One Identity Manager 9.1

Administration Guide for Connecting to HCL Domino

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 Administration Guide for Connecting to HCL Domino
Updated - 19 September 2022, 12:26

For the most recent documents and product information, see One Identity Manager documentation.

Contents

1

Managing HCL Domino environments

HCL Domino objects such as user accounts, groups, mail-in databases, servers, policies, and certificates can be administrated with One Identity Manager. By defining Notes domains in One Identity Manager, you are able to manage several productive Domino environments in parallel with a One Identity Manager database. In One Identity Manager, user and employee documents are managed as Notes user accounts. The Domino Directory's objects are mapped as Notes objects in One Identity Manager.

NOTE: One Identity Manager supports synchronization with different Domino versions, for example HCL Domino Server version 11 and IBM Domino Server version 10. Since managing objects in One Identity Manager is independent of whatever version the target system environment has, One Identity Manager references the target system uniformly as Domino.

One Identity Manager provides company employees with the necessary user accounts. You may use different mechanisms for connecting employees to their Notes user accounts. These user accounts can also be managed separately from employees and therefore administrative user accounts can be set up.

When you certify a new user, a series of user specific files are generated, which must be available to the user. When you add a user with the Domino connector, the user ID file for authentication, the mailbox file, and the user’s personal address book are created.

Groups and mail-in databases are managed by One Identity Manager along side user accounts. Groups are used to provide users the access permissions they need or they can be used for email distribution lists. Users can send or receive messages through shared mail-in databases. Users can access these mail-in databases when access permissions have been granted. If you add a mail-in database using One Identity Manager, the necessary mailbox file is created.

Server documents, certificates, policies, and templates for mailbox files are only loaded into the One Identity Manager database so they can be referenced when you set up user accounts and groups. One Identity Manager access lists can be defined for server documents in order to specify who has access to a server for what reason.

NOTE: The Domino module must be installed as a prerequisite for managing One Identity Manager in Domino Module For more information about installing, see the *One Identity Manager Installation Guide*.

Architecture overview

In One Identity Manager, the image of part of an operational Domino system is mapped to a Notes domain. To synchronize, One Identity Manager must have to access to the Domino Directory in this Domino environment in order.

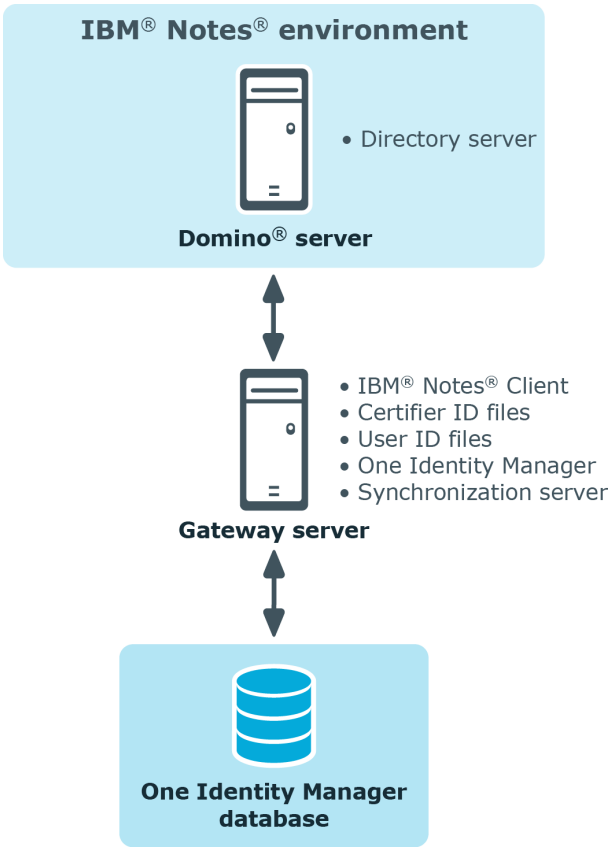
A server is defined within the One Identity Manager environment to run all the administrative tasks effecting the Domino environment. This server is named the gateway server in the rest of this chapter. The gateway server performs the function of the synchronization server. It is not a productive Domino server. A Notes client, the One Identity Manager Service, and the Domino connector are installed on the gateway server.

All Domino connector actions are run from the gateway server. The gateway server communicates with the productive environment's Domino server when actions are running in the target system. This Domino server is specially selected with a good network connection to the gateway server. The Domino connection requires access to the Domino Directory, therefore, you should preferably use a directory server.

For synchronization, provide an ID file with sufficient administrative permissions for accessing the productive Domino environment. If you want to work with a Certification Authority process (CA process), a certifier ID file must be provided. Both files must be available on the gateway server.

The gateway server runs One Identity Manager Service actions, like certifications, adding, modifying, and deleting document in the Domino Directory. In addition to this, databases can be also added to servers for users, mailbox files or mail-in databases on Domino servers. The One Identity Manager Service provides a Notes client context using the Notes COM library and processes all necessary functions for exchanging data with the Domino server in it (access to Domino objects, running Notes agents, creating administrative processes (AdminP), error handling).

Figure 1: Domino Connectors communication with Domino



The objects in Domino are mapped as follows in the One Identity Manager database:

Table 1: Mapping object types from this Domino installation in the One Identity Manager

Domino	One Identity Manager
Domino server	Notes server
Domino domain	No direct mapping
	Notes domain Properties of Notes objects to assign them to different Domino environments.
User	Notes user account
Group	Notes group
Mail-in DB	Notes mail-in database
Notes certi-ficate	Notes certificate

Domino	One Identity Manager
Template	Notes template
Policy	Notes policy

One Identity Manager users for managing Domino

The following users are used for setting up and administration of Domino.

Table 2: Users

Users	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other employees to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Domino** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have another identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor

Users	Tasks
	and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. One Identity Manager administrators: • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: • Assign groups to IT Shop structures.
Administrators for organizations	Administrators must be assigned to the **Identity Management | Organizations | Administrators** application role. Users with this application role: • Assign groups to departments, cost centers, and locations.
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role. Users with this application role: • Assign groups to business roles.

Configuration parameters for managing Domino environments

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

For more information, see Configuration parameters for managing a Domino environment on page 229.

2

Synchronizing a Domino environment

One Identity Manager supports synchronization with Domino in the following versions:

- IBM Domino Server versions 8, 9, and 10
- HCL Domino Server versions 11 and 12
- IBM Notes Client version 8.5.3 or 10.0
- HCL Notes Client versions 11.0.1 and 12.0

  The 64-bit variant of Notes Client 12.0.1 is currently not supported.

NOTE: Since managing objects in One Identity Manager is independent of whatever version the target system environment has, One Identity Manager references the target system uniformly as Domino.

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and Domino.

This sections explains how to:

- Set up synchronization to import initial data from Domino domains in to the One Identity Manager database.
- Adjust a synchronization configuration, for example, to synchronize different Notes domains with the same synchronization project.
- Start and deactivate the synchronization.
- Evaluate the synchronization results.

TIP: Before you set up synchronization with a Domino domain, familiarize yourself with the Synchronization Editor. For more information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Setting up initial synchronization of a Domino environment on page 17
- Adjusting the synchronization configuration for Domino environments on page 33

- Running synchronization on page 46
- Troubleshooting on page 53

Setting up initial synchronization of a Domino environment

The Synchronization Editor provides a project template that can be used to set up the synchronization of Notes user accounts and groups. You use these project templates to create synchronization projects with which you import the data from Domino into your One Identity Manager database. In addition, the required processes are created that are used for the provisioning of changes to target system objects from the One Identity Manager database into the target system.

To load Domino objects into the One Identity Manager database for the first time

1. In HCL Domino, prepare a user with sufficient permissions for synchronization.
2. One Identity Manager components for managing Domino environments are available if the **TargetSystem | NDO** configuration parameter is set.
    - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

      NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure the gateway server.
4. Create a synchronization project with the Synchronization Editor.
5. If user accounts in Domino are to be registered by the Domino connector, modify the required certificates in One Identity Manager. Enter the path for the certifier's ID file or the name of the CA database.

Detailed information about this topic

- Users and permissions for synchronizing with Domino on page 18
- System requirements for the gateway server on page 20
- Creating a synchronization project for initial synchronization of a Notes domain on page 26
- General main data for Notes certificates on page 172

- Default project template for Domino on page 232
- Configuration parameters for managing a Domino environment on page 229

Users and permissions for synchronizing with Domino

The following users are involved in synchronizing One Identity Manager with HCL Domino.

Table 3: Users for synchronization

User	Permissions
One Identity Manager Service user account	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires permissions for the internal web service. NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the target system (synchronization user)	The user who accesses the system required sufficient administrative permissions to the Domino Directory (`names.nsf`). The minimum requirements are: • **Editor** access function on the primary Domino directory • Permissions for deleting documents • **UserCreator** in addition to the default permissions • Remote console access

User	Permissions
	• Administrative access to a Domino server (server on which new user can be registered and AdminP tasks created) **Editor** is also required for the following databases: • certlog.nsf • admin4.nsf (Optional) If you want mailbox files to be created when Notes users register, the following permissions are required for the Domino connector to have read access to the new mailbox files. • Permissions for the synchronization user to transfer the template on the Domino server (`*.ntf`) that is used to create the mailbox files
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to run synchronization using an application server.

Related topics

- Creating mailbox files on page 43

Domino server configuration

Configure the following settings on the Domino server that the gateway server communicates with:

- Set up a full-text index for the Domino Directory.
- In the `Notes.ini` file, set `FT_MAX_SEARCH_RESULTS=2147483000`.

  If you apply filters in the Domino Directory, a maximum of 5,000 filtered values are returned. To obtain a complete result list of the elements that satisfy the filter condition, you must overwrite this value in the Domino server's `Notes.ini` file with the value given here.

For more information, see your Domino documentation.

Setting up a gateway server

The gateway server performs the function of the synchronization server. All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with

the One Identity Manager database are processed by the synchronization server. The synchronization server must be One Identity Managerdeclared as a Job server in .

To set up a gateway server

1. Configure the Notes client.
2. Install the One Identity Manager Service with Domino connector and declare the gateway server as Job server in the One Identity Manager database.
3. (Optional) You can add an archive database for backing up ID files in order to restore user ID files using the ID restore method.

Detailed information about this topic

- System requirements for the gateway server on page 20
- Configuring the Notes client on page 21
- Installing the One Identity Manager Service on the gateway server on page 23
- Setting up an archive database for backing up employee documents on page 26

System requirements for the gateway server

To set up a gateway server, a server has to be available with the following software installed:

- Windows operating system

  The following versions are supported:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework version 4.8 or later

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Installer
- IBM Notes Client version 8.5.3 or 10.0 or HCL Notes Client version 11.0.1 or 12.0

  NOTE:

  - Run the installation in single-user mode.
  - You must run a proper installation. Domino COM class libraries are registered during installation. This requires the Domino connector.

- Write access to the Notes client install directory and the One Identity Manager install directory.
- One Identity Manager Service, Domino connector
    - Install One Identity Manager components with the installation wizard.
        1. Select **Select installation modules with existing database**.
        2. Select the **Server | Job Server | Domino** machine role.

Special requirements for synchronizing an IBM Domino 8.5. or 9 environment

The following versions of the Domino and Notes components are the minimum requirements for synchronizing a Domino 8.5 or 9 environment.

- Domino Server version 8.5.1 with Fix Pack 2 or later or version 9.0.1.
- Notes client in version 8.5.3, Fix Pack 4 or Notes client version 10.0

Notes for synchronizing HCL Domino 12

If the connected Domino system uses Domino 12 and the Domino connector has write access to the target system, then the gateway server must have Notes client version 12 installed. The 64-bit variant of Notes Client 12.0.1 is currently not supported.

If read-only access to the target system is required, an older Notes client version can also be used on the gateway server.

Configuring the Notes client

To configure the Notes client

1. Extend the PATH variable to include the default search path (installation directory) and the data directory (`<Installation directory>\data`).
    - Enter the Notes installation path in the operating systems default search path (PATH variable). This is the path to find the `Notes.exe`.
    - Also add the path selected for the Notes data directory during the Notes client's installation to the PATH variables.
2. Specify the directory for the ID files repository (`<Installation directory>\data\IDS\<Name of the domain>`).
3. Ensure the synchronization user's user ID file is available.

    A separate ID file must be provided for this user. The path to this ID file is entered later into the custom INI file. User ID files with multiple passwords are not supported.

    NOTE: The administrator ID file that is created when the Notes server is installed may not be used because it is used for other administrative tasks.
4. Keep the certifier ID file available for certificate administration.

Set up all certifier ID files for registering users on the gateway server. Certifier ID files with multiple passwords are not supported.

5. Start the Notes client with the synchronization user's ID file and log in.

   This causes the configuration entries to be made on the computer. The access permissions can be checked by calculating a new user with the ID file as a test.
6. Copy the Domino Directory certificate documents into the user account's personal address book for synchronization.
7. Check whether the certification log `certlog.nsf` exists.
8. Create a custom INI file.

   The path of the synchronization user's ID file must be entered in this INI file.

NOTE:

- If you did not install the Notes client in the default install directory, modify the default search path and data directory in the PATH variables as well as the path entries in `Notes.ini` and your custom INI file to your install directory path.
- If you are using Notes client version 10.0, change the path to `Notes.ini`. Depending on the installation, this file can be saved in the user profile directory.

Detailed information about this topic

- Copying Notes certificates on page 22
- Creating custom INI files on page 22

Copying Notes certificates

When you are configuring the gateway server ensure that the certification documents are copied from the Domino Directory into the synchronization user's personal address book. This is necessary to enable the Domino connector to add, rename, or move user accounts in the target system.

TIP: Copy new certificates regularly from the Domino Directory into the synchronization user's personal address book. For more information about copying certificate documents, see your Domino documentation.

Creating custom INI files

When you configure the Notes client, a `Notes.ini` file is created. This file contains configuration information that the Domino connector needs to access the target system. Create a copy of this INI file and make it available to the Domino connector as a custom INI file. The custom INI file must contain the path to the synchronization user's ID file. Enter this INI file and the user ID file's password when you configure the system connection with the Synchronization Editor.

To add a custom INI file

1. Create a copy of the file `Notes.ini`. Use the synchronization user's ID file for this.
2. Check the following values in the copy.

Table 4: Parameters required in the custom INI file

Parameters	Description
Directory	Path to Notes data directory (local directory)
KeyFileName	Path to the ID file of the synchronization user (local directory).
KitType	Notes type: 1 = Client, 2 = Server.

Installing the One Identity Manager Service on the gateway server

The One Identity Manager Service must be installed on the gateway server with the Domino connector. The gateway server must be declared as a Job server in One Identity Manager.

Table 5: Properties of the Job server

Property	Value
Server function	Domino connector
Machine role	Server | Job Server | Domino

NOTE: If several target system environments of the same type are synchronized under the same synchronization server, it is recommended that you set up a Job server for each target system for performance reasons. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

Use the One Identity Manager Service to install the Server Installer. The program runs the following steps:

- Sets up a Job server.
- Specifies machine roles and server function for the Job server.
- Remotely installs One Identity Manager Service components corresponding to the machine roles.
- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: The program performs a remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

To remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed. For more information about installing a workstation, see the *One Identity Manager Installation Guide*.

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For more information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

To remotely install and configure One Identity Manager Service on a server

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.
3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.
    a. Select a Job server from the **Server** menu.

        - OR -

        To create a new Job server, click **Add**.

    b. Enter the following data for the Job server.
        - **Server**: Name of the Job server.
        - **Queue**: Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
        - **Full server name**: Full server name in accordance with DNS syntax.

          Syntax:

          `<Name of servers>.<Fully qualified domain name>`

    NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with the Designer.
4. On the **Machine roles** page, select **Domino**.
5. On the **Server functions** page, select **Domino connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

    NOTE: The initial service configuration is predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more information about configuring the service, see the *One Identity Manager Configuration Guide*.

- For a direct connection to the database:
    1. Select **Process collection > sqlprovider**.
    2. Click the **Connection parameter** entry, then click the **Edit** button.
    3. Enter the connection data for the One Identity Manager database.
- For a connection to the application server:
    1. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
    2. Click the **Connection parameter** entry, then click the **Edit** button.
    3. Enter the connection data for the application server.
    4. Click the **Authentication data** entry and click the **Edit** button.
    5. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. If the database is encrypted, on the **Select private key file** page, select the file with the private key.
11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Enter the name or IP address of the server that the service is installed and started on.
    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.
12. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.
13. Click **Finish** on the last page of the Server Installer.

    NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Setting up an archive database for backing up employee documents

You can add an archive database for backing up ID files in order to restore user ID files using the ID restore method. When you add a new user account in the One Identity Manager, a copy of the initial employee document is copied to an archive database on the gateway server. This archive database must initially added and should be part of a daily back up.

INFORMATION: The archive database is only required if the **ID vault enabled** option is disabled for the domain and if user ID files are supposed to be restored by One Identity Manager. For more information, see Restoring user ID files through ID restore on page 149.

The fastest method of adding an archive database is to create an empty copy of the local address book on the gateway server.

Table 6: Data required for the copy

Property	Value
Server	Local
Title	Any name
File Name	`Archive.nsf`
Database design only	Enabled

By default, the copy of the local address is encrypted for the current user. Therefore, the copy of the synchronization user's local address book must be encrypted in order for the Domino connector to access the archive database.

For more information about adding the address book copy, see your Domino documentation.

Creating a synchronization project for initial synchronization of a Notes domain

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Domino environment. The following describes the steps for initial configuration of a synchronization project. For more information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

After the initial configuration, you can customize and configure workflows within the synchronization project. Use the workflow wizard in the Synchronization Editor for this. The Synchronization Editor also provides different configuration options for a synchronization project.

Information required to set up Notes synchronization projects

Have the following information available for setting up a synchronization project.

Table 7: Information required for setting up a synchronization project

Data	Explanation
Domino server	Name of the Domino server which communicates with the gateway server.
Domino directory	Name of the Domino directory (`Names.nsf`).
Custom INI file	Name and path of the custom INI file. For more information, see Creating custom INI files on page 22.
ID file password	Synchronization user's ID file password. The path of this ID file must be given in the custom INI file. The Domino connector access the target system through the synchronization user. Make a user account available with sufficient permissions. For more information, see Users and permissions for synchronizing with Domino on page 18.
Synchronization server for the Notes domain	All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The gateway server performs the function of the synchronization server. The One Identity Manager Service with the Domino connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.

Table 8: Additional properties for the Job server

Property	Value
Server function	Domino connector
Machine role	Server/Job server/Domino

Data	Explanation
	For more information, see Installing the One Identity Manager Service on the gateway server on page 23.
One Identity Manager database connection data	• Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If the Synchronization Editor cannot be started directly on the gateway server, you can set up a remote connection. ***To use a remote connection*** 1. Provide a workstation on which the Synchronization Editor is installed. 2. Install the **RemoteConnectPlugin** on the gateway server. Thus the gateway server simultaneously assumes the function of the remote connection server. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed • Domino connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

Creating an initial synchronization project for Notes domains

NOTE: The following sequence describes how to configure a synchronization project if the Synchronization Editor is both:

- Run in default mode
- Started from the Launchpad

If you run the project wizard in expert mode or directly from the Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.

NOTE: Just one synchronization project can be created per target system and default project template used.

To set up an initial synchronization project for a Notes domain

1. Start the Launchpad on the gateway server and log in to the One Identity Manager database.

   NOTE: If synchronization is run by an application server, connect the database through the application server.

2. Select the **Target system type Domino** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. On the **System access** page, specify how One Identity Manager can access the target system.
   - If you started the Launchpad on the gateway server, do not change any settings.
   - If you started the Launchpad on the gateway server, do not change any settings.

     Enable the **Connect using remote connection server** option and, under **Job server**, select the gateway server to use for the connection.

4. On the **Configuration data for the Domino directory** page, enter the connection parameters required by the Domino connector to log in on the target system.

   Table 9: Connection data for Domino servers

Property	Description
INI file	Name and path of the custom INI file.
Domino server	Name of the Domino server which communicates with the gateway server.

Property	Description
Domino directory	Name of the Domino directory (`Names.nsf`).
ID file password	Synchronization user's ID file password. The path of this ID file must be given in the custom INI file.

