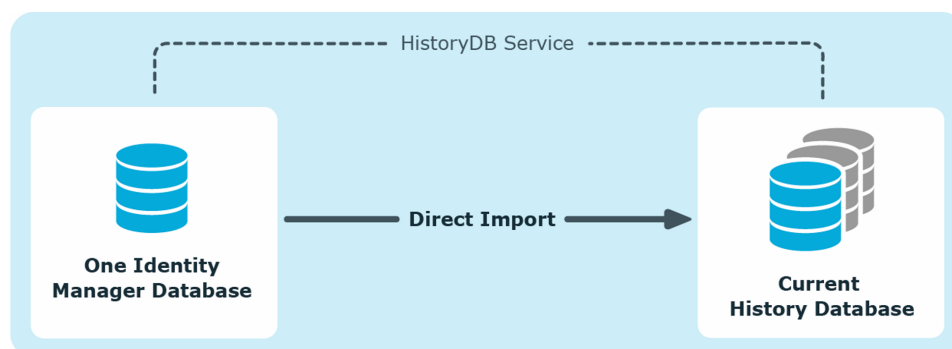
## Archiving procedure setup

All 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.

**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 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 planned operations.
- For the triggered action, there is at least one record in the section to be 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.
  - **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.

**Table 2: Configuration parameter for handling logged data**

<b>Configuration parameter</b>	<b>Meaning</b>
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.

**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.

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 planned operation.

You use configuration parameters to define the data retention periods for the individual sections.

**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:

<b>Time</b>	<b>Process Information</b>	<b>Process History</b>	<b>Data Changes</b>
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 section:

<b>Configuration</b>	<b>Process Information</b>	<b>Process History</b>	<b>Data Changes</b>
Export data	Yes	No	Yes
Retention period	3 days	4 days	5 days

This results in the following sequence:

<b>Time</b>	<b>Process Information</b>	<b>Process History</b>	<b>Data Changes</b>
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 sections.	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 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**.

## 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 the Designer.

## Related topics

- [Selecting an archiving procedure in the One Identity Manager database](#) on page 29
- [Declaring the database source in the One Identity Manager History Database](#) on page 25

# Direct deletion of records in the One Identity Manager database

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 DBQueue Processor database by One Identity Manager 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 29](#)

# 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	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 5: 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.
Common   ProcessState   ProgressView   Delete   TotalCount	This configuration parameter contains the total number of entries to be deleted in any processing run.

**Table 6: Configuration parameters for deleting process history**

<b>Configuration parameter</b>	<b>Meaning</b>
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 7: Configuration parameters for deleting process status entries**

<b>Configuration parameter</b>	<b>Meaning</b>
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.

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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## D

- data change
  - retention period 30

## O

### One Identity Manager History Database

- archiving method 28-29
- data archiving 4, 28-29
  - configure 32
- database user
  - Microsoft SQL Server 22
- install 5
- source database 25
- update 22

### One Identity Manager History Service

- configure 20
- installing 20

## P

- process history
  - retention period 30
- process information
  - archive 29
  - delete 32
  - export 32
  - import 32
  - retention period 30
- process monitoring
  - archive 28
  - retention period 30