

# HomeDirectory Maintenance

A tool for maintaining user home directories on OES.

## Introduction

If users are created in the OES environment using tools other than iManager or similar, it is often not possible to create a home directory. Even with iManager, the home directory is not renamed when the user is renamed (e.g., due to a name change through marriage). When the user is deleted, an orphaned directory remains, which means that over time, large amounts of potentially insecure data accumulate on the disks.

HomeDirectory Maintenance helps to circumvent these problems.

## Procedure

It is implemented as a single program called HDMaint.

HDMaint takes two separate approaches:

- **New creation**  
When new users are created, they need a home directory. To find new users efficiently, HDMaint uses LDAP to search the specified container (with subcontainers, if applicable) for user objects that have been created since the last run. It checks whether the attribute for the home directory is set. If it is not set, a new directory is created (if it does not already exist). If a directory with the user name already exists, it is used. HDMaint assigns the user the configured rights, sets the quota limit for the directory, and enters the directory in the user's home directory attribute. The user is also entered as the owner of the directory. Optionally, a predefined structure (skeleton) can be copied into the created directory. This new creation run is designed to use as few resources and computing power as possible, so that it can be executed frequently, e.g., every 5 minutes via cron.
- **Maintenance**  
During the maintenance run, all directories in the base directory for the home directories are checked, with the exception of those beginning with an underscore (\_). Here, orphaned directories and directories of renamed users are found. According to the specified actions, these are then renamed or deleted or moved to another directory for review. Once these actions have been performed, a corresponding message can be generated for the administrator.

## Requirements

HDMaint runs on OES24.4 and higher. The additional *libopenssl3* package must be installed. In principle, it can also be run on older versions; please inquire for more information. A newly compiled version may be necessary for OES 25.4 and higher (based on SLES15 SP7). This will be made available shortly after the release of the corresponding version.

HDMaint is cluster-aware. At startup, it checks whether the volume to be checked is mounted. If not, HDMaint terminates silently. This allows it to be installed on all cluster nodes on which the home directory volume could be mounted.

Since HDMaint uses APIs that are only accessible to the root user, it must be executed by the root user.

## Installation

To install, copy the HDMaint executable files to any directory on the server, e.g., /opt/HDMaint, and make them executable (chmod +x HDMaint).

If you have received an archive, please extract it into a directory as above; it should already contain an executable file named HDMaint.

## Configuration

Configuration is done via an .ini file. By default, this file is named HDMaint.ini. Other file names can also be specified using the -f or --infile parameter, e.g., for multiple configurations.

Paths in the configuration (HDBase, MoveTarget, Skeleton) are specified without a leading delimiter and with a slash ( / ).

Here is an example:

```
[LDAP]
LDAPHost=172.16.129.1
LDAPUser=cn=admin,o=bond
LDAPPass=XXXXXXX
LDAPCont=O=Test
LDAPScope=o

[Path]
VolObj=cn=James12_USER,ou=Server,O=bond
VolName=USER
HDBase=Test
OrphanAction=DELETE
MoveTarget=Test/_Delete.me
Skeleton=Test/_Skele.ton
SkelCopy=TRUE

[Dir]
FolderRights=rwcmf
DirQuota=10GB
AdjustQuota=TRUE

[Log]
LogLevel=1
LogDir=log
LogMax=10M

[RUN]
TickCount=10
Ticker=1
LastRun=20251118211737Z
```

The parameters in the ini file in detail:

Section	Name	Description
LDAP	LDAPHost	IP address or DNS name of the LDAP host, most easily the server itself.
LDAP	LDAPUser	User name in LDAP format, should have read and write access to the home directory attribute.
LDAP	LDAPPass	Password of the LDAP user. It is encrypted when HDMaint is started for the first time