5. You can test the connection on the **Verify connection settings** page. Click on **Verify project**.

   One Identity Manager tries to connect to the target system.

6. You can configure additional settings on the **Configuration settings** page.
   - To delete Notes objects using AdminP processes, enable **Delete objects using AdminP processes**. If the option is disabled, the objects are deleted directly in the system by the Domino connector.
   - Click **Finish**, to end the system connection wizard and return to the project wizard.

7. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE:
   - If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again.
   - This page is not shown if a synchronization project already exists.

8. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.

9. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 10: Specify target system access

Option	Meaning
	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**. • Processing methods in the synchronization steps are only defined for synchronization in the direction

Option	Meaning
	of **One Identity Manager**.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the **Target system**. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the **Target system**. • Synchronization steps are only created for such schema classes whose schema types have write access.

10. On the **Synchronization server** page, select the synchronization server to run the synchronization.

    If the synchronization server is not declared as a Job server in the One Identity Manager database yet, you can add a new Job server.

    a. Click to add a new Job server.

    b. Enter a name for the Job server and the full server name conforming to DNS syntax.

    c. Click **OK**.

    The synchronization server is declared as Job server for the target system in the One Identity Manager database.

    d. NOTE: After you save the synchronization project, ensure that this server is set up as a synchronization server.

11. To close the project wizard, click **Finish**.

    This creates and allocates a default schedule for regular synchronization. Enable the schedule for regular synchronization.

    This sets up, saves and immediately activates the synchronization project.

    NOTE:

    - If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.

      Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.

- If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically option**. In this case, save the synchronization project manually before closing the Synchronization Editor.
- The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

Related topics

- Configuring the synchronization log on page 32
- Adjusting the synchronization configuration for Domino environments on page 33
- Default project template for Domino on page 232

Configuring the synchronization log

All the information, tips, warnings, and errors that occur during synchronization are recorded in the synchronization log. You can configure the type of information to record separately for each system connection.

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the **Configuration > Target system** category in the Synchronization Editor.

   - OR -

   To configure the synchronization log for the database connection, select the **Configuration > One Identity Manager connection** category in the Synchronization Editor.
2. Select the **General** view and click **Configure**.
3. Select the **Synchronization log** view and set **Create synchronization log**.
4. Enable the data to be logged.

   NOTE: Some content generates a particularly large volume of log data. The synchronization log should only contain data required for error analysis and other analyzes.
5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In the Designer, enable the **DPR | Journal | LifeTime** configuration parameter and enter the maximum retention period.

Related topics

- Displaying synchronization results on page 47

Adjusting the synchronization configuration for Domino environments

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a Notes domain, you can use the synchronization project to load Notes objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Domino environment.

You must customize the synchronization configuration to be able to regularly compare the database with the Domino environment and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- To specify which Notes objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.
- Use variables to set up a synchronization project for synchronizing different domains. Store a connection parameter as a variable for logging in to the domain.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

For more information about configuring synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- How to configure Domino synchronization on page 34
- Configuring synchronization of several Notes domains on page 34
- Updating schemas on page 37
- Changing system connection settings of Notes domains on page 35

How to configure Domino synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the primary system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing Domino

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This creates a workflow with **Target system** as its direction of synchronization.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related topics

- Configuring synchronization of several Notes domains on page 34

Configuring synchronization of several Notes domains

Prerequisites

- The target system schema of both domains are identical.
- All virtual schema properties used in the mapping must exist in the extended schema of both domains.
- The connection parameters to the target system are defined as variables.

To customize a synchronization project for synchronizing another domain

1. Set up a synchronization user with sufficient permissions in the other domain.
2. In the Synchronization Editor, open the synchronization project.
3. Create a new base object for every other domain.
   - Use the wizard to attach a base object.
   - In the wizard, select the Domino connector.

- Declare the connection parameters. The connection parameters are saved in a special variable set.

A start up configuration is created that uses the newly created variable set.

4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related topics

- How to configure Domino synchronization on page 34

Changing system connection settings of Notes domains

When you set up synchronization for the first time, the system connection properties are set to default values that you can modify. There are two ways to do this:

a. Specify a specialized variable set and change the values of the affected variables.

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).

b. Edit the target system connection with the system connection wizard and change the effected values.

   The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- Editing connection parameters in the variable set on page 35
- Editing target system connection properties on page 36

Editing connection parameters in the variable set

The connection parameters were saved as variables in the default variable set when synchronization was set up. You can change the values in these variables to suit you requirements and assign the variable set to a start up configuration and a base object. This means that you always have the option to use default values from the default variable set.

NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project is used for synchronizing different Notes domains.

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.

   Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.

   All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on in the variable set view's toolbar.
   - To rename the variable set, select the variable set and click the variable set view in the toolbar. Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration > Base objects** category.
13. Select the base object and click .

    - OR -

    To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

For more information about using variables and variable sets, or restoring default values and adding base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Editing target system connection properties on page 36

Editing target system connection properties

You can also use the system connection wizard to change the connection parameters. If variables are defined for the settings, the changes are transferred to the active variable set.

NOTE: In the following circumstances, the default values cannot be restored:

- The connection parameters are not defined as variables.
- The default variable set is selected as an active variable set.

In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit connection parameters using the system connection wizard

1. In the Synchronization Editor, open the synchronization project.
2. In the toolbar, select the active variable set to be used for the connection to the target system.

   NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.

   This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- Editing connection parameters in the variable set on page 35

Updating schemas

All the schema data (schema types and schema properties) of the target system schema and the One Identity Manager schema are available when you are editing a synchronization project. Only a part of this data is really needed for configuring synchronization. If a synchronization project is finished, the schema is compressed to remove unnecessary data from the synchronization project. This can speed up the loading of the synchronization project. Deleted schema data can be added to the synchronization configuration again at a later point.

If the target system schema or the One Identity Manager schema has changed, these changes must also be added to the synchronization configuration. Then the changes can be added to the schema property mapping.

To include schema data that have been deleted through compression and schema modifications in the synchronization project, update each schema in the synchronization project. This may be necessary if:

- A schema was changed by:
  - Changes to a target system schema
  - Customizations to the One Identity Manager schema

        - A One Identity Manager update migration
    - A schema in the synchronization project was shrunk by:
        - Enabling the synchronization project
        - Saving the synchronization project for the first time
        - Compressing a schema

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.

   - OR -

   Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.

   Opens the Mapping Editor. For more information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

NOTE: The synchronization is deactivated if the schema of an activated synchronization project is updated. Reactivate the synchronization project to synchronize.

Speeding up synchronization with revision filtering

When you start synchronization, all synchronization objects are loaded. Some of these objects have not be modified since the last synchronization and, therefore, must not be processed. Synchronization is accelerated by only loading those object pairs that have changed since the last synchronization. One Identity Manager uses revision filtering to accelerate synchronization.

Domino supports revision filtering. The Notes document's last change date is used as revision counter. Each synchronization saves the last date is was run as a revision in the One Identity Manager database (`DPRRevisionStore` table, `Value` column). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is synchronized the next time, the Notes objects' change date is compared with the revision saved in the One Identity Manager database. Only those objects that have been changed since this date are loaded from the target system.

The revision is found at start of synchronization. Objects modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

Revision filtering can be applied to workflows and start up configuration.

To permit revision filtering on a workflow

- In the Synchronization Editor, open the synchronization project.
- Edit the workflow properties. Select the **Use revision filter** item from **Revision filtering** menu.

To permit revision filtering for a start up configuration

- In the Synchronization Editor, open the synchronization project.
- Edit the start up configuration properties. Select the **Use revision filter** item from the **Revision filtering** menu.

NOTE: The Domino connector can only load date information from Notes documents if a full text search for the Domino Directory is configured on the Domino server.

For more information about revision filtering, see the *One Identity Manager Target System Synchronization Reference Guide*.

Configuring the provisioning of memberships

Memberships, such as user accounts in groups, are saved in assignment tables in the One Identity Manager database. During provisioning of modified memberships, changes made in the target system may be overwritten. This behavior can occur under the following conditions:

- Memberships are saved as an object property in list form in the target system.

  Example: List of user accounts in the `Member` property of a Notes group (`Group`)
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and previously deleted memberships are added again.

To prevent this, provisioning can be configured such that only the modified membership is provisioned in the target system. The corresponding behavior is configured separately for each assignment table.

To allow separate provisioning of memberships

1. In the Manager, select the **HCL Domino > Basic configuration data > Target system types** category.
2. In the result list, select the **Domino** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.

   NOTE:

   - This option can only be enabled for assignment tables that have a base table with a `XDateSubItem` column.
   - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.

     Example: `NDOGroupInGroup`, `NDOMailInDBInGroup`, `NDOServerInGroup`, and `NDOUSerInGroup`
6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. Therefore, only newly added and deleted assignments are processed. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and not the entire members list.

NOTE: The complete members list is updated by synchronization. During this process, objects with changes but incomplete provisioning are not handled. These objects are logged in the synchronization log.

You can restrict single provisioning of memberships with a condition. Once merge mode has been disabled for a table, the condition is deleted. Tables that have had the condition deleted or edited are marked with the following icon:  . You can restore the original condition at any time.

To restore the original condition

1. Select the auxiliary table for which you want to restore the condition.
2. Right-click on the selected row and select the **Restore original values** context menu item.
3. Save the changes.

NOTE: To create the reference to the added or deleted assignments in the condition, use the `i` table alias.

Example of a condition on the `NDOUserInGroup` assignment table:

```
exists (select top 1 1 from NDOGroup g
     where g.UID_NDOGroup = i.UID_NDOGroup
     and <limiting condition>)
```

For more information about provisioning memberships, see the *One Identity Manager Target System Synchronization Reference Guide*.

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

- A synchronization step exists that can import the changes to the changed object into One Identity Manager.
- The path to the base object of the synchronization is defined for the table that contains the changed object.

Single object synchronization is fully configured for synchronization projects created using the default project template. If you want to incorporate custom tables into this type of synchronization project, you must configure single object synchronization for these tables. For more information about this, see the *One Identity Manager Target System Synchronization Reference Guide*.

To define the path to the base object for synchronization for a custom table

1. In the Manager, select the **HCL Domino > Basic configuration data > Target system types** category.
2. In the result list, select the **Domino** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

   Example: `FK(UID_NDODomain).XObjectKey`
8. Save the changes.

Related topics

- Synchronizing single objects on page 49
- Post-processing outstanding objects on page 50

Accelerating single object synchronization

To smooth out spikes in data traffic, handling of processes for single object synchronization can be distributed over several Job servers. This accelerates single object synchronization.

Load balancing is not used for provisioning processes in Domino, to prevent inconsistent data being generated in the target system through parallel processing. If the maximum number of instances on the process task or process component is set to **1** or **-1**, load balancing cannot take place.

NOTE: You should not implement load balancing for single object synchronization on a permanent basis. Parallel processing of object might result in dependencies not being resolved because referenced objects from another Job server have not been completely processed.

Once load balancing is no longer required, ensure that the synchronization server runs the processes for single object synchronization.

To configure load balancing

1. Configure the servers and declare them as Job servers in One Identity Manager.
   - Job servers that share processing must have the **No process assignment** option enabled.
   - Assign the **Domino connector** server function to the Job server.

   All Job servers must access the same Notes domain as the synchronization server for the respective base object.
2. In the Synchronization Editor, assign a custom server function to the base object.

   This server function is used to identify all the Job servers being used for load balancing.

   If there is no custom server function for the base object, create a new one.

   For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.
3. In the Manager, assign this server function to all the Job servers that will be processing single object synchronization for the base object.

   Only select those Job servers that have the same configuration as the base object's synchronization server.

Once all the processes have been handled, the synchronization server takes over single object synchronization again.

To use the synchronization server without load balancing.

- In the Synchronization Editor, remove the server function from the base object.

For more information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Job server for Domino-specific process handling on page 221

Specify user types

New users are registered in Domino by default as **Full Client User**. The user type for registering is specified by the synchronization variable **UserType**. Possible values:

- **174**: LIMITED CLIENT USER
- **175**: DESKTOP CLIENT USER
- **176**: FULL CLIENT USER

To modify the default user type

- In the synchronization project, edit the **UserType** variable and enter your value.

  To edit a variable

  1. In the Synchronization Editor, open the synchronization project.
  2. Select the **Configuration > Variables** category.
  3. Select the variable and edit its value.
  4. Save the changes.

For more information about variables and variable sets, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Editing connection parameters in the variable set on page 35

Creating mailbox files

If and in what way mailbox files are created in Domino depends on the user account data and the configuration parameter settings.

Prerequisites

- The mailbox's path and file name are given in the user account.

  If this information is missing, the mailbox file cannot be created.
- The directory where the mailbox files are stored on the mail server is given in the **TargetSystem | NDO | MailFilePath** configuration parameter.

Configuring access levels

By default, the access level **Manager** is set for the mailbox file's owner.

To set another access level

- In the Designer, set the **TargetSystem | NDO | Accounts | MailFileAccessRole** configuration parameter and select an access level as the value that is given to all new mailbox files. Possible values are **Manager**, **Editor**, **Designer**.

Creating a mailbox file

By default, the mailbox file is created after the Notes user has registered with the target system. This uses a template given in the user account. If there is no template given in the mailbox file, the template in the **TargetSystem | NDO | DefTemplatePath** configuration parameter is used. The template must exist on the gateway server.

The mailbox file can also be created when the Notes user registers. In this case, the template of the Notes server's on which the user is registered is used.

To create a mailbox file during registration

- Edit the **UserCreateMailDb** variable in the synchronization project. Enter the value **1**.

  To edit a variable

  1. In the Synchronization Editor, open the synchronization project.
  2. Select the **Configuration > Variables** category.
  3. Select the variable and edit its value.
  4. Save the changes.

NOTE: The One Identity Manager Service does not access to mailboxes created like this. Different actions, for example, loading mailbox sizes, are therefore not possible.

Ensure that the template of the mailbox file on the Domino server has permissions set to transfer to the synchronization user so that the Domino connector has read access to the new mailbox files.

Related topics

- Notes user account email system on page 134
- Additional main data of Notes user accounts on page 136

- Editing connection parameters in the variable set on page 35

Creating and saving user ID files

When you add a user in the target system, a user ID file is created for authenticating the user. The Domino connector requires information about the minimum password length, the password strength, and the ID file's repository. When ID files are created, the settings in the following synchronization variables are taken into account.

Table 11: Settings for new user ID files

Variable	Description
UserIsNorthAmerican	Specifies whether the newly created ID files are compatible with the American (US) and Canadian Domino version. Value **1**: All new user ID files are calculated with North American encryption strength. Default: **0**
UserMinPwdLen	Specifies the minimum password length that is set in all newly calculated user ID files. Default: **0**
UserStoreIDInAddressbook	Specifies whether the ID file is attached to the employee document or saved on the gateway server. Default: **0** - The ID file is attached to the employee document.

To edit a variable

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Variables** category.
3. Select the variable and edit its value.
4. Save the changes.

For more information about variables and variable sets, see the *One Identity Manager Target System Synchronization Reference Guide*.

To save the user ID files on the gateway server

1. In the synchronization project, edit the **UserStoreIDInAddressbook** variable. Enter the value **1**.
2. Edit the domain's main data in the Manager and enter the **user ID files path**. Enter the path under which you want the files to be saved.

If a default path is not given by the domain, you can add the path to the user accounts' mail servers. If there is no path given either by the domain or the mail server, use the default Domino connector path, which is stored with the variable **UserIDFilesDefaultPath** in the synchronization project.

Detailed information about this topic

- General main data for Notes domains on page 126
- General main data for Notes servers on page 189
- Notes user account email system on page 134
- Editing connection parameters in the variable set on page 35

Running synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Starting synchronization on page 46
- Deactivating synchronization on page 48
- Displaying synchronization results on page 47
- Pausing handling of target system specific processes (Offline mode) on page 54

Starting synchronization

When you set up the initial synchronization project using the Launchpad, a default schedule for regular synchronization is created and assigned. Activate this schedule to synchronize on a regular basis.

To synchronize on a regular basis

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Edit schedule**.
4. Edit the schedule properties.
5. To enable the schedule, click **Activate**.
6. Click **OK**.

You can also start synchronization manually if there is no active schedule.

To start initial synchronization manually

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

IMPORTANT: As long as a synchronization process is running, you must not start another synchronization process for the same target system. This especially applies, if the same synchronization objects would be processed.

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
    - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
    - Use the schedule to ensure that the start up configurations are run in sequence.
    - Group start up configurations with the same start up behavior.

Displaying synchronization results

Synchronization results are summarized in the synchronization log. You can specify the extent of the synchronization log for each system connection individually. One Identity Manager provides several reports in which the synchronization results are organized under different criteria.

To display a synchronization log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ▶ in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking it.

   An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ↯ in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking it.

   An analysis of the provisioning is shown as a report. You can save the report.

The log is marked in color in the navigation view. This mark shows you the status of the synchronization/provisioning.

TIP: The logs are also displayed in the Manager under the **<target system> > synchronization log** category.

Related topics

- Configuring the synchronization log on page 32
-

Deactivating synchronization

Regular synchronization cannot be started until the synchronization project and the schedule are active.

To prevent regular synchronization

1. In the Synchronization Editor, open the synchronization project.
2. Select the start up configuration and deactivate the configured schedule.

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited extend. The schema in the synchronization project must be updated if schema modifications are required. The synchronization project is deactivated in this case and can be edited again.

Furthermore, the synchronization project must be deactivated if synchronization should not be started by any means (not even manually).

To deactivate the synchronization project

1. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Related topics

- Pausing handling of target system specific processes (Offline mode) on page 54

Synchronizing single objects

Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated.

NOTE: If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

To synchronize a single object

1. In the Manager, select the **HCL Domino** category.
2. Select the object type in the navigation view.
3. In the result list, select the object that you want to synchronize.
4. Select the **Synchronize this object** task.

   A process for reading this object is entered in the job queue.

Features of synchronizing memberships

If you synchronize changes in an object's member list, run single object synchronization on the assignment's root object, The base table of an assignment contains an `XDateSubItem` column containing information about the last change to the memberships.

Example:

Base object for assigning user accounts to groups is the group.

In the target system, a user account was assigned to a group. To synchronize this assignment, in the Manager, select the group that the user account was assigned to and run single object synchronization. In the process, all of the group's memberships are synchronized.

The user account must already exist as an object in the One Identity Manager database for the assignment to be made.

Detailed information about this topic

- Configuring single object synchronization on page 41

Tasks following synchronization

After the synchronization of data from the target system into the One Identity Manager database, rework may be necessary. Check the following tasks:

- Post-processing outstanding objects on page 50
- Managing Notes user accounts through account definitions on page 53

Post-processing outstanding objects

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select the **HCL Domino > Target system synchronization: Domino** category.

   The navigation view lists all the synchronization tables assigned to the **Domino** target system type.
2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

   All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the

synchronization log and which processing method was run. The **No log available** entry can mean the following:

- The synchronization log has already been deleted.

  - OR -

- An assignment from a member list has been deleted from the target system.

  The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

- An object that contains a member list has been deleted from the target system.

  During synchronization, the object and all corresponding entries in the assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.

TIP:

To display object properties of an outstanding object

1. Select the object on the target system synchronization form.
2. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.
4. Click on one of the following icons in the form toolbar to run the respective method.

Table 12: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

5. Confirm the security prompt with **Yes**.

NOTE: By default, the selected objects are processed in parallel, which speeds up the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.

Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.

To disable bulk processing

- Disable the icon in the form's toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the **Connection is read-only** option must not be set for the target system connection.

Related topics

- Adding custom tables to the target system synchronization on page 52

Adding custom tables to the target system synchronization

You must customize your target system synchronization to synchronize custom tables.

To add custom tables to target system synchronization

1. In the Manager, select the **HCL Domino > Basic configuration data > Target system types** category.
2. In the result list, select the **Domino** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

Related topics

- Post-processing outstanding objects on page 50

Managing Notes user accounts through account definitions

In the default installation, after synchronizing, employees are automatically created for the user accounts.If an account definition for the domain is not known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

Detailed information about this topic

- Assigning account definitions to linked user accounts on page 83

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

  The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.

- Analyzing synchronization

  You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.

- Logging messages

  One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.

- Reset start information

  If synchronization stopped unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.

For more information about these topics, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Displaying synchronization results on page 47

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > One Identity Manager connection** category.
3. In the **General** view, click **Edit connection**.

   This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

   This option is only effective if **Continue on error** is set in the synchronization workflow.

   Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.
5. Save the changes.

IMPORTANT: If this option is set, One Identity Manager tries to ignore commit errors that could be related to data errors in a single column. This causes the data changed in the affected column to be discarded and the object is subsequently saved again. This effects performance and leads to loss of data.

Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

Pausing handling of target system specific processes (Offline mode)

If a target system connector is not able to reach the target system temporarily, you can enable offline mode for the target system. This stops target system specific processes from being frozen and having to be manually re-enabled later.

Whether offline mode is generally available for a target system connection is set in the base object of the respective synchronization project. Once a target system is truly unavailable, the target system connection can be switched offline and online again with the Launchpad.

In offline mode, all Job servers assigned to the base object are stopped. This includes the synchronization server and all Job servers involved in load balancing. If one of the Job servers also handles other tasks, these are not processed either.

Prerequisites

Offline mode can only be specified for a base object if certain prerequisites are fulfilled.

- The synchronization server is not used for any other base object as a synchronization server.
- If a server function is assigned to the base object, none of the Job servers with this server function may have any other server function (for example, update server).
- A dedicated synchronization server must be set up to exclusively process the Job queue for this base object. The same applies to all Job servers that are determined by the server function.

To allow offline mode for a base object

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Base objects** category.
3. Select a base object in the document view and click .
4. Enable **Offline mode available**.
5. Click **OK**.
6. Save the changes.

IMPORTANT: To prevent data inconsistencies, the offline phase should be kept as short as possible.

The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and the target system, all pending processes must be handled before synchronization can start.

Only use offline mode, if possible, for short system downtimes such as maintenance windows.

To flag a target system as offline

1. Start the Launchpad on the gateway server and log in to the One Identity Manager database.
2. Select **Manage > System monitoring > Flag target systems as offline**.
3. Click **Run**.

   This opens the **Manage offline systems** dialog. The **Base objects** section displays the base objects of target system connections that can be switched to offline.
4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

   This stops all the Job servers assigned to the base object. No more synchronization or provisioning Jobs are performed. The Job Queue Info program shows when a Job server has been switched offline and the corresponding tasks are not being processed.

For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Deactivating synchronization on page 48

3

Managing Notes user accounts and employees

The main feature of One Identity Manager is to map employees together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

Because requirements vary between companies, One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following methods for linking employees and their user accounts:

- Employees can automatically obtain their account definitions using user account resources.

  If an employee does not yet have a user account in a Notes domain, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanisms and subsequent process handling.

  Employee documents can also be created through account definitions.

  When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.
- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

For more information about employee handling and administration, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Account definitions for Notes user accounts on page 58
- Assigning employees automatically to Notes user accounts on page 77
- Creating and editing Notes user accounts on page 130

Account definitions for Notes user accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a central user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role. Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

Specify the manage level for an account definition for managing user accounts. The user account's manage level specifies the extent of the employee's properties that are inherited by the user account. This allows an employee to have several user accounts in one target system, for example:

- Default user account that inherits all properties from the employee.
- Administrative user account that is associated to an employee but should not inherit the properties from the employee.

For more detailed information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Collecting IT operating data
- Assigning account definitions to employees and target systems

Detailed information about this topic

- Creating Notes account definitions on page 59
- Editing Notes account definitions on page 59
- Main data for Notes account definitions on page 60
- Editing manage levels on page 62
- Creating manage levels on page 63
- Main data for manage levels on page 64
- Creating mapping rules for IT operating data on page 65
- Entering IT operating data on page 67
- Modify IT operating data on page 68
- Assigning Notes account definitions to employees on page 69
- Assigning Notes account definitions to target systems on page 75
- Deleting Notes account definitions on page 75

Creating Notes account definitions

To create a new account definition

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Related topics

- Main data for Notes account definitions on page 60
- Editing Notes account definitions on page 59

Editing Notes account definitions

To edit an account definition

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.

4. Enter the account definition's main data.
5. Save the changes.

Related topics

- Main data for Notes account definitions on page 60
- Creating Notes account definitions on page 59

Main data for Notes account definitions

Enter the following data for an account definition:

Table 13: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. Leave empty for HCL Domino domains.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assigning the account definition to employees. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource can also be assigned

Property	Description
	directly to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is automatically assigned to all internal employees. To automatically assign the account definition to all internal employee, use the **Enable automatic assignment to employees** The account definition is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this account definition. To automatically remove the account definition assignment from all employees, use the **Disable automatic assignment to employees**. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily deactivated employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk.

Property	Description
	Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the employee but they do no inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed**: User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

NOTE: The **Full managed** and **Unmanaged** manage levels are analyzed in templates. You can customize the supplied templates in the Designer.

You can define other manage levels depending on your requirements. You need to amend the templates to include manage level approaches.

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For more

information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

- Employee user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the employee is reinstated at a later date, the user accounts are also reactivated.
- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted.

To edit a manage level

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list.
3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

Related topics

- Main data for manage levels on page 64
- Creating manage levels on page 63
- Assigning manage levels to Notes account definitions on page 64

Creating manage levels

One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

IMPORTANT: In the Designer, extend the templates by adding the procedure for the additional manage levels. For more information about templates, see the *One Identity Manager Configuration Guide*

To create a manage level

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Manage levels** category.
2. Click in the result list.
3. On the main data form, edit the main data of the manage level.
4. Save the changes.

Related topics

- Main data for manage levels on page 64
- Editing manage levels on page 62

Assigning manage levels to Notes account definitions

IMPORTANT: The **Unmanaged** manage level is assigned automatically when you create an account definition and it cannot be removed.

To assign manage levels to an account definition

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage level.

   TIP: In the **Remove assignments** pane, you can remove assigned manage levels.

   To remove an assignment

   - Select the manage level and double-click ✓.
5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 14: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. (Default) • **Always**: Data is always updated. • **Only initially**: Data is only determined at the start.

Property	Description
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the employee's primary roles.

The following IT operating data is used in the One Identity Manager default configuration for automatically creating user accounts for an employee in the target system and modifying them.

- Domino server
- Domino certificate
- Mailbox template
- Groups can be inherited
- Identity
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
    - **Column**: User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
    - **Source**: Specifies which roles to use in order to find the user account properties. You have the following options:
        - Primary department
        - Primary location
        - Primary cost center
        - Primary business roles

          NOTE: The business role can only be used if the Business Roles Module is available.
        - Empty

          If you select a role, you must specify a default value and set the **Always use default value** option.
    - **Default value**: Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
    - **Always use default value**: Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
    - **Notify when applying the default**: Specifies whether an email is sent to a specific mailbox when the default value is used. The **Employee - new user account with default properties created** mail template is used.

      To change the mail template, in the Designer, adjust the **TargetSystem | NDO | Accounts | MailTemplateDefaultValues** configuration parameter.
5. Save the changes.

Related topics

- Entering IT operating data on page 67

Entering IT operating data

To create user accounts with the **Full managed** manage level, the required IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the business roles, departments, locations, or cost centers. An employee is assigned a primary business role, primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

You can also specify IT operating data directly for a specific account definition.

Example:

Normally, each employee in department A obtains a default user account in the domain A. In addition, certain employees in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

Specify the effective IT operating data of department A for the domain A. This IT operating data is used for standard user accounts. In addition, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.
3. Click **Add** and enter the following data.
    - **Effects on**: Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

      To specify an application scope

        a. Click → next to the field.

        b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table or an account definition.

        c. Select the specific target system or account definition under **Effects on**.

        d. Click **OK**.
    - **Column**: Select the user account property for which the value is set.

In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

- **Value**: Enter a fixed value to assign to the user account's property.

4. Save the changes.

Related topics

- Creating mapping rules for IT operating data on page 65

Modify IT operating data

If IT operating data changes, you must transfer the changes to the existing user accounts. To do this, templates must be rerun on the affected columns. Before you can run the templates, you can check what effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

Prerequisites

- The IT operating data of a department, a cost center, a business role, or a location have been changed.

  - OR -

- The default values in the IT operating data template were modified for an account definition.

NOTE: If the assignment of an employee to a primary department, cost center, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Run templates** task.

   This displays a list of all user accounts that were created with the selected account definition and whose properties were changed by modifying the IT operating data. That means:

   - **Old value**: Value of the object property before changing the IT operating data.
   - **New value**: Value of the object property after changing the IT operating data.
   - **Selection**: Specifies whether the new value is copied to the user account.

4. Mark all the object properties in the **selection** column that will be given the new value.
5. Click **Apply**.

   The templates are applied to all selected user accounts and properties.

Assigning Notes account definitions to employees

Account definitions are assigned to company employees.

Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations, or roles. The employees are categorized into these departments, cost centers, locations, or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees.

You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. Department managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or added directly to the IT Shop as products.

In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

NOTE: If a user account already exists and is disabled, then it is re-enabled. In this case, you must change the user account manage level afterward.

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted.

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (departments, cost centers, locations, or business roles).

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task and configure the permitted assignments.
    - To generally allow an assignment, enable the **Assignments allowed** column.
    - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

For more information about preparing role classes to be assigned, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Assigning Notes account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
    - On the **Departments** tab, assign departments.
    - On the **Locations** tab, assign locations.
    - On the **Cost centers** tab, assign cost centers.

    TIP: In the **Remove assignments** pane, you can remove assigned organizations.

    To remove an assignment

    - Select the organization and double-click .
5. Save the changes.

Assigning Notes account definitions to business roles

NOTE: This function is only available if the Business Roles Module is installed.

To add account definitions to hierarchical roles

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign business roles** task.

4. In the **Add assignments** pane, select the role class and assign business roles.

   TIP: In the **Remove assignments** pane, you can remove assigned business roles.

   To remove an assignment

   - Select the business role and double-click ✓.

5. Save the changes.

Assigning Notes account definitions to all employees

Use this task to assign the account definition to all internal employees. Employees that are marked as external do not obtain this account definition. Once a new internal employee is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

IMPORTANT: Only run this task if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.

To assign an account definition to all employees

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to employees** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all employees, run the DISABLE AUTOMATIC ASSIGNMENT TO EMPLOYEES task. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.

Assigning Notes account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.

3. Select the **Assign to employees** task.
4. In the **Add assignments** pane, add employees.

   TIP: In the **Remove assignments** pane, you can remove assigned employees.

   To remove an assignment

   - Select the employee and double-click ✓.
5. Save the changes.

Assigning Notes account definitions to system roles

NOTE: This function is only available if the System Roles Module is installed.

Account definitions with the **Only use in IT Shop** option can only be assigned to system roles that also have this option set.

To add account definitions to a system role

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.
5. Save the changes.

Adding Notes account definitions to the IT Shop

An account definition can be requested by shop customers when it is assigned to an IT Shop shelf. To ensure it can be requested, further prerequisites need to be guaranteed.

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in the Web Portal, assign a service category to the service item.

- If the account definition is only assigned to employees using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

NOTE: IT Shop administrators can assign account definitions to IT Shop shelves if login is role-based. Target system administrators are not authorized to add account definitions in the IT Shop.

To add an account definition to the IT Shop (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To add an account definition to the IT Shop (non role-based login)

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves (non role-based login)

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from all IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

1. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

For more information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Main data for Notes account definitions on page 60
- Assigning Notes account definitions to departments, cost centers, and locations on page 70
- Assigning Notes account definitions to business roles on page 70
- Assigning Notes account definitions directly to employees on page 71
- Assigning Notes account definitions to system roles on page 72

Assigning Notes account definitions to target systems

The following prerequisites must be fulfilled if you implement automatic assignment of user accounts and employees resulting in administered user accounts (**Linked configured** state):

- The account definition is assigned to the target system.
- The account definition has the default manage level.

User accounts are only linked to the employee (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.

To assign the account definition to a target system

1. In the Manager, select the domain in the **HCL Domino > Domains** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Related topics

- Assigning employees automatically to Notes user accounts on page 77

Deleting Notes account definitions

You can delete account definitions if they are not assigned to target systems, employees, hierarchical roles or any other account definitions.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.
    b. Select an account definition in the result list.
    c. Select the **Change main data** task.
    d. Select the **Disable automatic assignment to employees** task.
    e. Confirm the security prompt with **Yes**.
    f. Save the changes.
2. Remove direct assignments of the account definition to employees.

a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Assign to employees** task.

d. In the **Remove assignments** pane, remove employees.

e. Save the changes.

3. Remove the account definition's assignments to departments, cost centers, and locations.

a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Assign organizations** task.

d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.

e. Save the changes.

4. Remove the account definition's assignments to business roles.

a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Assign business roles** task.

d. In the **Remove assignments** pane, remove the business roles.

e. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

For more detailed information about unsubscribing requests, see the *One Identity Manager Web Designer Web Portal User Guide*.

To remove an account definition from all IT Shop shelves (role-based login)

a. In the Manager, select the **Entitlements > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Remove from all shelves (IT Shop)** task.

d. Confirm the security prompt with **Yes**.

e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Remove from all shelves (IT Shop)** task.

d. Confirm the security prompt with **Yes**.

e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Change main data** task.

d. From the **Required account definition** menu, remove the account definition.

e. Save the changes.

7. Remove the account definition's assignments to target systems.

a. In the Manager, select the domain in the **HCL Domino > Domains** category.

b. Select the **Change main data** task.

c. On the **General** tab, remove the assigned account definitions.

d. Save the changes.

8. Delete the account definition.

a. In the Manager, select the **HCL Domino > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Click to delete an account definition.

Assigning employees automatically to Notes user accounts

When you add a user account, an existing employee can automatically be assigned to it. If necessary, a new employee can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user

account is created either manually or through synchronization.

Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

If you run this procedure during working hours, automatic assignment of employees to user accounts takes place from that moment onwards. If you disable the procedure again later, the changes only affect user accounts added or updated after this point in time. Existing employee assignments to user accounts remain intact.

NOTE: It is not recommended to assign employees using automatic employee assignment in the case of administrative user accounts. Use **Change main data** to assign employees to administrative user accounts for the respective user account.

For more information about assigning employees automatically, see the *One Identity Manager Target System Base Module Administration Guide*.

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | NDO | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the **TargetSystem | NDO | PersonAutoDefault** configuration parameter and select the required mode.
- In the **TargetSystem | NDO | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to employees shall take place.

  Example:

  `ADMINISTRATOR`

  TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic employee assignment** dialog.

  To edit the exclude list for automatic employee assignment

  1. In the Designer, edit the **PersonExcludeList** configuration parameter.
  2. Click **...** next to the **Value** field.

     This opens the **Exclude list for Notes user accounts** dialog.
  3. To add a new entry, click **Add**.

     To edit an entry, select it and click **Edit**.
  4. Enter the name of the user account that does not allow employees to be assigned automatically.

     Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.

5. To delete an entry, select it and click **Delete**.
6. Click **OK**.

- Use the **TargetSystem | NDO | PersonAutoDisabledAccounts** configuration parameter to specify whether employees can be automatically assigned to locked user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the domain. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employees assigned to the domain.

NOTE:

The following applies for synchronization:

- Automatic employee assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:

- Automatic employee assignment takes effect if user accounts are added.

NOTE:

In the default installation, after synchronizing, employees are automatically created for the user accounts.If an account definition for the domain is not known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

For more information, see Managing Notes user accounts through account definitions on page 53.

Related topics

- Creating Notes account definitions on page 59
- Assigning Notes account definitions to target systems on page 75
- Changing the manage level in Notes user accounts on page 82
- Editing search criteria for automatic employee assignment on page 79

Editing search criteria for automatic employee assignment

NOTE: One Identity Manager supplies a default mapping for employee assignment. Only carry out the following steps when you want to customize the default mapping.

The criteria for employee assignments are defined for the domain. You specify which user account properties must match the employee's properties such that the employee can be

assigned to the user account. You can limit search criteria further by using format definitions.

The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (`AccountToPersonMatchingRule`) in the `NDODomain` table.

Search criteria are evaluated when employees are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly.

NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

To specify criteria for employee assignment

1. In the Manager, select the **HCL Domino > Domains** category.
2. Select the domain in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 15: Default search criteria for user accounts

Apply to	Column for employee	Column for user account
Notes user accounts	First name (`FirstName`) AND last name (`LastName`)	First name (`FirstName`) AND last name (`LastName`)
Enabled Notes user accounts	First name (`FirstName`) AND last name (`LastName`)	First name (`FirstName`) AND last name (`LastName`)

5. Save the changes.

For more information about defining search criteria, see the One Identity Manager Target System Base Module Administration Guide.

Related topics

- Assigning employees automatically to Notes user accounts on page 77
- Finding employees and directly assigning them to user accounts on page 80

Finding employees and directly assigning them to user accounts

Based on the search criteria, you can create a suggestion list for the assignment of employees to user accounts and make the assignment directly. User accounts are grouped

in different views for this.

Table 16: Manual assignment view

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an employee is assigned.
Without employee assignment	This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.

To apply search criteria to user accounts

1. In the Manager, select the **HCL Domino > Domains** category.
2. Select the domain in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. At the bottom of the form, click **Reload**.

   All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

TIP: By double-clicking on an entry in the view, you can view the user account and employee main data.

The assignment of employees to user accounts creates connected user accounts (**Linked** state). To create managed user accounts (**Linked configured** state), you can assign an account definition at the same time.

To assign employees directly over a suggestion list

- Click **Suggested assignments**.
  1. Click the **Selection** box of all user accounts to which you want to assign the suggested employees. Multi-select is possible.
  2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
  3. Click **Assign selected**.
  4. Confirm the security prompt with **Yes**.

     The employees determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

  - OR -

- Click **No employee assignment**.

1. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.
2. Click the **Selection** box of all user accounts to which you want to assign the selected employees. Multi-select is possible.
3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
4. Click **Assign selected**.
5. Confirm the security prompt with **Yes**.

   The employees displayed in the **Employee** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.
  1. Click the **Selection** box of all the user accounts you want to delete the employee assignment from. Multi-select is possible.
  2. Click **Remove selected**.
  3. Confirm the security prompt with **Yes**.

     The assigned employees are removed from the selected user accounts.

Changing the manage level in Notes user accounts

The default manage level is applied if you create user accounts using automatic employee assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Related topics

- General main data for Notes user accounts on page 131

Assigning account definitions to linked user accounts

An account definition can be subsequently assigned to user accounts with **Linked** status. This may be necessary, for example, if:

- Employees and user accounts have been linked manually.
- Automatic employee assignment is configured, but an account definition is not yet assigned to the customer when inserting a user account.

To manage user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **HCL Domino > User accounts > Linked but not configured > Domain>** category.
    b. Select the **Assign account definition to linked accounts** task.
    c. In the **Account definition** menu, select the account definition.
    d. Select the user accounts that contain the account definition.
    e. Save the changes.

Detailed information about this topic

- Account definitions for Notes user accounts on page 58
- Assigning Notes account definitions to target systems on page 75

Manually linking employees to Notes user accounts

An employee can be linked to multiple Notes user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One employee can also use default user accounts with different types.

NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

To manually assign user accounts to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list and run the **Assign Notes user accounts** task.
3. Assign the user accounts.
4. Save the changes.

Related topics

- Supported user account types on page 84

Supported user account types

Different types of user accounts, such as default user accounts, administrative user accounts, service accounts, or privileged user accounts, can be mapped in One Identity Manager.

The following properties are used for mapping different user account types.

- Identity

  The **Identity** property (`IdentityType` column) is used to describe the type of user account.

  Table 17: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.	Organizational
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

The primary identity, the organizational identity, and the personalized admin identity are used for different user accounts, which can be used by the same actual employee to perform their different tasks within the company.

To provide user accounts with a personalized admin identity or an organizational identity for an employee, you create subidentities for the employee. These subidentities are then linked to user accounts, enabling you to assign the required permissions to the different user accounts.

User accounts with a sponsored identity, shared identity, or service identity are linked to pseudo employees that do not refer to a real employee. These pseudo employees are needed so that permissions can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether pseudo employees need to be considered separately.

For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

- Privileged user account

  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are labeled with the **Privileged user account** property (`IsPrivilegedAccount` column).