LDAP	LDAPCont	LDAP context: Start context for searching for newly created users
LDAP	LDAPScope	Search scope: o means only the specified context, s also the subordinate contexts
Path	VolObj	Name of the volume object in LDAP format
Path	VolName	Volume name – Attention: case sensitive
Path	HDBase	If the user directories are not located directly in the main directory of the volume, a subdirectory can be specified here. Again, please note that the system distinguishes between upper- and lower-case letters
Path	OrphanAction	Determines how to handle "orphaned" directories. MOVE means move to the MoveTarget directory, DELETE means delete. If this option is empty or invalid, the directories remain.
Path	MoveTarget	The directory to which the orphaned directories are to be moved, relative to the volume (they can only be moved within the volume), without a leading slash. The name should start with an underscore (_), as directories with underscores are ignored during the check.
Path	Skeleton	If SkelCopy is TRUE, the subdirectories and files located in this directory are copied to the new HomeDirectory. The name should also begin with an underscore if it is located within the HDBase directory (or if HDBase is empty).
Path	SkelCopy	If True -> see above
Dir	FolderRights	The rights to be assigned to the user for the directory, in the form of a list of lowercase letters: r = read w=write c = create e = erase m=modify (meaning rename, etc.) f=file scan a= access control s=supervisor
Dir	DirQuota	The directory quota for the HomeDirectory in KB, MB or GB. Must be a multiple of 4K
Dir	AdjustQuota	Specifies whether an existing quota that is smaller than DirQuota should be adjusted. TRUE => Yes, FALSE = No
RUN	TickCount	Number of make runs after which a check run is performed
Log	LogLevel	Defines how detailed the output to the logfile is: 0: no Output 1: (default) Only Output for Changes: new users, renames or deletions 2: additionally: for each run a line telling what run was performed 3: complete, as with interactive
Log	LogDir	Directory for the logfile. If this has no leading slash (/) it is assumed relative to the program directory, otherwise absolute path. Default: log The name of the logfile is HDMaint.log
Log	LogMax	Maximum size of the logfile. If the logfile is bigger than this at the start of a run, it will be renamed by appending the current date and time and a new one will be started.
RUN	Ticker	Current counter for make runs. When this reaches the TickCount value, a check run is performed instead of a make run. The value is then reset to 1.
RUN	LastRun	The LDAP timestamp (YYYYMMDDThhmmssZ) of the last execution (minus 1 minute). Updated each time Check or Make is executed.

If HDMaint is called with the parameter -g, it creates an empty .ini file if one does not already exist.

## Command line options

HDMaint is primarily intended for execution via cron. For more information, see the Automation section.

### Interactive (-i)

Since HDMaint is normally executed via cron, no output is generated. This option enables the output of actions and errors.

After creating or changing the configuration, you should call HDMaint at least once via the command line with this option to check that it is running as desired.

### DryRun (-d)

Performs a dry run. Applies to the Make (-m) and Check (-c) options. Instead of making actual changes, only messages are output. Includes the Interactive [option](#).

### Version (-v)

This option outputs the version, the current tree name, context, the number of user objects, and the licensing information.

### ListDir (-l)

This option includes Interactive. It outputs two lists: The users (from LDAP) with their HomeDirectory attribute and the directories from the base directory with quotas, owners, and rights assignments

### Make (-m)

This is the option that should be executed via cron. Depending on the status of the ticker, it performs a Make or a Check run (see below).

The Make operation is deliberately designed to be economical in order to save resources, so that it can be executed frequently without any problems (e.g., every 5 minutes). Make uses LDAP to check for new user objects since the last execution (ini parameter LastRun). If new objects have been created, it creates the appropriate home directories and optionally copies the contents of the skeleton directory into them.

### Check (-c)

The check run is automatically executed every TickCount times instead of the make run. However, with this option, it can also be executed directly (for control purposes). The check performs two actions:

**For all LDAP users** (inside the configured container): Check whether a home directory has been assigned and whether it has the same name as the user. If there are any discrepancies, they are corrected. This means that renaming is recognized and applied to the directory.

**For all directories** (in the base directory): Check whether a user is assigned. If so, the rights and quota allocation are checked. If less storage space is allowed than the default, or if there is no restriction, the space restriction is assigned according to the default. If no rights exist, the rights are set according to the default. Furthermore, the owner assignment is checked and corrected if necessary. If no assigned user exists, the directory is either moved to the target directory for orphaned directories, deleted, or ignored.

### Prune (-p)

Deletes the directory specified as a parameter (absolute path) including all subdirectories and files. If attributes such as Deletelnhibit are set, they are reset beforehand.

### OrphanPrune (-o)

Deletes the contents of the directory specified as the target directory for orphaned home directories, also by resetting attributes that could prevent deletion.

### GenIni (-g)

Creates a template for the .ini file in the current directory.

## Automation

To execute HDMaint regularly you need to enter it in root's crontab:

```
# crontab -e
```

In the editor (vi or vim by default), start a new line with <Shift> A and enter the following:

```
*/5 * * * * /opt/HDMaint/HDMaint -m
```

If HDMaint is installed in a different folder, specify the corresponding folder.

Then exit the editor with <Esc> : wq.

## License

HDMaint already includes a free license for any tree name and 50 user objects. If your user container contains more than 50 users, you must purchase a license. This license refers to the tree name and, if applicable, the number of users. You can find out both with the -v option.

Once you have purchased a license, you will receive a license file named HDMaint.lic. This file must be located in the same directory as HDMaint. For organizational reasons, you may receive a license file that is not named HDMaint.lic. In this case, simply rename it.

After installing the license file, you should also use the -v option to check whether the license is recognized.

## Version History

### 1.0 (20.11.2025)

Initial Release

### 1.1 (23.11.2025)

Added Interface to NIT (Network Identity Translator), because some GUID from LDAP did not correspond to the GUIDs of NSS.

### 1.2 (26.11.2025)

Added Logging