Detailed information about this topic

- Default user accounts on page 85
- Administrative user accounts on page 86
- Providing administrative user accounts for one employee on page 87
- Providing administrative user accounts for several employees on page 88
- Privileged user accounts on page 89

Default user accounts

Normally, each employee obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the employee. The effect of the link and the scope of the employee's inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.

2. Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

   The type of IT operating data required depends on the target system. The following setting are recommended for default user accounts:

   - In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable the **Always use default value** option.
   - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

   Specify in the departments, cost centers, locations, or business roles that IT operating data should apply when you set up a user account.
5. Assign the account definition to employees.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

Related topics

- Account definitions for Notes user accounts on page 58

Administrative user accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as **Administrator**.

Administrative user accounts are imported into One Identity Manager during synchronization.

NOTE: Some administrative user accounts can be automatically identified as privileged user accounts. To do this, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

Related topics

- Providing administrative user accounts for one employee on page 87
- Providing administrative user accounts for several employees on page 88

Providing administrative user accounts for one employee

Prerequisites

- The user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be linked to a main identity.

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
    a. In the Manager, select the **HCL Domino > User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change main data** task.
    d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
2. Link the user account to the employee who will be using this administrative user account.
    a. In the Manager, select the **HCL Domino > User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change main data** task.
    d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

    TIP: If you are the target system manager, you can choose to create a new person.

Related topics

- Providing administrative user accounts for several employees on page 88
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

- The user account must be labeled as a shared identity.
- A pseudo employee must exist. The pseudo employee must be labeled as a shared identity and must have a manager.
- The employees who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.
    a. In the Manager, select the **HCL Domino > User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change main data** task.
    d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to a pseudo employee.
    a. In the Manager, select the **HCL Domino > User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change main data** task.
    d. On the **General** tab, select the pseudo employee from the **Employee** menu.

    TIP: If you are the target system manager, you can choose to create a new pseudo employee.
3. Assign the employees who will use this administrative user account to the user account.
    a. In the Manager, select the **HCL Domino > User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Assign employees authorized to use** task.
    d. In the **Add assignments** pane, add employees.

    TIP: In the **Remove assignments** pane, you can remove assigned employees.

    To remove an assignment

    - Select the employee and double-click .

Related topics

- Providing administrative user accounts for one employee on page 87
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are labeled with the **Privileged user account** property (`IsPrivilegedAccount` column).

NOTE: The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the `TSBVAccountIsPrivDetectRule` table (which is a table of the **Union** type). The evaluation is done in the `TSB_SetIsPrivilegedAccount` script.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.
3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for the IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

   The type of IT operating data required depends on the target system. The following settings are recommended for privileged user accounts:

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
   - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.
5. Enter the effective IT operating data for the target system.

   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

6. Assign the account definition directly to employees who work with privileged user accounts.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, specify how the login names are formatted in the template.

Related topics

- Account definitions for Notes user accounts on page 58

Specifying deferred deletion for Notes user accounts

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or blocked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is **30** days.

  In the Designer, enter a different value for deferred deletion in the `Deferred deletion [days]` property of the **NDOUser** table.

- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

  To use object-specific deferred deletion, in the Designer, create a `Script (deferred deletion)` for the **NDOUser** table.

  Example:

  Deferred deletion of privileged user accounts is 10 days. The following **Script (deferred deletion)** is entered in the table.

```
If Not $IsPrivilegedAccount:Bool$ Then
     Value = 10
End If
```

For more information on editing table definitions and configuring deferred deletion in the Designer, see the *One Identity Manager Configuration Guide*.

4

Managing memberships in Notes groups

In Notes, user accounts can be grouped into Notes groups. Notes groups regulate access to resources in Domino.

In One Identity Manager, you can assign Notes groups directly to user accounts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request Notes groups through the Web Portal. To do this, Notes groups are provided in the IT Shop.

Detailed information about this topic

- Assigning Notes groups to Notes user accounts on page 92
- Effectiveness of membership in Notes user groups on page 101
- Notes group inheritance based on categories on page 103
- Overview of all assignments on page 106

Assigning Notes groups to Notes user accounts

In One Identity Manager, Notes groups can be assigned directly or indirectly to Notes user accounts.

In the case of indirect assignment, employees and Notes groups are arranged in hierarchical roles. The number of groups assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If you add an employee to roles and that employee owns a Notes user account, the user account is added to the Notes group.

Furthermore, Notes groups can be requested through the Web Portal. To do this, add employees to a shop as customers. All Notes groups are assigned to this shop can be requested by the customers. Requested groups are assigned to the employees after approval is granted.

You can use system roles to group Notes groups together and assign them to employees as a package. You can create system roles that contain only Notes groups. You can also group any number of company resources into a system role.

To react quickly to special requests, you can assign Notes groups directly to Notes user accounts.

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide* *One Identity Manager Business Roles Administration Guide*
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Prerequisites for indirect assignment of Notes groups to Notes user accounts on page 93
- Assigning Notes groups to departments, cost centers and locations on page 94
- Assigning Notes groups to business roles on page 96
- Assigning Notes user accounts directly to a Notes group on page 99
- Adding Notes groups to system roles on page 97
- Adding Notes groups to the IT Shop on page 98
- Assigning Notes groups directly to a Notes user account on page 100

Prerequisites for indirect assignment of Notes groups to Notes user accounts

In the case of indirect assignment, employees, and Notes groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning Notes groups indirectly, check the following settings and modify them if necessary:

1. The assignment of employees and Notes groups is permitted for departments, cost centers, locations, or business roles.

For more detailed information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
   - To generally allow an assignment, enable the **Assignments allowed** column.
   - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

2. Settings for assigning Notes groups to Notes user accounts.
   - Notes user accounts are marked with the **Groups can be inherited** option.
   - Notes user accounts are linked with an employee through the `UID_Person` (**Person**) column.
   - Notes user accounts and groups belong to the same Notes domain.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Creating and editing Notes user accounts on page 130
- General main data for Notes user accounts on page 131

Assigning Notes groups to departments, cost centers and locations

Assign groups to departments, cost centers, or locations so that the group can be assigned to user accounts through these organizations. This task is not available for dynamic groups.

To assign a group to departments, cost centers, or locations (non role-based login)

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

   TIP: In the **Remove assignments** pane, you can remove assigned organizations.

   To remove an assignment
   - Select the organization and double-click ✓.
5. Save the changes.

To assign groups to a department, a cost center, or a location (non role-based login or role-based login)

1. In the Manager, select the **Organizations > Departments** category.

   - OR -

   In the Manager, select the **Organizations > Cost centers** category.

   - OR -

   In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign Notes groups** task.
4. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment
   - Select the group and double-click ✓.
5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Notes groups to Notes user accounts on page 93
- Assigning Notes groups to business roles on page 96
- Assigning Notes user accounts directly to a Notes group on page 99
- Adding Notes groups to system roles on page 97

- Adding Notes groups to the IT Shop on page 98
- One Identity Manager users for managing Domino on page 13

Assigning Notes groups to business roles

NOTE: This function is only available if the Business Roles Module is installed.

Assign the group to business roles so that the group is assigned to user accounts through these business roles. This task is not available for dynamic groups.

To assign a group to a business role (non role-based login)

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

   TIP: In the **Remove assignments** pane, you can remove assigned business roles.

   To remove an assignment

   - Select the business role and double-click ✓.
5. Save the changes.

To assign groups to a business role (non role-based login or role-based login)

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign Notes groups** task.
4. In the **Add assignments** pane, assign the groups.
   - (Optional) To filter the groups, select a domain in the **Notes Domains** input field.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Notes groups to Notes user accounts on page 93
- Assigning Notes groups to departments, cost centers and locations on page 94
- Assigning Notes user accounts directly to a Notes group on page 99

- Adding Notes groups to system roles on page 97
- Adding Notes groups to the IT Shop on page 98
- One Identity Manager users for managing Domino on page 13

Adding Notes groups to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add a group to system roles.

If you assign a system role to employees, all Notes user accounts owned by these employees inherit the group.

This task is not available for dynamic groups.

NOTE: Groups with **Only use in IT Shop** set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

To assign a group to system roles

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.
5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Notes groups to Notes user accounts on page 93
- Assigning Notes groups to departments, cost centers and locations on page 94
- Assigning Notes groups to business roles on page 96
- Assigning Notes user accounts directly to a Notes group on page 99
- Adding Notes groups to the IT Shop on page 98

Adding Notes groups to the IT Shop

When you assign a group to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed:

- The group is not a dynamic group.
- The group must be labeled with the **IT Shop** option.
- The group must be assigned a service item.

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the group easier to find in the Web Portal, assign a service category to the service item.
- If you only want the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

NOTE: With role-based login, the IT Shop administrators can assign groups to IT Shop shelves. Target system administrators are not authorized to add groups to IT Shop.

To add a group to the IT Shop.

1. In the Manager, select the **HCL Domino > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Notes groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane, assign the group to the IT Shop shelves.
6. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager, select the **HCL Domino > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Notes groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
6. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **HCL Domino > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Notes groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The group is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this group are canceled.

For more information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Prerequisites for indirect assignment of Notes groups to Notes user accounts on page 93
- General main data for Notes groups on page 154
- Assigning Notes groups to departments, cost centers and locations on page 94
- Assigning Notes groups to business roles on page 96
- Assigning Notes user accounts directly to a Notes group on page 99
- Adding Notes groups to system roles on page 97

Assigning Notes user accounts directly to a Notes group

To react quickly to special requests, you can assign groups directly to user accounts. This task is not available for dynamic groups.

To assign user accounts directly to a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **User** tab.
5. In **Add assignments** pane, assign user accounts.

- (Optional) To filter the user accounts, select a domain in the **Notes domains** input field.

TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

To remove an assignment

- Select the user account and double-click ✓.

6. Save the changes.

Related topics

- Assigning Notes groups directly to a Notes user account on page 100
- Assigning Notes groups to departments, cost centers and locations on page 94
- Assigning Notes groups to business roles on page 96
- Adding Notes groups to system roles on page 97
- Adding Notes groups to the IT Shop on page 98
- Assigning owners to Notes groups on page 162
- Assigning administrators to Notes groups on page 163

Assigning Notes groups directly to a Notes user account

Groups can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and groups in hierarchical roles, such as departments, cost centers, locations, or business roles. If the employee has a Notes user account, groups in the hierarchical roles are inherited by this user account.

To react quickly to special requests, you can assign groups directly to user accounts. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign groups directly to user accounts

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign the groups.
    - (Optional) To filter the groups, select a domain in the **Notes Domains** input field.

TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click ✓.

5. Save the changes.

User accounts cannot be manually added to dynamic groups. You can assign user accounts additionally to dynamic groups using the additional list.

Related topics

- Maintaining excluded lists and additional lists for Notes user accounts on page 146
- Memberships in dynamic groups on page 166
- Assigning Notes user accounts directly to a Notes group on page 99
- Assigning Notes groups to departments, cost centers and locations on page 94
- Assigning Notes groups to business roles on page 96
- Adding Notes groups to system roles on page 97
- Adding Notes groups to the IT Shop on page 98

Effectiveness of membership in Notes user groups

When groups are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually exclusive groups. To do this, you specify which of the two groups should apply to the user accounts if both are assigned.

It is possible to assign an excluded group at any time either directly, indirectly, or with an IT Shop request. One Identity Manager determines whether the assignment is effective.

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" `AND` "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.
- One Identity Manager does not check if membership of an excluded group is permitted in another group (`NDOGroupInGroup` table).

The effectiveness of the assignments is mapped in the `NDOUserInGroup` and `BaseTreeHasNDOGroup` tables by the `XIsInEffect` column.

Example: The effect of group memberships

- The groups A, B, and C are defined in a domain.
- Group A is assigned through the "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

Jo User1 has a user account in this domain. They primarily belong to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to them secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B, and C.

By using suitable controls, you want to prevent an employee from obtaining authorizations of groups A and group B at the same time. That means, groups A, B, and C are mutually exclusive. A user, who is a member of group C cannot be a member of group B at the same time. That means, groups B and C are mutually exclusive.

Table 18: Specifying excluded groups (`NDOGroupExclusion` table)

Effective group	Excluded group
Group A	
Group B	Group A
Group C	Group B

Table 19: Effective assignments

Employee	Member in role	Effective group
Pat Identity1	Marketing	Group A
Jan User3	Marketing, finance	Group B
Jo User1	Marketing, finance, control group	Group C
Chris User2	Marketing, control group	Group A, Group C

Only the group C assignment is in effect for Jo User1. It is published in the target system. If Jo User1 leaves the "control group" business role at a later date, group B also takes effect.

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

Table 20: Excluded groups and effective assignments

Employee	Member in role	Assigned group	Excluded group	Effective group
Chris User2	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

- The **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.

  In the Designer, set the configuration parameter and compile the database.

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive groups belong to the same domain

To exclude a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

   In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.
5. Save the changes.

Notes group inheritance based on categories

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table.

Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

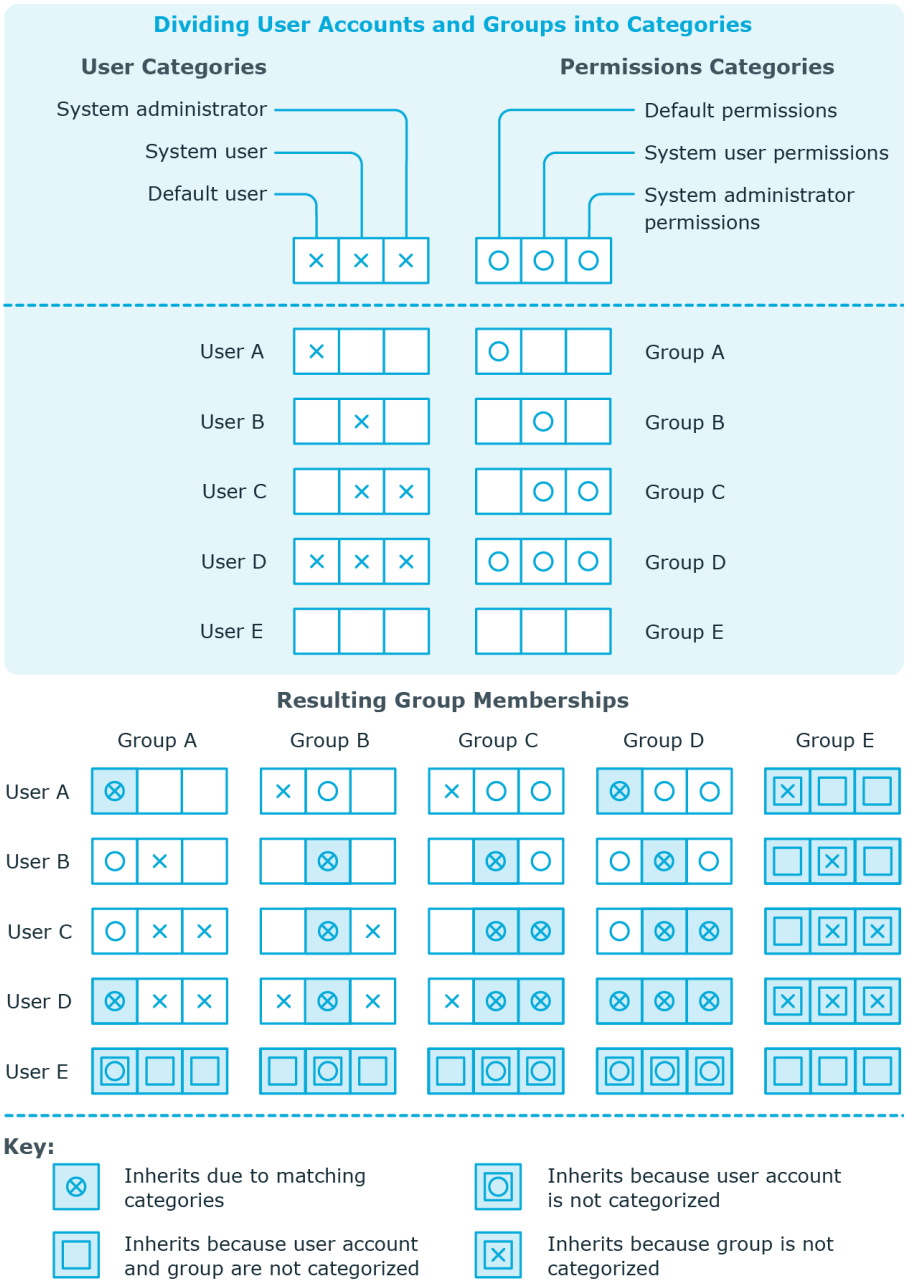
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or the user account is not put into categories.

NOTE: Inheritance through categories is only taken into account when groups are assigned indirectly through hierarchical roles. Categories are not taken into account when groups are directly assigned to user accounts.

Table 21: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	System user permissions
3	System administrator	System administrator permissions

Figure 2: Example of inheriting through categories.



To use inheritance through categories

1. In the Manager, define the categories in the domain.
2. Assign categories to user accounts through their main data.
3. Assign categories to groups through their main data.

Related topics

- Defining categories for the inheritance of Notes groups on page 128
- General main data for Notes user accounts on page 131
- General main data for Notes groups on page 154

Overview of all assignments

The **Overview of all assignments** report is displayed for some objects, such as authorizations, compliance rules, or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles, and IT Shop structures in which there are employees who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Examples:

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees who violate this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the icon in the report's toolbar.
- Double-click a control to show all child roles belonging to the selected role.

- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employees for tracking. This creates a new business role to which the employees are assigned.

Figure 3: Toolbar of the Overview of all assignments report.

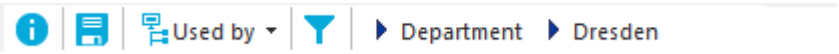


Table 22: Meaning of icons in the report toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

Login information for Notes user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login information generated to users.

Detailed information about this topic

- Password policies for Notes user accounts on page 108
- Initial password for new Notes user accounts on page 120
- Email notifications about login data on page 120

Password policies for Notes user accounts

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined password policies on page 109
- Using password policies on page 110
- Creating password policies on page 111
- Editing password policies

- Custom scripts for password requirements on page 116
- Password exclusion list on page 119
- Checking passwords on page 119
- Testing password generation on page 120

Predefined password policies

You can customize predefined password policies to meet your own requirements if necessary.

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time log in on the Web Portal (`Person.Passcode`).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

For more information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** defines the settings for the (`Person.CentralPassword`) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Employee central password policy** does not violate the target system-specific requirements for passwords.

For more information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 9.1, the configuration parameter settings for forming passwords are passed on to

the target system-specific password policies.

The **Notes password policy** is predefined for HCL Domino. You can apply this password policy to Notes user accounts (`NDOUser.UserPassword`, `NDOUser.InternetPassword`, and `NDOUser.InitialPassword`) of a Notes domain.

If the domains' password requirements differ, it is recommended that you set up your own password policies for each domain.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Using password policies

The **Notes password policy** is predefined for HCL Domino. You can apply this password policy to Notes user accounts (`NDOUser.UserPassword`, `NDOUser.InternetPassword`, and `NDOUser.InitialPassword`) of a Notes domain.

If the domains' password requirements differ, it is recommended that you set up your own password policies for each domain.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policies of the user account's Notes domain.
4. The **One Identity Manager password policy** (default policy).

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.

- **Apply to**: Application scope of the password policy.

  To specify an application scope

  1. Click → next to the field.
  2. Select one of the following references under **Table**:
     - The table that contains the base objects of synchronization.
     - To apply the password policy based on the account definition, select the **TSBAccountDef** table.
     - To apply the password policy based on the manage level, select the **TSBBehavior** table.
  3. Under **Apply to**, select the table that contains the base objects.
     - If you have selected the table containing the base objects of synchronization, next select the specific target system.
     - If you have selected the **TSBAccountDef** table, next select the specific account definition.
     - If you have selected the **TSBBehavior** table, next select the specific manage level.
  4. Click **OK**.

- **Password column**: Name of the password column.
- **Password policy**: Name of the password policy to use.

5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Creating password policies

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

To create a password policy

1. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
2. Click in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

Detailed information about this topic

- General main data of password policies on page 113
- Policy settings on page 113
- Character classes for passwords on page 114
- Custom scripts for password requirements on page 116
- Editing password policies on page 112

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.

Detailed information about this topic

- General main data of password policies on page 113
- Policy settings on page 113
- Character classes for passwords on page 114
- Custom scripts for password requirements on page 116
- Creating password policies on page 111

General main data of password policies

Enter the following main data of a password policy.

Table 23: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Text field for additional explanation. Translate the given text using the button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Policy settings

Define the following settings for a password policy on the **Password** tab.

Table 24: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.

Property	Meaning
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into account. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 25: Character classes for passwords

Property	Meaning
Required number of character classes	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for **Min. number letters**, **Min. number lowercase**, **Min. number uppercase**, **Min. number digits**, and **Min. number special characters**. That means: • Value **0**: All character class rules must be fulfilled. • Value **>0**: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value **>0**. NOTE: Generated passwords are not tested for this.
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.

Property	Meaning
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

- Checking passwords with a script on page 116
- Generating passwords with a script on page 118

Checking passwords with a script

You can implement a script if additional policies need to be used for checking a password that cannot be mapped with the available settings.

Syntax of check scripts

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
```

With parameters:

`policy` = password policy object

`spwd` = password to check

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

Example: Script that checks a password

A password cannot start with **?** or **!** . The password cannot start with three identical characters. The script checks a given password for validity.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or
            '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in
            password")#)
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
    e. Save the changes.

Related topics

- Generating passwords with a script on page 118

Generating passwords with a script

You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

With parameters:

`policy` = password policy object

`spwd` = generated password

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

Example: Script that generates a password

In random passwords, this script replaces the invalid characters **?** and **!** at the beginning of a password with **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.

d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.

e. Save the changes.

Related topics

- Checking passwords with a script on page 116

Password exclusion list

You can add words to a list of restricted terms to prohibit them from being used in passwords.

NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking passwords

When you verify a password, all the password policy settings, custom scripts, and the restricted passwords are taken into account.

To verify if a password conforms to the password policy

1. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.

   A display next to the password shows whether it is valid or not.

Testing password generation

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. In the Manager, select the **HCL Domino > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new Notes user accounts

You can issue an initial password for a new Notes user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword** configuration parameter.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.

Related topics

- Password policies for Notes user accounts on page 108
- Email notifications about login data on page 120

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text in a mail

template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

The following prerequisites must be fulfilled in order to use notifications:

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
2. In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.
3. Ensure that all employees have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
4. Ensure that a language can be determined for all employees. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

When a randomly generated password is issued for the new user account, the initial login data for a user account is sent by email to a previously specified person.

To send initial login data by email

1. In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword** configuration parameter.
2. In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.
3. In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

   By default, the message sent uses the mail template **Employee - new user account created**. The message contains the name of the user account.
4. In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

   By default, the message sent uses the mail template **Employee - initial password for new user account**. The message contains the initial password for the user account.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Using AdminP requests for handling Domino processes

Domino contains an asynchronous mechanism for processing various internal tasks. For example, if the name of a Jo User1anges, this mechanism ensures that the access control list from the Notes database is also modified.

The request is processed by the Notes server task **AdminP** that runs on every Notes server. This task checks at set intervals whether there are new requests pending that require handling. These are placed in the Notes database `admin4.nsf` in the form of request documents and then replicated on every Notes server. After a request has been processed, the running Notes server creates a response document and if necessary a follow-up request.

AdminP requests are queued by certain changes in One Identity Manager, for example, to change parts of a users name, exchanging certificates, or when restoring a user ID.

Several factors are involved in determining when these will be processed:

- When was the request replicated on the running Notes server?
- How often does the AdminP server task run on the running Notes server?
- Which type of request is it?

Related topics

- AdminP request main data on page 123
- Automatically confirming AdminP requests on page 122

Automatically confirming AdminP requests

Certain AdminP requests have to be confirmed first by the administrator before they can be run. It is possible to confirm them automatically with One Identity Manager. Prerequisite for this is regular synchronization of the Admin4 database.

To confirm pending AdminP requests regularly

- In the Designer, configure and enable the **Automatically confirm Domino request from AdminP** schedule.

  For more information about editing schedules, see the *One Identity Manager Operational Guide*.

Confirmation of the following requests has currently been implemented:

- `Approve MailfileDeletion`
- `Approve MovedReplicaDeletion`
- `Approve ReplicaDeletion`

Related topics

- Using AdminP requests for handling Domino processes on page 122

AdminP request main data

Properties of synchronized AdminP requests are displayed in the Manager.

To display the main data of a request document

- In the Manager, select the **HCL Domino > Hierarchical view > <domain> > Administration requests > <filter> > <object> > <action>** category.

Table 26: Main data of an AdminP request document

Property	Description
Action	Action to be run by the AdminP request.
Executing server	Server to run the request.
Object	Name of the object to which the action will be applied.
Author	Name of the AdminP request author.
Database file	File name of the database to be processed.
Approval code	Specifies whether the AdminP request has been approved by an administrator.
Change label	Specifies whether the AdminP request was changed.

To display the main data of an response document

1. In the Manager, select the **HCL Domino > Hierarchical view > <domain> > Administration requests > <filter> > <object> > <action>** category.
2. Select the response document in the result list.

Table 27: Main data of an AdminP response document

Property	Description
Action	Action that was run by the AdminP request.
request document	Unique ID for the associated request document
Object	Name of the object that was processed.
Author	Name of the AdminP request author.
Executing server	Server that run the request.
Employee on	Creation date of the request.
Database file	File name of the database processed.
Error code	Specifies whether errors occurred while processing AdminP requests.

Related topics

- Using AdminP requests for handling Domino processes on page 122
- Automatically confirming AdminP requests on page 122

Mapping of Notes objects in One Identity Manager

You use One Identity Manager to manage all objects of the Domino that are required for the optimization of access control in the target system. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

Detailed information about this topic

Notes domains

In One Identity Manager, a domain corresponds to the image of a specific area in Domino, such as an operational Domino system. Using this construction, which is far more stringently handled in One Identity Manager than in Domino, it is possible to manage several productive Domino environments in parallel using a One Identity Manager database. Even if a user's relation to their domain is not maintained in Domino, One Identity Manager is capable of assigning the domain to each user account and thus to separate environments.

NOTE: The Synchronization Editor sets up the domains in the One Identity Manager database.

Related topics

- Editing main data of Notes domains on page 126
- Defining categories for the inheritance of Notes groups on page 128
- Editing the synchronization project for a Notes domain on page 128
- Editing search criteria for automatic employee assignment on page 79
- Synchronizing single objects on page 49

Editing main data of Notes domains

To edit the main data of a Notes domain

1. In the Manager, select the **HCL Domino > Domains** category.
2. Select the domain in the result list.
3. Select the **Change main data** task.
4. Edit the domain's main data.
5. Save the changes.

Related topics

- General main data for Notes domains on page 126
- Defining categories for the inheritance of Notes groups on page 128

General main data for Notes domains

Enter the following data on the **General** tab.

Table 28: General main data of a Notes domain

Property	Description
Full name	Full domain name.
Display name	The display name is used to display the domain in the user interface.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this domain and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for

Property	Description
	example.
Target system managers	Application role in which target system managers are specified for the domain. Target system managers only edit the objects from domains that are assigned to them. Each domain can have different target system managers assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this domain. Use the button to add a new application role.
Synchronized by	Type of synchronization through which data is synchronized between the domain and One Identity Manager. You can no longer change the synchronization type once objects for these domains are present in One Identity Manager. If you create a domain with the Synchronization Editor, **One Identity Manager** is used.
User ID file path	Path of the gateway server used for creating new user ID files. For more information, see Creating and saving user ID files on page 45.
Description	Text field for additional explanation.
ID vault enabled	Specifies whether Domino ID vault function is used to restore user ID files.

Table 29: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Domino connector	Domino connector
No synchronization	none	none

NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.

Related topics

- Account definitions for Notes user accounts on page 58
- Assigning Notes account definitions to target systems on page 75
- Target system managers for Domino domains on page 226
- Restoring user ID files on page 147

Defining categories for the inheritance of Notes groups

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the domain in the **HCL Domino > Domains** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. To enable the category, double-click  .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- Notes group inheritance based on categories on page 103

Editing the synchronization project for a Notes domain

Synchronization projects in which a domain is already used as a base object can also be opened in the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor:

1. In the Manager, select the **HCL Domino > Domains** category.
2. Select the domain in the result list.

3. Select the **Change main data** task.
4. Select the **Edit synchronization project** task.

Related topics

- Adjusting the synchronization configuration for Domino environments on page 33

Notes user accounts

Use the One Identity Manager to manage users and employee documents in Domino. These are mapped in the One Identity Manager database as Notes user accounts. All user accounts known to the Domino Directory are mapped. Users obtain access to network resources through membership in groups and through assigned policies.

When a user is added, the user ID file for authentication, the mailbox file and the user's personal address book are added. The mailbox file is created on the given mail server, the ID file and the personal address book are created on the gateway server.

If no certificate is assigned when a new user account is added in One Identity Manager, only the employee document is created in the target system. No user ID file, mailbox file nor personal address book is created.

Detailed information about this topic

- Creating and editing Notes user accounts on page 130
- Supported user account types on page 84
- Managing Notes user accounts and employees on page 57
- Assigning Notes groups directly to a Notes user account
- Assigning extended properties to Notes user accounts on page 140
- Specifying Notes user accounts as owners for documents on page 140
- Assigning owners to Notes user accounts on page 142
- Specifying Notes user accounts as administrators for documents on page 143
- Assigning administrators to Notes user accounts on page 145
- Maintaining excluded lists and additional lists for Notes user accounts on page 146
- The Notes user account overview on page 147
- Restoring user ID files on page 147
- Locking and unlocking Notes user accounts on page 150
- Deleting and restoring Notes user accounts on page 151
- Specify user types on page 43
- Creating mailbox files on page 43
- Creating and saving user ID files on page 45

Creating and editing Notes user accounts

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the main data described in the following is mapped through templates from employee main data.

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

To create a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Click in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

To manually assign a user account for an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign Notes user accounts** task.
4. Assign a user account.
5. Save the changes.

Detailed information about this topic

- General main data for Notes user accounts on page 131
- Additional main data of Notes user accounts on page 136
- Notes user account email system on page 134
- Notes user account address data on page 136
- Administrative data of Notes user accounts on page 137

Related topics

- Account definitions for Notes user accounts on page 58
- Supported user account types on page 84
- Managing Notes user accounts and employees on page 57
- Login information for Notes user accounts on page 108

General main data for Notes user accounts

Enter the following data on the **General** tab.

Table 30: General main data of a Notes user account

Property	Description
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click next to the input field and enter the required employee main data. Which login data is required depends on the selected identity type.
No link to an employee required	Specifies whether the user account is intentionally not assigned an employee. The option is automatically set if a user account is included in the exclusion list for automatic employee assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an employee (for example, if several employees use the user account). If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an employee can be filtered according to various criteria.
Not linked to an employee	Indicates why the **No link to an employee required** option is enabled for this user account. Possible values: • **By administrator**: The option was set manually by the administrator. • **By attestation**: The user account was attested.

Property	Description
	• **By exclusion criterion**: The user account is not associated with an employee due to an exclusion criterion. For example, the user account is included in the exclude list for automatic employee assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved. NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (`XOrigin=1`). Employee documents can also be created through account definitions.
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
First name	The user's first name.
Middle name	User's middle name.
Last name	The user's last name.
Short name	The user's short name.
Phonetic name	The user's name in phonetic letters.
Notes domain	User account's user account.
Certificate	Certificate with which the user ID file and the user's mailbox file will be registered (when first added) or were registered. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. No certificate is assigned to pure employee documents. If a certificate is not assigned when a new user account is saved, the certificate cannot be assigned later. If a certificate is assigned when a new user account is saved, the certificate cannot be removed later.

Property	Description
Organizational unit	Additional organization unit belonging to the user account.
Display name	User account display name. The display name is made up of the full name or the first and last names.
Title	User's title.
Generational affix	User's generational affix, for example, **Junior**.
Alternative language	Alternative language for the alternative names.
Alternative name	Alternative name in the user's local language. This can be used to display and search for names in the Domino environment. The alternative name has to linked to one of the user account`s alternative language.
Email system	Type of email system used by the user. **1 - Notes** is entered by default. The other input fields shown on the main data form depend on the type of email system selected.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
User account is disabled	Specifies whether the user account is blocked from logging in to the domain.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative permissions, used by one employee. • **Sponsored identity**: User account to use for a specific purpose. Training, for example. • **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this

Property	Description
	user account. • **Service identity**: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.

Related topics

- Account definitions for Notes user accounts on page 58
- Managing Notes user accounts and employees on page 57
- Supported user account types on page 84
- Notes user account email system on page 134
- Defining categories for the inheritance of Notes groups on page 128
- Locking and unlocking Notes user accounts on page 150

Notes user account email system

Select the email system that the user uses from the **Email system** menu on the general main data form. You have the following options:

- 1 - Notes
- 2 - cc:Mail
- 3 - Other
- 4 - X.400
- 5 - Other Internet Mail
- 6 - POP or IMAP
- 100 - None

  If no mail system is used, enter **None**.

The properties described in the following are displayed depending on the selected email system.

NOTE: Check whether the mail server and the mailbox file name are required for the selected email system. Enter the data necessary to create the mailbox file.

Table 31: Notes user account email system data

Email system	Property	Description
Notes POP or IMAP	Mail server	Notes server used as a mail server. All Notes servers marked with the **Has Notes mailbox files** option are available.
Notes	Mailbox template	Name of the Notes template to use for creating the mail-in database. The template determines which client version is used to create the mailbox file for a user. The template must exist on the gateway server. The data can be determined with the employee's IT operating data. If you do not enter a template, the template entered in **TargetSystem | NDO | DefTemplatePath** is used.
Notes POP or IMAP	Mailbox file	Name and path of the mailbox file. These are created using the template. The mailbox file is stored on the given mail server in a special directory under the installation directory. The directory name is given in the **TargetSystem | NDO | MailFilePath** configuration parameter. To use another directory, edit the value of this configuration parameter in the Designer.
Notes POP or IMAP	Mailbox file display name	Display name of the mailbox file. A template is used to make up the name from the first and last names and the postfix **Mailfile**.
Notes Other Other Internet Mail POP or IMAP	Forwarding address	Email address to which to forward messages. The email address must be complete (including domain).
Notes POP or IMAP	Message storage	Visible part of the mailbox storage. You have the following options: • **0 - Notes** • **1 - Notes and Internet Mail** • **2 - Internet Mail**

Email system	Property	Description
Notes cc:Mail Other Other Internet Mail POP or IMAP	Internet address	Complete SMTP address of the user account. The Internet address is used to identify the message recipient when a message is received through SMTP in the Domino environment. The Internet address is created from the employee's default email address depending on the manage level of the user account.
cc:Mail	cc:Mail post office	Post office containing the user's mailbox.
cc:Mail	cc:Mail user name	Mailbox's user name.
cc:Mail	cc:Mail location type	Location type of the mailbox. Select **LOCAL** or **REMOTE**.
X.400	X.400 server	Notes server used as X.400 server. All Notes servers marked with the **Has Notes mailbox files** option are available.
X.400	X.400 address	User's mail address in X.400 format (including domain name).

Detailed information about this topic

- Creating mailbox files on page 43

Notes user account address data

Enter the address and telephone information for contacting the employee that uses this user account on the **Company** and **Private** tabs. Enter other known data for describing the employee in more detail. This data is copied from the employee‘s main data depending on the manage level of the user account.

Additional main data of Notes user accounts

Enter the additional data for a user account on the **Miscellaneous** tab. This data is mainly for the mailbox file and message forwarding. You can find the size of a user account's mailbox on regular basis using a scheduled process plan. Prerequisite for this is that you enter the correct mail server data and the mailbox file path on the **General** tab.

To find out the size of the user account's mailbox file

- In the Designer, configure and enable the **Domino: Load mailbox file sizes** schedule.

  For more information about configuring schedules, see the *One Identity Manager Operational Guide*.

Table 32: Additional main data of a Notes user account

Property	Description
Size [KB]	Logical size of the mailbox file.
Physical size [KB]	Physical size of the mailbox file.
Max. size [KB]	Maximum permitted size of the mailbox.
Warn at [KB]	When this threshold is exceeded, users are sent an email.
Internet password/Password confirmation	The user's internet password. Web users must use this password for authentication on a Domino web server. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
Sametime server	Notes server used as a sametime server. Enter a sametime server for user accounts, which use the Domino sametime function.
Calendar domain	The domain that applies if the user account uses different calendar and schedule functionality.
Website	The user's website.
Comment	Text field for additional explanation.

Related topics

- Password policies for Notes user accounts on page 108

Administrative data of Notes user accounts

Enter the administrative data of a user account on the **Administration** tab.

Table 33: Administrative data for a Notes user account

Property	Description
Assigned policy	Policy that is explicitly assigned. You can assign a policy belonging to the same domain as the user account.

Property	Description
	NOTE: Policy settings basically replace all the user account settings.
Password check type	Specifies how users must authenticate themselves on the server. Password check types are: • **0 - don't check**: Do not check password The user must not provide a password to log in on the server. • **1 - check**: Check password The user must provide a password to log in to the server. • **2 - Lockout ID**: Lock the ID The user cannot log in on any server in the domain that checks passwords. When a new user account is created, the **0 - don't check** password check type is applied by default.
Password change interval	Interval for changing the password in days. After the password change interval has expired, the user is blocked from accessing servers until the password has been changed.
Time extension	Extension to the password change interval in days. If the password is not changed within the given extension period, the user cannot log in to the server anymore.
Last change date	Date on which the user account was last changed.
Internet password last change date	Last time the internet password was changed.
Password/Password confirmation	Password for the user account. The employee's central password can be mapped to the user account password. For more information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. No password is required for purely employee documents. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's

Property	Description
	requirements.
Change password at next login	Specifies whether the user account password must be changed on the next login.
Notes client license	License type of the Notes client. The license type determines the range of user access. Possible license types are: • **0 - HCL Domino** • **1 - HCL Domino Mail** • **2 - HCL Domino Desktop** • **3 - HCL Domino Designer** • **4 - HCL Domino Administration** • **5 - HCL iNotes®/Domino® CAL** When a new user account is created, the **0 - HCL Domino** license type is applied by default.
Setup profile	Name of the user configuration profile to apply when the working system is set up.
Allow foreign directory synchronization	Specifies whether the user name is synchronized with other systems.
User account	User account used for synchronizing between Domino and other systems, such as Active Directory.
Full name	Full name of the user account. Full name is made up of the first name, last name, certificate, and organizational unit.
ID expires	User ID file's expiry date. The expiry date is calculated using a template. User ID file for enabled user accounts that will expire in less that 10 days can be extended by two years. ***To extend the expiry date*** • In the Designer, configure and enable the **Automatically extend Domino ID expiry data** schedule. For more information about configuring schedules, see the *One Identity Manager Operational Guide*.

Related topics

- Notes server on page 188
- Password policies for Notes user accounts on page 108
- Initial password for new Notes user accounts on page 120

Assigning extended properties to Notes user accounts

Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager.

For more information about using extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To specify extended properties for a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click .
5. Save the changes.

Specifying Notes user accounts as owners for documents

Specify in which documents to enter the user account as owner. You can only assign documents belonging to the same domain as the user account.

To specify a user account as owner for user accounts

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To specify a user account as group owner

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Group** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

To specify a user account as owner for mail-in databases

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.

   TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

   To remove an assignment

   - Select the mail-in database and double-click .
6. Save the changes.

To specify a user account as certificate owner

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.

   TIP: In the **Remove assignments** pane, you can remove assigned certificates.

   To remove an assignment

   - Select the certificate and double-click .
6. Save the changes.

To specify a user account as owner for server documents

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Server document** tab.
5. In the **Add assignments** pane, assign server documents.

   TIP: In the **Remove assignments** pane, you can remove assigned server documents.

   To remove an assignment

   - Select the server document and double-click .
6. Save the changes.

Assigning owners to Notes user accounts

Specify which user accounts and groups are allowed to edit the selected user account.

To specify user accounts as owner

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To specify groups as owner

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign owner** task.
4. Select the **Group** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

6. Save the changes.

Specifying Notes user accounts as administrators for documents

Specify which documents the user account is allowed to administrate. You can only assign documents belonging to the same domain as the user account.

To specify a user account as administrator for user accounts

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify a user account as administrator for groups

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Group** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

To specify a user account as administrator for mail-in databases

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.

3. Select the **Assign administrable documents** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.

   TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

   To remove an assignment

   - Select the mail-in database and double-click ✓.
6. Save the changes.

To specify a user account as administrator for certificates

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.

   TIP: In the **Remove assignments** pane, you can remove assigned certificates.

   To remove an assignment

   - Select the certificate and double-click ✓.
6. Save the changes.

To specify a user account as administrator for servers

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

To specify a user account as administrator for server documents

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Server document** tab.

5. In the **Add assignments** pane, assign server documents.

   TIP: In the **Remove assignments** pane, you can remove assigned server documents.

   To remove an assignment

   - Select the server document and double-click .

6. Save the changes.

Assigning administrators to Notes user accounts

Specify which user accounts and groups are allowed to administrate the selected user account.

To specify user accounts as administrators

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrators** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify groups as administrators

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrators** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

Maintaining excluded lists and additional lists for Notes user accounts

Use this task to add the user account to additional and excluded lists for dynamic groups.

To add a user account to a dynamic group's additional list

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Additional** tab.
5. In the **Add assignments** pane, assign groups with an additional list that will contain the user account as a member.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

To add a user account to a dynamic group's excluded list

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Excluded** tab.
5. In the **Add assignments** pane, assign groups with an excluded list that will contain the user account as a member.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Related topics

- Memberships in dynamic groups on page 166

The Notes user account overview

Use this task to obtain an overview of the most important information about a user account.

To obtain an overview of a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select **Notes user account overview** category.

Restoring user ID files

If a user has forgotten the password to a user account and lost the user ID file, the user ID file can be restored. Since Domino version 8.5, Domino provides the ID vault function to do this.

One Identity Manager uses **ID restore** to provide its own method for restoring the user ID files. This can be used if an older version of Domino is in use or if ID Vault should not be used.

NOTE: The method to be used for restoring user ID files is specified by the domain. This option is valid for all user accounts in the domain.

Detailed information about this topic

- Restoring user ID files using ID vault on page 147
- Restoring user ID files through ID restore on page 149

Restoring user ID files using ID vault

The ID vault is a Domino database that stores copies of user ID files. This allows Domino to be able to restore user ID files and to reset user account passwords. One Identity Manager provides a process for resetting the passwords in the ID vault.

Prerequisites

- The Domino server that communicates with the gateway server, is also the ID vault server.
- There are running permissions defined for agents for the synchronization user account. For more information, see Running restricted LotusScript/Java agents on page 212.

- ID vault database permissions for the synchronization user account are set to: **Manager** access function and **Auditor** role. For more detailed information, see your Domino documentation.
- Permissions for restoring passwords of the synchronization administrative user account and the ID vault server are set. For more detailed information, see your Domino documentation.

To use the ID vault

1. In the Manager, select the **HCL Domino > Domains** category.
2. Select the domain you want to use for the ID vault in the result list and run the **Change main data** task.
3. Set the **ID vault enabled** option.

   This setting effects all user accounts in the domain.
4. Save the changes.

NOTE: If certain user accounts are excluded from the ID vault by the ID vault policy in Domino, the password cannot be reset by One Identity Manager.

In order to ensure the passwords for all user accounts in a domain can be reset, assign a policy for ID Vault that cover the whole organization.

When a new user account is published in Domino, One Identity Manager saves the initial password in the One Identity Manager database (`NDOUser.PasswordInitial`). This initial password is used when a user account password needs to be reset. Passwords are saved automatically for user accounts that are initially setup in One Identity Manager. The initial password for all other user accounts has to be transferred to the One Identity Manager database by a customized process.

To reset a user account password

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **ID restore** task.

This task starts the `NDO_NDOUser_PWReset_from_Vault` process. This process replaces the password from the user ID file saved in the ID Vault with the initial password from the One Identity Manager database. If the user is logged into the Notes client at this point, the user`s local ID file is replaced with the update copy from the ID Vault. The user has to login with the initial password when the Notes client is started the next time. If the user is not logged into the Notes client when the password is reset, the updated ID file must be provided separately.

Once the password has been successfully reset, the user must be provided with initial password and the ID file if necessary. This process has to be customized to meet your needs.

Restoring user ID files through ID restore

ID restore is a One Identity Manager mechanism that can be used when a user has forgotten his password or the ID file itself has been lost. If the user ID file is restored with the ID restore procedure, the full name of the user account and the display name are determined from the user account name, organizational unit and certificate.

The following information is required to run an ID restore:

- An ID file that is initially imported into the database including the associated password (`NotesUser.NotesID`, `NotesUser.PasswordInitial`)
- The certifier that the initial ID file was created with (`NotesUser.UID_NotesCertifierInitial`)
- A copy of the initially loaded or added employee document in the gateway server's archive database `archiv.nsf`
- The GUID of the document copy in the archive database (`NotesUser.ObjectGUID_Archiv`)

This data is automatically generated and saved for the user accounts that were added in the One Identity Manager. A one-off custom import of the files mentioned above has to be run for all other user accounts.

To restore the user ID file

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **ID restore** task.

   The ID restore process carries out the following steps:

   - Deletes all current employee documents from the Domino directory.
   - Copies initial employee documents from archive database to the Domino directory.
   - Exports the initially saved ID files to the gateway server.
   - Starts the AdminP request to track the changes made to the original ID up until now. This includes changes to the components of the user's name, changes to the ID expiry date and exchanging certifiers.
   - Update the restored employee document using the known values.
4. If the ID file is restored, provide the user with the ID file and the initial password.

Related topics

- Setting up an archive database for backing up employee documents on page 26

Locking and unlocking Notes user accounts

A user is considered to be locked in Domino if it is no longer possible for the user to log on to a server in the domain with this user account. The user loses access to the mailbox file through this. Access to a server can be prevented if the user account has the **Not access server** permissions type for the corresponding server document. This is very complicated in environments with several servers because a user account, which is going to be locked, must be given this permissions type for every server document.

For this reason, denied access groups are used. Each denied access group initially gets the **Not access server** permissions type for each server document. A user that is going to be locked becomes a member of the denied access group and therefore is automatically prevented from accessing the domain servers.

The way you lock user accounts depends on how they are managed.

Scenario:

The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `NDOUser.AccountDisabled` column.

Scenario:

The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the employee's user accounts are locked when the employee is permanently or temporarily disabled.
- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To lock the user account when the configuration parameter is disabled

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Scenario:

User accounts not linked to employees.

To lock a user account that is no longer linked to an employee

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

The user account becomes anonymous when it is locked and is not shown in address books. Access to Notes servers is removed. The **TargetSystem | NDO | MailBoxAnonymPre** configuration parameter is checked if the user is made anonymous.

To unlock a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Disable the **Account is disabled** option on the **General** tab.
5. Save the changes.

   Anonymity is rescinded and the user account removed from denied access groups.

Detailed information about this topic

- Locking groups on page 164

Related topics

- Account definitions for Notes user accounts on page 58
- Creating manage levels on page 63

Deleting and restoring Notes user accounts

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted.

You can delete a user account that was not created using an account definition through the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. Depending on the deferred deletion setting, the user account is either deleted immediately from the address books and the One Identity Manager database or at a later date.

For more information about deactivating and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

To delete a user account that is not managed using an account definition

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. In the Manager, select the **HCL Domino > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.

Related topics

- Locking and unlocking Notes user accounts on page 150
- Specifying deferred deletion for Notes user accounts on page 90

Notes groups

You manage groups in a Domino environment with One Identity Manager. These are mapped in the One Identity Manager database as Notes groups. All groups known to the Domino Directory are mapped. Users obtain access to network resources through membership in groups and through assigned policies.

Users, mail-in databases, groups, and servers can be grouped together into groups. Domino divides groups into different group types. The group's type specifies its intended purpose and whether it is visible in the Domino Directory.

Detailed information about this topic

- Creating Notes groups on page 153
- Editing main data of Notes groups on page 153
- Deleting Notes groups on page 170
- Locking groups on page 164
- Dynamic groups on page 165
- Assigning Notes user accounts directly to a Notes group on page 99
- Assigning Notes mail-in databases to Notes groups on page 155
- Assigning Notes servers to Notes groups on page 156
- Adding Notes groups to Notes groups on page 157
- Specifying Notes groups as document owners on page 158
- Specifying Notes groups as document administrators on page 160

- Assigning owners to Notes groups on page 162
- Assigning administrators to Notes groups on page 163
- Assigning extended properties to Notes groups on page 163
- Displaying the Notes group overview on page 164

Creating Notes groups

To create a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Click in the result list.
3. On the main data form, edit the main data of the group.
4. Save the changes.

Detailed information about this topic

- General main data for Notes groups on page 154

Related topics

- Deleting Notes groups on page 170
- Editing main data of Notes groups on page 153

Editing main data of Notes groups

To edit group main data

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Detailed information about this topic

- General main data for Notes groups on page 154

Related topics

- Deleting Notes groups on page 170
- Creating Notes groups on page 153

General main data for Notes groups

Edit the following data for groups.

Table 34: General main data of a Notes group

Property	Description
Group	Name of the group.
Display name	Display name of the group.
Notes domain	Domain in which the group is managed.
Group type	Purpose of the group. The group type defines the visibility of the group in the Domino Directory. Applicable group types are: • **0 - Multi-purpose** • **1 - Mail only** • **2 - ACL only** • **3 - Deny list only** • **4 - Servers only**
Parent Notes group	Unique identifier of the dynamic group to which the extension group belongs. This property is maintained for all extension groups in a dynamic group.
Service item	Service item data for requesting the group through the IT Shop.
Internet address	Internet email address of the group.
Notes category	Categorizes the group further. To create a new Notes category, click .
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.

Property	Description
Import dynamic members	Method for specifying members of a dynamic group. • **Home server**: The group members are determined dynamically from the homer server's members. Excluded and additional lists are synchronized for this group. • **None**: The group is not a dynamic group.
Description	Text field for additional explanation.
Allow foreign directory synchronization	Specifies whether the information about this group can be forwarded to a foreign directory.
Locked group	Specifies whether the group is set as a denied access group.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles. The option cannot be set if the group is a dynamic group.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Dynamic group	Specifies whether this is a dynamic group. This option is set depending on the setting of **Import dynamic members**.

Detailed information about this topic

- Extension groups on page 166
- Dynamic groups on page 165
- Locking groups on page 164
- Defining categories for the inheritance of Notes groups on page 128
- Adding Notes groups to the IT Shop on page 98

Assigning Notes mail-in databases to Notes groups

You can assign mail-in databases directly to a group.

To assign mail-in databases to a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.
    - (Optional) To filter the mail-in databases, select a domain in the **Notes domains** input field.

    TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

    To remove an assignment

    - Select the mail-in database and double-click .
6. Save the changes.

Related topics

- Assigning Notes user accounts directly to a Notes group on page 99
- Assigning Notes servers to Notes groups on page 156
- Adding Notes groups to Notes groups on page 157
- Assigning mail-in databases to Notes groups on page 184

Assigning Notes servers to Notes groups

You can assign Notes servers directly to a group.

To assign servers to a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers.
    - (Optional) To filter the servers, select a domain in the **Notes domains** input field.

    TIP: In the **Remove assignments** pane, you can remove assigned servers.

To remove an assignment

- Select the server and double-click ✓.

6. Save the changes.

Related topics

- Assigning Notes user accounts directly to a Notes group on page 99
- Assigning Notes mail-in databases to Notes groups on page 155
- Adding Notes groups to Notes groups on page 157

Adding Notes groups to Notes groups

You can assign parent or child groups to a Notes group.

To assign child groups

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign child groups.
    - (Optional) To filter the groups, select a domain in the **Notes Domains** input field.

    TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

    To remove an assignment

    - Select the child group and double-click ✓.
6. Save the changes.

To assign parent groups

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign parent groups** task.
4. In the **Add assignments** pane, assign parent groups.
    - (Optional) To filter the groups, select a domain in the **Notes Domains** input field.

    TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the parent group and double-click ✓.

5. Save the changes.

Related topics

- Assigning Notes user accounts directly to a Notes group on page 99
- Assigning Notes servers to Notes groups on page 156
- Assigning Notes mail-in databases to Notes groups on page 155

Specifying Notes groups as document owners

Specify in which documents to enter a group as owner. You can only assign documents belonging to the same domain as the group.

To specify a group as user account owner

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.

6. Save the changes.

To specify a group as group owner

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click ✓.

6. Save the changes.

To specify a group as mail-in database owner

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select **Mail-in DB**.
5. In the **Add assignments** pane, assign mail-in databases.

   TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

   To remove an assignment

   - Select the mail-in database and double-click ✓.

6. Save the changes.

To specify a group as certificate owner

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.

   TIP: In the **Remove assignments** pane, you can remove assigned certificates.

   To remove an assignment

   - Select the certificate and double-click ✓.

6. Save the changes.

To specify a group as server owner

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

To remove an assignment

- Select the server and double-click .

6. Save the changes.

Specifying Notes groups as document administrators

Specify which documents the group should administrate. You can only assign documents belonging to the same domain as the group.

To specify a group as administrator for user accounts

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify a group as administrator for groups

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

To specify a group as administrator for mail-in databases

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.

3. Select the **Assign administrable documents** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.

   TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

   To remove an assignment

   - Select the mail-in database and double-click ✓.
6. Save the changes.

To specify a group as administrator for certificates

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.

   TIP: In the **Remove assignments** pane, you can remove assigned certificates.

   To remove an assignment

   - Select the certificate and double-click ✓.
6. Save the changes.

To specify a group as administrator for server documents

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Server document** tab.
5. In the **Add assignments** pane, assign server documents.

   TIP: In the **Remove assignments** pane, you can remove assigned server documents.

   To remove an assignment

   - Select the server document and double-click ✓.
6. Save the changes.

To specify a group as administrator for servers

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.

4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Assigning owners to Notes groups

Specify which user accounts and groups are allowed to edit the selected group.

To specify user accounts as owner of a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as owner of a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign owner** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Assigning administrators to Notes groups

Specify which user accounts and groups are allowed to administrate the selected Notes group.

To specify user accounts as administrators for groups

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrators** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as administrators for groups

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrators** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Assigning extended properties to Notes groups

Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager.

For more information about setting up extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To specify extended properties for a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click ✓.
5. Save the changes.

Displaying the Notes group overview

Use this task to obtain an overview of the most important information about a group.

To obtain an overview of a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Select the **Notes group overview** task.

Locking groups

A user is considered to be locked in Domino if it is no longer possible for the user to log on to a server in the domain with this user account. The user loses access to the mailbox file through this. Access to a server can be prevented if the user account has the **Not access server** permissions type for the corresponding server document. This is very complicated in environments with several servers because a user account, which is going to be locked, must be given this permissions type for every server document.

For this reason, denied access groups are used. Each denied access group initially gets the **Not access server** permissions type for each server document. A user that is going to be locked becomes a member of the denied access group and therefore is automatically prevented from accessing the domain servers.

Immediately after a user account has been locked in One Identity Manager, a denied access group is found for the user. If a denied access group of the right type is not found, the One Identity Manager Service creates a new group, **Deny list only**, and automatically stores it on each server with **Not access server**. The group name is made up of a prefix and a sequential index (for example **viDenyAccess0001**). Furthermore, this group is labeled with **Denied access group>**.

To change the prefix of an denied access group.

1. In the Designer, edit the value in the **TargetSystem | NDO | DenyAccessGroups | Prefix** configuration parameter.
2. Enter the prefix when a denied access group is initially created.
3. Save the changes.

It is also possible to specify the maximum number of user accounts in a denied access group. This is necessary in an environment with a large number of user accounts to prevent the maximum number of user names in one group being exceeded. If this limit is reached, a new denied access group is created with an index value incremented by **1** and added with the permissions type **Not access server** on all domain servers.

To change the number of user accounts permitted in a denied access group

- In the Designer, edit the value in the **TargetSystem | NDO | DenyAccessGroups | Memberlimit** configuration parameter.

TIP: The denied access groups are found using the `VI_Notes_GetOrCreateRestrictGroup` script and then added. If denied access groups already exist in Domino, they are handled like normal groups.

To use these groups for the locking process in One Identity Manager

1. In the Manager, set the **Locking group** option for this group.
2. In the Designer, modify the prefix in **TargetSystem | NDO | DenyAccessGroups | Prefix** if necessary.
3. Modify the `NDO_Notes_GetOrCreateRestrictGroup` script according to your requirements.

Dynamic groups

Since Domino version 8.5, it is possible to assign user accounts to groups by certain selection criteria. A criteria is, for example, the user account's mail server. Furthermore, members can be explicitly excluded or additionally added to the group. A group is mapped as a dynamic group in One Identity Manager, if **Home server** is selected in **Load dynamic member** (column `AutoPopulateInput = '1'`). Members cannot be assigned directly to these groups.

Dynamic groups are excluded from inheritance through hierarchical roles. This means that system roles, business roles, and organizations cannot be assigned to dynamic groups. Inheritance exclusion cannot be defined and dynamic groups cannot be requested in the IT Shop.

Detailed information about this topic

- Extension groups on page 166
- Memberships in dynamic groups on page 166

- Assigning home servers on page 167
- Editing the excluded list on page 167
- Editing the inclusion list on page 169
- Maintaining excluded lists and additional lists for Notes mail-in databases on page 186
- Maintaining excluded lists and additional lists for Notes user accounts on page 146

Extension groups

If the maximum number of members in a group has been reached, Domino adds so called extension groups. These extension groups are imported into the One Identity Manager database by synchronization and cannot be edited. The connection to the dynamic group is created using the **Parent Notes group** property (`UID_NotesGroupParent` column). Excluded and additional lists are maintained exclusively for parent dynamic groups. Extension groups are only shown on the overview form.

Memberships in dynamic groups

You cannot assign members directly to dynamic groups. Members are determined over the home servers assigned to the group. All user accounts that are assigned as mail server to this server are automatically members of the dynamic group. In addition, memberships can be edited through an excluded and additional list. At the same time, user accounts that are assigned to both the excluded and additional lists cannot be members of the dynamic group. User accounts and groups can both be added to the excluded and additional lists.

When Domino is calculating effective members, it finds all the user accounts that:

- The home server is assigned to as mail server
- Are directly assigned to an additional list
- Are assigned to an additional list as a member of a Notes group
- Are assigned to an excluded list
- Are assigned to an excluded list as a member of a Notes group.

Effective memberships in dynamic groups (table `NDOUserInGroup`) are not maintained in One Identity Manager, but only loaded in the One Identity Manager by synchronization. Excluded and additional lists can be edited in the Manager. Changes are immediately provisioned in the target system. Membership lists are recalculated there. After resynchronizing, the changes to the effective memberships are visible in One Identity Manager and can be taken into account by, for example, compliance checking.

If you use One Identity Manager's identity audit functionality and also check memberships in dynamic Notes groups in compliance rules, note the following:

> NOTE: Changes to the excluded and additional lists in the Manager, cannot be immediately acted upon as effective memberships in dynamic groups are not updated

until after resynchronization. Customize the synchronization schedule for your Domino environment such that changes to effective memberships are promptly transferred to the One Identity Manager database.

For more information about editing synchronization schedules, see the *One Identity Manager Target System Synchronization Reference Guide*.

Assigning home servers

You can assign home servers to dynamic groups. All user accounts, only using this server as mail server become members of the dynamic group.

To assign a home server to a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Assign home server** task.
4. In the **Add assignments** pane, assign the servers.
    - (Optional) To filter the servers, select a domain in the **Notes domains** input field.

    TIP: In the **Remove assignments** pane, you can remove assigned servers.

    To remove an assignment

    - Select the server and double-click .
5. Save the changes.

Editing the excluded list

Use the excluded list to specify which objects you want to exclude from membership in a dynamic group.

To exclude user accounts from a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Users** tab.
5. Assign user accounts in **Add assignments**.

    TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

To remove an assignment

- Select the user account and double-click .

6. Save the changes.

To exclude groups from a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

To exclude servers from a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click .

6. Save the changes.

To exclude mail-in databases from a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.

   TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

To remove an assignment

- Select the mail-in database and double-click .

6. Save the changes.

Editing the inclusion list

Use the additional list to specify which objects you want to additionally include in membership in a dynamic group.

To add additional user accounts to a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Users** tab.
5. Assign user accounts in **Add assignments**.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To add additional groups to a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

To add additional servers to a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.

4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click .
6. Save the changes.

To add additional mail-in databases to a dynamic group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.

   TIP: In the **Remove assignments** pane, you can remove assigned mail-in databases.

   To remove an assignment

   - Select the mail-in database and double-click .
6. Save the changes.

Deleting Notes groups

Groups are deleted permanently from the One Identity Manager database and from the Domino address book.

To delete a group

1. In the Manager, select the **HCL Domino > Groups** category.
2. Select the group in the result list.
3. Click in the result list.
4. Confirm the security prompt with **Yes**.

Notes certificates

You manage certificates in Domino with One Identity Manager. These are mapped in the One Identity Manager database as Notes certificates. All certificates known to the Domino directory are mapped.

Certificates are loaded into the One Identity Manager database through synchronization so they can be referenced when new user accounts are added. User accounts that are added with One Identity Manager contain a reference to the certificate in use. This means you can recover their ID files with this certificate at anytime. The certificate is the deciding factor for mapping more user account properties when managing user accounts with account definitions.

You can only synchronize Domino directory certificates. If a user in the target system has been created with an external certificate, One Identity Manager cannot determine the certificate and therefore cannot allocate it to the user account.

Detailed information about this topic

- Editing main data of Notes certificates on page 171
- Assigning owners to Notes certificates on page 173
- Assigning administrators to Notes certificates on page 174
- Displaying the Notes certificate overview on page 174
- Post-processing new Notes certificates on page 175
- Displaying Notes certificate requests on page 175

Editing main data of Notes certificates

To edit a certificate's main data

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list.
3. Select the **Change main data** task.
4. Enter the required data on the main data form.
5. Save the changes.

Detailed information about this topic

- General main data for Notes certificates on page 172
- Notes certificates contact data on page 172

General main data for Notes certificates

Enter the following data on the **General** tab.

Table 35: General main data of a Notes certificate

Property	Description
Full name	Full name of the certificate.
Parent certifier	Unique ID for the parent certifier. Enter the name of the issuer of the certificate.
Notes domain	Unique domain name.
Notes server	Notes server on which the certifier's mailboxes are stored.
Mailbox file	Path to the certifier's mailbox file.
ID file name (including path)	Name and path of the certificate's ID file. If user accounts should be registered with the certificate, enter the full path of the certifier's ID file. The directory to save the ID file in, must be reachable by the gateway server. This data is only required if the **CA process possible** option is disabled.
Password and password confirmation	Password of the certifier's ID file. This data is only required if the **CA process possible** option is disabled.
CA process possible	Specifies whether the CA process is used for certifying user accounts. If this option is not set, a certifier ID file is required for certification.
CA database server	Server which provides the CA database for this certificate. This data is only required if the **CA process possible** option is enabled.
CA database name	Name or path of the CA database file. This data is only required if the **CA process possible** option is enabled.
Due date	Certificate expiry date.
Certificate type	Type of certificate.

Notes certificates contact data

Enter the certifier's contact data on the **Contact** tab.

Table 36: Notes certifier's contact data

Property	Description
Company	Certifier's company.
Department	Certifier's department.
Location	Certifier's location.
Email address	Certifier's email address.
Phone, office	Certifier's office telephone number.
Comment	Text field for additional explanation.

Assigning owners to Notes certificates

Specify which user accounts and groups are entered as certificate document owners.

To specify user accounts as owners of a certificate

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To specify groups as owners of a certificate

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

6. Save the changes.

Assigning administrators to Notes certificates

Specify which user accounts and groups are allowed to administrate the certificate document.

To specify user accounts as administrators for a certificate

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify groups as administrators for a certificate

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

Displaying the Notes certificate overview

Use this task to obtain an overview of the most important information about a certificate.

To obtain an overview of a certificate

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list.
3. Select **certificate overview**.Notes

Post-processing new Notes certificates

To add new users with One Identity Manager or to recertify existing users, copy the new certificate to the synchronization user's personal address book on a regular basis.

To use new certificates for registering user accounts

1. Copy the certificates from the Domino directory in the synchronization user's personal address book.
2. Check whether the certificate ID files are reachable from the gateway server.
3. Enter the name and path of the certificate ID file on the gateway server in the certificate's main data in One Identity Manager. This data is only required for certificates that are not used by the CA process.

Related topics

- Copying Notes certificates on page 22
- General main data for Notes certificates on page 172

Displaying Notes certificate requests

Certificate requests are mapped in One Identity Manager for all documents that were certified using the CA process. All certificate requests for a certificate are displayed on the certificate's overview form.

To display a certificate request's properties

1. In the Manager, select the **HCL Domino > Certificates** category.
2. Select a certificate in the result list. Select the **Notes certificate overview** task.
3. Select a certificate request on the **Notes certificate requests** form element.
4. Select the **Change main data** task.

Table 37: Notes certificate request main data

Property	Description
Object	Name of the certified object.
CA certificate	Name of the certificate to use for certification.
Staff	Name of the official certifier.
Certificate	Unique certificate identifier.
Notes domain	Certificate request's domain.
State of request	Current state of the certificate request.

Notes templates

You use One Identity Manager to manage templates in Domino. These are mapped in the One Identity Manager database as Notes templates. All templates known to the Domino Directory are mapped. To allow the Domino connector to add users in the target system, you must add a template to the user account specifying which template to use when the user's mailbox is created.

To obtain an overview of a template

1. In Manager, select the **HCL Domino > Notes templates** category.
2. Select the template in the result list.
3. Select the **Notes template overview** task.

To edit a template's main data

1. In Manager, select the **HCL Domino > Notes templates** category.
2. Select the template in the result list.
3. Select the **Change main data** task.
4. Enter the required data on the main data form.
5. Save the changes.

Table 38: Notes template main data

Property	Description
Notes template	Template name.
Notes domain	Domain in which to apply the template.
File Name	Name of the template file.

Notes policies

You use One Identity Manager to manage policies in Domino. These are mapped in the One Identity Manager database as Notes policies. All policies known to the Domino Directory are mapped.

You can use policies to specify settings to apply to users and groups. Policies and policy settings are loaded into the One Identity Manager database during synchronization and can be assigned to user accounts. The policies can be assigned to user accounts and groups as members, owners, or administrators.

Detailed information about this topic

- Displaying Notes policies main data on page 177
- Displaying Notes policy settings on page 178
- Assigning members to Notes policies on page 179
- Assigning owners to Notes policies on page 180
- Assigning administrators to Notes policies on page 180
- Displaying the Notes policy overview on page 181

Displaying Notes policies main data

To display policy main data

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

Detailed information about this topic

- Notes policy main data on page 177

Notes policy main data

Following information about policies is displayed.

Table 39: Notes policy main data

Property	Description
Name	Name of the policy.
Full name	The policy's full name.
Parent policy	Policy above this one in the hierarchy.
Description	Description of the policy.
Policy type	Type of policy.
Category	Category of the policy.
Explicit policy	Specifies whether the policy settings are ignored by other policies.
Archive policy	Assigned archive policy setting.
Desktop policy	Assigned desktop policy setting.
Mail policy	Assigned mail policy setting.
Registration policy	Assigned registration policy setting.
Security policy	Assigned security setting.
Set up policy	Assigned set up policy setting.

Displaying Notes policy settings

The policy settings mapped in One Identity Manager are those used in synchronized Notes policies.

To display policy settings main data

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select a policy in the result list.
3. Select the **Change main data** task.
4. Select an assigned policy setting and open the context menu.
5. Click **Go to assigned object**.
6. Select the **Change main data** task.

Table 40: Main data of a Notes policy setting

Property	Description
Full name	Full name of the policy setting.

Property	Description
Description	Describes the policy setting.
Setting type	Type of policy setting.
Notes domain	Policy setting domain.

Related topics

- Notes policy main data on page 177

Assigning members to Notes policies

Assign the user accounts and groups to which the policy will apply.

To assign user accounts to a policy

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Assign members** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To assign groups to a policy

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Assign members** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

Assigning owners to Notes policies

You can define owner relations for policies. To do this, specify which user accounts and groups are permitted to edit the policy.

To specify user accounts as owner

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To specify groups as owner

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

Assigning administrators to Notes policies

You can define administrator relations for policies. To do this, specify which user accounts and groups are permitted to manage the policy.

To specify user accounts as administrators

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.

3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as administrators

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Displaying the Notes policy overview

Use this task to obtain an overview of the most important information about a policy.

To obtain an overview of a policy

1. In the Manager, select the **HCL Domino > Policies** category.
2. Select the policy in the result list.
3. Select the **Notes policy overview** task.

Notes mail-in databases

You manage mail-in databases in Domino with One Identity Manager. These are mapped in the One Identity Manager database as Notes mail-in databases. All mail-in databases known to the Domino Directory are mapped.

Mail-in databases can be directly assigned to groups and become members of dynamic groups. The mail-in databases can be assigned to user accounts and groups as owners or administrators.

Detailed information about this topic

- Creating Notes mail-in databases on page 182
- Editing main data for Notes mail-in databases on page 183
- Deleting Notes mail-in databases on page 187
- Display the Notes mail-in database overview on page 187
- Assigning mail-in databases to Notes groups on page 184
- Assigning owners to Notes mail-in databases on page 184
- Assigning administrators to Notes mail-in databases on page 185
- Maintaining excluded lists and additional lists for Notes mail-in databases on page 186

Creating Notes mail-in databases

To create a mail-in database

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Click in the result list.
3. Edit the mail-in database's main data.
4. Save the changes.

Detailed information about this topic

- General main data of Notes mail-in databases on page 183

Related topics

- Editing main data for Notes mail-in databases on page 183
- Deleting Notes mail-in databases on page 187

Editing main data for Notes mail-in databases

To edit mail-in database main data

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Change main data** task.
4. Edit the mail-in database's main data.
5. Save the changes.

Detailed information about this topic

- General main data of Notes mail-in databases on page 183

Related topics

- Creating Notes mail-in databases on page 182
- Deleting Notes mail-in databases on page 187

General main data of Notes mail-in databases

Enter the following data for mail-in databases:

Table 41: General main data of a mail-in database

Property	Description
Mail-in DB	Name of the mail-in database.
Display name	Display name for the mail-in database
Notes domain	Domain in which the mail-in database is managed.
Notes server	Full name of the Notes server where the mail-in database is stored.
Internet address	SMTP address with the format `mailfile@organization.domain`.
File Name	File name and path of the mail-in database relative to the Domino directory.

Property	Description
Message storage	Type of message storage.
Allow foreign directory synchronization	Specifies whether entries in the mail-in database can be viewed in the foreign directory.
Encrypt incoming post	Specifies whether incoming emails are encrypted.
Notes template	Name of the template to use for creating the mail-in database.
Description	Text field for additional explanation.

Assigning mail-in databases to Notes groups

To set up permissions for accessing mail-in databases, you assign Notes groups to the mail-in databases.

To assign groups to a mail-in database

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign the groups.
   - (Optional) To filter the groups, select a domain in the **Notes Domains** input field.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment
   - Select the group and double-click ✓.
5. Save the changes.

Related topics

- Assigning Notes mail-in databases to Notes groups on page 155

Assigning owners to Notes mail-in databases

You can define owner relations for mail-in databases. To do this, specify which user accounts and groups are permitted to edit the mail-in database.

To specify user accounts as owner

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as owner

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Assigning administrators to Notes mail-in databases

You can define administrator relations for mail-in databases. To do this, specify which user accounts and groups are permitted to manage the mail-in database.

To specify user accounts as administrators

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

To remove an assignment

- Select the user account and double-click .

6. Save the changes.

To specify groups as administrators

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

Maintaining excluded lists and additional lists for Notes mail-in databases

Mail-in databases can be members of dynamic groups. Use the excluded list to specify which mail-in databases you want to exclude from membership in a dynamic group. Use the additional list to specify which mail-in databases you want to additionally include in membership in a dynamic group.

To add a mail-in database to a dynamic group's additional list

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Additional** tab.
5. In the **Add assignments** pane, assign groups with an additional list that will contain the mail-in database.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click ✓.

6. Save the changes.

To add a mail-in database to a dynamic group's excluded list

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Excluded** tab.
5. In the **Add assignments** pane, assign groups with an excluded list that will contain the mail-in database.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.

6. Save the changes.

Related topics

- Memberships in dynamic groups on page 166

Display the Notes mail-in database overview

Use this task to obtain an overview of the most important information about a mail-in database.

To obtain an overview of a mail-in database

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Select **Notes mail-in database overview**.

Deleting Notes mail-in databases

Mail-in databases are deleted permanently from the One Identity Manager database and from the Domino address book.

To delete a mail-in database

1. In the Manager, select the **HCL Domino > Mail-in databases** category.
2. Select a mail-in database in the result list.
3. Click .
4. Confirm the security prompt with **Yes**.

Notes server

You use One Identity Manager to manage servers in Domino. These are mapped in the One Identity Manager database as Notes servers. All servers known to the Domino Directory are mapped.

Detailed information about this topic

- Signing or running unrestricted methods and operations on page 211
- Running restricted LotusScript/Java agents on page 212
- Running simple agents and formula agents on page 213
- Maintaining excluded lists and additional lists on page 214
- Displaying the Notes server overview on page 215

Editing main data of Notes servers

To edit the main data of a Notes server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Change main data** task.
4. Enter the required data on the main data form.
5. Save the changes.

Detailed information about this topic

- General main data for Notes servers on page 189
- Notes server location data on page 190
- Notes server security settings on page 191

Related topics

- Deleting Notes servers on page 215

General main data for Notes servers

Enter the following general main data of Notes servers.

Table 42: General main data of a Notes server

Property	Description
Notes server	Hierarchical name of the server in the Domino directory.
Title	Additional name of the server. You can enter more than one value.
Notes domain	Notes domain to which the server belongs.
Version	Notes build version of the server.

Property	Description
User ID file path	Path of the gateway server used for creating new user ID files. For more information, see Creating and saving user ID files on page 45.
Has Notes mailbox file	Specifies whether mailbox files are managed on the server. This server is available for selection as mail servers when users are set up.
Mailbox file path	Mailbox file repository path relative to the data directory. This data is only required if the **Has Notes mailbox files** option is enabled.
Server document	Specifies whether the Notes server only corresponds to a server document in the Domino Directory and does not exist physically.
Cluster name	Name of the cluster if the server belongs to a cluster.
DNS server name	Full name of the server.
Load internet configuration	Specifies whether the internet protocol configuration is loaded from the internet site documents in the Domino directory. If this option is not set, the information is taken from the server document.
Starts SMTP service automatically	Specifies whether the SMTP service is started automatically when the server is started.
Operating system	Name of the operating system installed.
Formula processing time	The maximum time, in seconds, that a formula can run.
Is vault server	Specifies whether this server is used as an ID vault server.

Related topics

- Notes server location data on page 190
- Notes server security settings on page 191
- Editing main data of Notes servers on page 189

Notes server location data

Edit location data for Notes servers on the **Location** tab.

Table 43: Location data for a Notes servers

Property	Description
Phone	Telephone number in case the server can take calls over a modem.
Time zone difference w.r.t. GMT	Local time zone at server's location. This is given as the different to coordinated universal time (UTC).
Daylight saving time	Specifies whether summertime applies at the server's location.
Mail server	Mail server used at the server's location.
Passthru server	Passthru server used at the server's location. Corresponds to the home server.

You can find more location information on the **Contact** tab.

Table 44: Contact data for a Notes server

Property	Description
Location	Server's location.
Department	Server's department.
Comment	Text field for additional explanation.
Detailed description	Text field for additional explanation.

Related topics

- General main data for Notes servers on page 189
- Notes server security settings on page 191
- Editing main data of Notes servers on page 189

Notes server security settings

Edit a server's security settings on the **Security** tab.

Table 45: Security settings for a Notes server

Property	Description
Compare public keys with keys in Domino Directory	Specifies whether public keys of all users and servers must be checked once they have logged in to the server.

Property	Description
Permit anonymous connections	Specifies whether users and servers without valid certificates can log in to the server.
Examine ID file passwords	Specifies whether user ID file passwords are checked when the users log in to the server.

Related topics

- General main data for Notes servers on page 189
- Notes server location data on page 190
- Editing main data of Notes servers on page 189

Assigning Notes servers to Notes groups

You can add servers to a group as members.

To add a Notes server to a group

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign groups**.
4. In the **Add assignments** pane, assign the groups.
   - (Optional) To filter the groups, select a domain in the **Notes Domains** input field.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
5. Save the changes.

Related topics

- Assigning Notes servers to Notes groups on page 156

Assigning mail servers to Notes user accounts

Notes servers can be assigned directly to user accounts as mail servers. The server is entered in all selected user accounts as mail server (column `UID_NDOServer`). The task is only available if the **Has Notes mailbox files** option is enabled.

To assign Notes servers directly to user accounts

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
5. Save the changes.

Related topics

- Notes user account email system on page 134

Assigning owners to server documents

Specify which user accounts and groups are entered as server document owners.

To specify user accounts as owners of a server document

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Assign document owner** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as owners of a server document

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Assign document owner** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Assigning administrators to server documents

Specify which user accounts and groups are allowed to administer server documents.

To specify user accounts as administrators for a server document

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign document administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as administrators for a server document

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign document administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

6. Save the changes.

Specifying administrator access

In Domino, you can limit administrator's access permissions, whereby you issue permissions only at specific access levels. You can, for example, specify database administrators or issue full permissions to individual administrators.

Assigning administrators with full permissions to Notes servers

Assign user accounts and groups that are to have full access on servers.

To specify user accounts as full access administrator for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign full access administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify groups as full access administrator for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign full access administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

6. Save the changes.

Related topics

- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Assigning administrators to Notes servers

You can specify user accounts and groups that are allowed to administrate servers. Administrators obtain all permissions and entitlements of a database administrator and an administrator with full remote console permissions.

To specify user accounts as administrator for a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify groups as administrators for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click ✓.

6. Save the changes.

Related topics

- Assigning database administrators to Notes servers on page 197
- Assigning administrators with full remote console access to Notes servers on page 198
- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Assigning database administrators to Notes servers

Assign the user accounts and groups to administrate databases on servers.

To specify user accounts as database administrator for a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign database administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.

6. Save the changes.

To specify groups as database administrators for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign database administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .

6. Save the changes.

Related topics

- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Assigning administrators with full remote console access to Notes servers

Assign user accounts and groups that are allowed to use the remote console to run commands on this server. That includes permissions and entitlements of an administrator with read-only access.

To specify user accounts as remote console administrators for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign full remote console administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To specify groups as remote console administrators for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign full remote console administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click ✓.

6. Save the changes.

Related topics

- Assign read-only administrators on Notes servers on page 199
- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Assign read-only administrators on Notes servers

Assign user accounts and groups that are only allowed to use the remote console to run commands supplying system information.

To specify user accounts as read-only administrators for a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign view only administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.

6. Save the changes.

To specify groups as read-only administrators for a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign view only administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.

6. Save the changes.

Related topics

- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Assigning system administrators to Notes servers

Assign the user accounts and groups that can run any operating system commands on the server.

To specify user accounts as system administrators for a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign system administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To specify groups as system administrators for a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign system administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

Related topics

- Assign restricted system administrators to Notes servers on page 201
- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Assign restricted system administrators to Notes servers

Assign user accounts and groups that can only run restricted operating system commands on the server.

To specify user accounts as restricted system administrators for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign restricted system administrators**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To specify groups as restricted system administrators for servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Assign restricted system administrators**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Related topics

- Assigning system administrators to Notes servers on page 200
- Specifying administrator access on page 195
- Assigning administrators to server documents on page 194

Setting up server permissions for Notes servers

In the server document, access lists are defined that specify what access is given to users, groups, or servers for different purposes.

Allow server access

By default, all user accounts, groups, and servers can access the server. To limit server access, you can explicitly assign user accounts, groups, and servers that may access the server. After you have assigned the objects, server access is denied for all other user accounts, groups, and servers.

To only deny server access for individual user accounts, groups, and servers, use the **Not access server** task. For more information, see Restricting server access on page 203.

To explicitly ensure server access to user accounts

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Server access** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To explicitly ensure server access to groups

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Server access** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click ✓.

6. Save the changes.

To explicitly ensure server access to servers

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Server access** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.

6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Restricting server access

The given user accounts, groups, and servers cannot access the server. If no user accounts, groups, or servers are assigned, all user accounts, groups, and servers with server access permissions can access the server. For more information, see Allow server access on page 202.

To deny user accounts access to the server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Deny server access** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.

6. Save the changes.

To deny groups access to the server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Deny server access** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

To deny servers access to the server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Deny server access** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Creating databases and templates

The given user accounts, groups, and servers can create new databases and templates on the server. If no user accounts, groups, and servers are assigned, everyone is allowed to create new databases.

To allow user accounts to create databases and templates

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Create databases and templates** task.

4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To allow groups to create databases and templates

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Create databases and templates** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

To allow servers to create databases and templates

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Create databases and templates** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Creating new replicas

The given user accounts, groups, and servers can create new replicas on the server. If no user accounts, groups, and servers are assigned, everyone is allowed to create new replicas.

To allow user accounts to create replicas

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Create new replicas** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .
6. Save the changes.

To allow groups to create replicas

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Create new replicas** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

To allow servers to create replicas

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Create new replicas** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

To remove an assignment

- Select the server and double-click ✓.

6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Allow routing through servers

The given user accounts, groups, and servers use the server as passthru servers without taking server access into account. If there are no user accounts, groups, or servers assigned, the server cannot be used as a passthru server.

Servers must be set up as passthru destinations for assignments to take effect. For more information, see Setting up Notes servers as passthru servers for routing on page 208.

To allow user accounts to use the server as passthru server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Route through Server** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.

6. Save the changes.

To allow groups to use the server as passthru server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Route through Server** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.

6. Save the changes.

To allow servers to use the server as passthru server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Route through Server** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Setting up Notes servers as passthru servers for routing

The given user accounts, groups, and servers can access the server using passthru servers. Server access must also be set up on this server for user accounts, groups, and servers. For more information, see Allow server access on page 202.

If there are no user accounts, groups, or servers assigned, the server cannot be used as a passthru destination.

To allow user accounts to use the server as passthru destination

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Access this server** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To allow groups to use the server as passthru destination

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Access this server** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

To allow servers to use the server as passthru destination

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Access this server** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202
- Allow routing through servers on page 207

Cause calling with the passthru server

The given user accounts, groups, and servers can access other servers by using this passthru server as a modem. If no user accounts, groups, and servers are assigned, dial up is not permitted.

Servers must be set up as passthru destinations for assignments to take effect. For more information, see Setting up Notes servers as passthru servers for routing on page 208. Furthermore, the user accounts, groups, or servers these servers can use must be defined. For more information, see Allow routing through servers on page 207.

To allow user accounts to use the passthru server for placing calls

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Cause calling** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click ✓.
6. Save the changes.

To allow groups to use the passthru server for placing calls

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Cause calling** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

To allow servers to use the passthru server for placing calls

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Cause calling** task.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Destinations permitted for passthru servers

The passthru server allows you to enter the destination servers that can be reached through this passthru server. If no destination server is given, all servers given as passthru destinations can be accessed.

Servers must be set up as passthru destinations for assignments to take effect. For more information, see Setting up Notes servers as passthru servers for routing on page 208. Furthermore, the user accounts, groups, or servers these servers can use must be defined. For more information, see Allow routing through servers on page 207.

To specify the destination server for a passthru server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Destinations allowed**.
4. In the **Table** field, select the **Notes server** table.
5. In the **Add assignments** pane, assign the target servers.

   TIP: In the **Remove assignments** pane, you can remove assigned servers.

   To remove an assignment

   - Select the server and double-click ✓.
6. Save the changes.

Related topics

- Setting up server permissions for Notes servers on page 202

Signing or running unrestricted methods and operations

The given users and groups can run all agents on the server that are signed with their user ID file. Permissions for running restricted LotusScript and Java agents and for running simple and formula agents are included. If no user accounts or groups are assigned, nobody can run these agents on the server.

To allow user accounts to run unrestricted methods and operations on a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Run or sign unrestricted methods and operations**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

To remove an assignment

- Select the user account and double-click .

6. Save the changes.

To allow groups to run unrestricted methods and operations on a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Run or sign unrestricted methods and operations**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

Related topics

- Running restricted LotusScript/Java agents on page 212
- Running simple agents and formula agents on page 213
- Setting up server permissions for Notes servers on page 202

Running restricted LotusScript/Java agents

The given user accounts and groups can run certain LotusScript and Java agents on the server. If no user accounts or groups are assigned, nobody can run these agents on the server.

To allow user accounts to run restricted LotusScript/Java agents on a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Run restricted LotusScript/Java agents**.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

To remove an assignment

- Select the user account and double-click .

6. Save the changes.

To allow groups to run restricted LotusScript/Java agents on a server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **Run restricted LotusScript/Java agents**.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .

6. Save the changes.

Related topics

- Signing or running unrestricted methods and operations on page 211
- Setting up server permissions for Notes servers on page 202

Running simple agents and formula agents

The given user accounts and groups can run simple agents and formula agents on the server (private as well as common). If no user accounts or groups are assigned, all user accounts and groups can run these agents.

To allow user accounts to run simple agents and formula agents on the server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Run simple and formula agents** task.
4. In the **Table** field, select the **Notes user accounts** table.
5. In the **Add assignments** pane, assign the user accounts.

   TIP: In the **Remove assignments** pane, you can remove assigned user accounts.

   To remove an assignment

   - Select the user account and double-click .

6. Save the changes.

To allow groups to run simple agents and formula agents on the server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Run simple and formula agents** task.
4. In the **Table** field, select the **Notes groups** table.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Related topics

- Signing or running unrestricted methods and operations on page 211
- Setting up server permissions for Notes servers on page 202

Maintaining excluded lists and additional lists

Notes servers can be members of dynamic groups. Use the excluded list to specify which servers you want to exclude from membership in a dynamic group. Use the additional list to specify which servers you want to additionally include in membership in a dynamic group.

To add a Notes server to a dynamic group's additional list

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Additional** tab.
5. In the **Add assignments** pane, assign groups with an additional list that will contain the server.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

To add a Notes server to a dynamic group's exclusion list

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Excluded** tab.
5. In the **Add assignments** pane, assign groups with an excluded list that will contain the server.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

Related topics

- Memberships in dynamic groups on page 166

Displaying the Notes server overview

Use this task to obtain an overview of the most important information about a Notes server.

To obtain an overview of a Notes server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Select **server overview**.Notes

Deleting Notes servers

Servers are permanently deleted from the One Identity Manager database and from the Domino address book.

To delete a Notes server

1. In the Manager, select the **HCL Domino > Notes servers** category.
2. Select the server in the result list.
3. Click .
4. Confirm the security prompt with **Yes**.

Reports about Notes objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for Domino environments.

Table 46: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	group	This report finds all roles containing employees who have the selected system entitlement.
Show overview	group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	group	This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Certificate	The report finds all roles containing employees whose Notes user account was created with the selected certificate.
Show entitlement drifts	Domain	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts	Domain	This report returns all the user accounts with

Report	Published for	Description
overview (incl. history)		their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average number of system entitlements	Domain	This report contains all user accounts with an above average number of system entitlements.
Show employees with multiple user accounts	Domain	This report shows all the employees that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Domain	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Domain	This report finds all roles containing employees with at least one user account in the selected target system.
Show unused user accounts	Domain	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Domain	This report shows all user accounts to which no employee is assigned.

Table 47: Additional reports for the target system

Report	Description
Notes user account and group administration	This report contains a summary of user account and group distribution in all Notes domains. You can find the report in the **My One Identity Manager > Target system overviews** category.
Data quality summary for Notes user accounts	This report contains different evaluations of user account data quality in all Notes domains. You can find the report in the **My One Identity Manager > Data quality analysis** category.

Related topics

- Overview of all assignments on page 106

8

Handling of Notes objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and employees

  An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized person, such as a manager.

- Managing group assignments

  When a group is assigned to an IT Shop shelf, the group can be requested by the customers of the shop in the Web Portal. The request undergoes a defined approval process. The group is not assigned until it has been approved by an authorized person.

  In the Web Portal, managers and administrators of organizations can assign groups to the departments, cost centers, or locations for which they are responsible. The groups are passed on to all persons who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, managers, and administrators of business roles can assign groups in the Web Portal to the business roles for which they are responsible. The groups are passed on to all persons who are members of these business roles.

  If the System Roles Module is available, supervisors of system roles can assign groups to the system roles in the Web Portal. The groups are passed on to all persons to whom these system roles are assigned.

- Attestation

  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

  If the Compliance Rules Module is available, you can define rules that identify the invalid group memberships and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check and resolve rule violations and to grant exception approvals.

  If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

  You can use the risk index of groups to evaluate the risk of entitlement assignments for the company.One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the employees, user accounts, and their entitlements and risks.

For more information about the named topics, see Assigning Notes groups to Notes user accounts on page 92 and refer to the following guides:

- One Identity Manager Web Designer Web Portal User Guide
- One Identity Manager Attestation Administration Guide
- One Identity Manager Compliance Rules Administration Guide
- One Identity Manager Company Policies Administration Guide
- One Identity Manager Risk Assessment Administration Guide

Basic data for managing a Domino environment

To manage a Domino environment in One Identity Manager, the following basic data is relevant.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

  For more information, see Account definitions for Notes user accounts on page 58.

- Password policy

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

  Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

  For more information, see Password policies for Notes user accounts on page 108.

- Target system types

  Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

  For more information, see Post-processing outstanding objects on page 50.

- Target system managers

  A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all Notes domains in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual domains. The application roles must be added under the default application role.

For more information, see Target system managers for Domino domains on page 226.

- Servers

  Servers must be informed of your server functionality in order to handle Domino-specific processes in One Identity Manager. For example, the gateway server.

  For more information, see Job server for Domino-specific process handling on page 221.

Job server for Domino-specific process handling

In order to handle Domino specific processes in One Identity Manager, the synchronization server and its server functionality must be declared. You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **HCL Domino > Basic configuration data > Server** category and edit the Job server main data.

  Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

NOTE: One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

To edit a Job server and its functions

1. In the Manager, select the **HCL Domino > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.
4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- General main data of Job servers on page 222
- Specifying server functions on page 224

Related topics

- Installing the One Identity Manager Service on the gateway server on page 23

General main data of Job servers

NOTE: All editing options are also available in the Designer under **Base Data > Installation > Job server**.

NOTE: More properties may be available depending on which modules are installed.

Table 48: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: `<Name of servers>.<Fully qualified domain name>`
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the `Robocopy` and `rsync` programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the `Robocopy` program between servers with a Windows operating system or with the `rsync` program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is

Property	Meaning
	applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the `QBM_PJobQueueLoad` procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
Paused due to	Specifies whether task processing for this queue has been stopped

Property	Meaning
unavailability of a target system	because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 224

Specifying server functions

NOTE: All editing options are also available in the Designer under **Base Data > Installation > Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

NOTE: More server functions may be available depending on which modules are installed.

Table 49: Permitted server functions

Server function	Remark
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
HCL Domino	Gateway server for synchronizing One Identity Manager with HCL

Server function	Remark
gateway server	Domino.
HCL Domino connector	Server on which the HCL Domino connector is installed. This server synchronizes the HCL Domino target system.
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Generic database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for synchronizing an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows	The server can run Windows PowerShell version 3.0 or later.

Server function	Remark
PowerShell connector	

Related topics

- General main data of Job servers on page 222

Target system managers for Domino domains

A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all Notes domains in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual domains. The application roles must be added under the default application role.

For more information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.

   Target system managers with the default application role are authorized to edit all the Notes domains in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual domains.

Table 50: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Domino** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects.

User	Tasks
	• Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have another identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)
2. Select the **One Identity Manager Administration > Target systems > Administrators** category.
3. Select the **Assign employees** task.
4. Assign the employee you want and save the changes.

To add the first employees to the default application as target system managers

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > Domino** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

1. Log in to the Manager as a target system manager.
2. Select the application role in the **HCL Domino > Basic configuration data > Target system managers** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To specify target system managers for individual domains

1. Log in to the Manager as a target system manager.
2. Select the **HCL Domino > Domains** category.
3. Select the domain in the result list.
4. Select the **Change main data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

   Next to the **Target system manager** menu, click to create a new application role.

   a. Enter the application role name and assign the **Target systems | Domino** parent application role.

   b. Click **OK** to add the new application role.
6. Save the changes.
7. Assign employees to this application role who are permitted to edit the domain in One Identity Manager.

Related topics

- One Identity Manager users for managing Domino on page 13
- General main data for Notes domains on page 126

Appendix A

Configuration parameters for managing a Domino environment

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 51: Configuration parameters for managing a Domino environment

Configuration parameter	Meaning if Set
TargetSystem | NDO	Preprocessor relevant configuration parameter for controlling database model components for Domino target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
TargetSystem | NDO | Accounts	Parameter for configuring Notes user account data.
TargetSystem | NDO | Accounts | InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | NDO | Accounts | InitialRandomPassword | SendTo	Employee to receive an email with the random generated password (manager cost center/department/location/business role, employee's manager or `XUserInserted`). If no recipient can be found, the email is sent to the address stored in the **TargetSystem | NDO | DefaultAddress** configuration parameter.
TargetSystem | NDO |	Mail template name that is sent to supply users with the login

Configuration parameter	Meaning if Set
Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	credentials for the user account. The **Employee - new user account created** mail template is used.
TargetSystem | NDO | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem | NDO | Accounts | MailFileAccessRole	Access level that is set for a mailbox file owner when the mailbox file is created. Possible values are **Manager**, **Editor**, **Designer**. If the configuration parameter is not set, the access level **Manager** is applied.
TargetSystem | NDO | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | NDO | BuildShortnameFullSync	Specifies whether short names are created for employee documents during synchronization, which do not have short names in Domino. If this parameter is set, short names are created. If the parameter is not set, short names are created. If not, user accounts without a short name cannot be added to the One Identity Manager database.
TargetSystem | NDO | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | NDO | DefTemplatePath	Default template for adding the mailbox files on a Notes server.
TargetSystem | NDO | DenyAccessGroups	Parameter for configuring the denied access groups for locking user accounts.
TargetSystem | NDO | DenyAccessGroups | Memberlimit	Specifies the maximum number of members per denied access group. When this limit is reached, another denied access group is created automatically.
TargetSystem | NDO | DenyAccessGroups | Prefix	Prefix used for formatting the group name for a denied access group.
TargetSystem | NDO | MailBoxAnonymPre	Prefix for user account anonymity.

Configuration parameter	Meaning if Set
TargetSystem | NDO | MailFilePath	Directory on the mail server, in which the user account's mailbox files are stored.
TargetSystem | NDO | MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem | NDO | PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | NDO | PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to locked user accounts. User accounts do not obtain an account definition.
TargetSystem | NDO | PersonAutoFullsync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem | NDO | PersonExcludeList	Listing of all user account without automatic employee assignment. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
TargetSystem | NDO | UpdateAddressbook	If the configuration is set, entries in the Domino Directory are added when new user ID files are created.
TargetSystem | NDO | VerifyUpdates	Specifies whether changed properties are checked when the system is updated. If this parameter is set, the objects in the target system are verified after every update.

Appendix B

Default project template for Domino

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows, and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

The project template uses mappings for the following schema types.

Table 52: Mapping Notes schema types to tables in the One Identity Manager schema

Schema type in Domino	Table in the One Identity Manager Schema
AdminRequest	NDOAdmin4
Certifier	NDOCertifier
CertificateRequest	NDOCertifierRequest
Database	NDOMailInDB
CurrentDomain	NDODomain
Group	NDOGroup
Employee	NDOUser
PolicyMaster	NDOPolicy
PolicyArchive	NDOPolicySetting
PolicyDesktop	NDOPolicySetting
PolicyMail	NDOPolicySetting
PolicyRegistration	NDOPolicySetting

Schema type in Domino	Table in the One Identity Manager Schema
PolicySecurity	NDOPolicySetting
PolicySetup	NDOPolicySetting
Server	NDOServer
Template	NDOTemplate

Appendix C

Processing methods of Domino system objects

The following table describes permitted processing methods for Domino schema types and the necessary restrictions for processing the system objects.

Table 53: Methods available for processing Domino schema types

Schema type	Read	Paste	Delete	Refresh
Admin4 database (`AdminRequest`)	Yes	No	No	No
Certificate request (`CertificateRequest`)	Yes	No	No	No
Certificate (`Certifier`)	Yes	No	Yes	Yes
Domain (`CurrentDomain`)	Yes	No	No	No
Mail-in database (`Database`)	Yes	Yes	Yes	Yes
Group (`Group`)	Yes	Yes	Yes	Yes
User account (`Person`)	Yes	Yes	Yes	Yes
Policy setting (`PolicyArchive`)	Yes	No	No	No
Policy setting (`PolicyDesktop`)	Yes	No	No	No
Policy setting (`PolicyMail`)	Yes	No	No	No
Policy (`PolicyMaster`)	Yes	No	No	Yes
Policy setting (`PolicyRegistration`)	Yes	No	No	No
Policy setting (`PolicySecurity`)	Yes	No	No	No
Policy setting (`PolicySetup`)	Yes	No	No	No
Server (`Server`)	Yes	No	Yes	Yes
Template (`Template`)	Yes	No	No	No

Appendix D

Domino connector settings

The following settings are configured for the system connection with the Domino connector.

Table 54: Domino connector settings

Setting	Meaning
Domino server	Name of the Domino server which communicates with the gateway server. Variable: `CP_NDOserver`
Domino Directory	Name of the Domino Directory. Default value: **Names.nsf** Variable: `CP_NDOdatabasename`
Custom INI file	Name and path of the custom INI file. Default value: **C:\Program Files (x86)\IBM\Notes\vinotes.ini** Variable: `CP_NDOinifile`
ID file password	Synchronization user's ID file password. The path of this ID file must be given in the custom INI file. Variable: `CP_BASEpassword`
Delete objects using AdminP processes	Specifies whether to delete Notes objects using AdminP processes. Default value: **True** Variable: `CP_NDOuseadminpdel`
Domain	Distinguished name of the Notes domain. Variable: `CP_ADRootdn`
Access level	Access level that is set for a mailbox file owner when the mailbox file is created. Possible values are **Manager**, **Editor**, **Designer**. Default value: **0** (Manager)

Setting	Meaning
	Variable: `MailFileAccessType`
UserCreateMailDb	Specifies whether the mailbox file is created after a Notes user registers. This uses the template given in the user account or in the **TargetSystem | NDO | DefTemplatePath** configuration parameter. Default value: **0** Variable: `UserCreateMailDb` The value **1** specifies that the mailbox file is already created during Notes user registration. In this case, the template of the Notes server's on which the user is registered is used.
UserIDFilesDefaultPath	Default path for saving the user ID files on the gateway server. Default value: **C:\Program Files (x86)\IBM\Lotus\Notes\Data\IDS** Variable: `UserIDFilesDefaultPath`
UserIsNorthAmerican	Specifies whether the newly created ID files are compatible with the American (US) and Canadian Domino version. Value **1**: All new user ID files are calculated with North American encryption strength. Default value: **0** Variable: `UserIsNorthAmerican`
UserMinPwdLen	Specifies the minimum password length that is set in all newly calculated user ID files. Default value: **0** Variable: `UserMinPwdLen`
UserStoreIDInAddressbook	Specifies whether the ID file is attached to the employee document or saved on the gateway server. Default value: **0** - The ID file is attached to the employee document. Variable: `UserStoreIDInAddressbook`
UserType	User type generated by registration. Possible values are **176** (FULL CLIENT USER), **175** (DESKTOP CLIENT USER), **174** (LIMITED CLIENT USER). Default value: **176** Variable: `UserType`

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

D

E

G

I

J

L

M

N

O

P

R

S

T

U

V