Dell™ One Identity Manager 7.1.3

Administration Guide for Connecting to IBM® Notes®

Legend

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

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

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

One Identity Manager Administration Guide for Connecting to IBM® Notes®
Updated - November 2017
Version - 7.1.3

Contents

1

Managing IBM® Notes® Environments

IBM® Notes® environment 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 IBM® Notes® environments in parallel with a One Identity Manager database. Notes user and employee documents are managed as user accounts in One Identity Manager.

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 for working with IBM® Notes®. When you add a user with the IBM® Notes® 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 the 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. The One Identity Manager access lists can be defined for server documents in order to specify who has access to a server for what reason.

Architecture Overview

The visible area of a productive IBM® Notes® environment is mapped to a Notes domain in One Identity Manager. One Identity Manager needs access to this IBM® Notes®'s Domino Directory for synchronization.

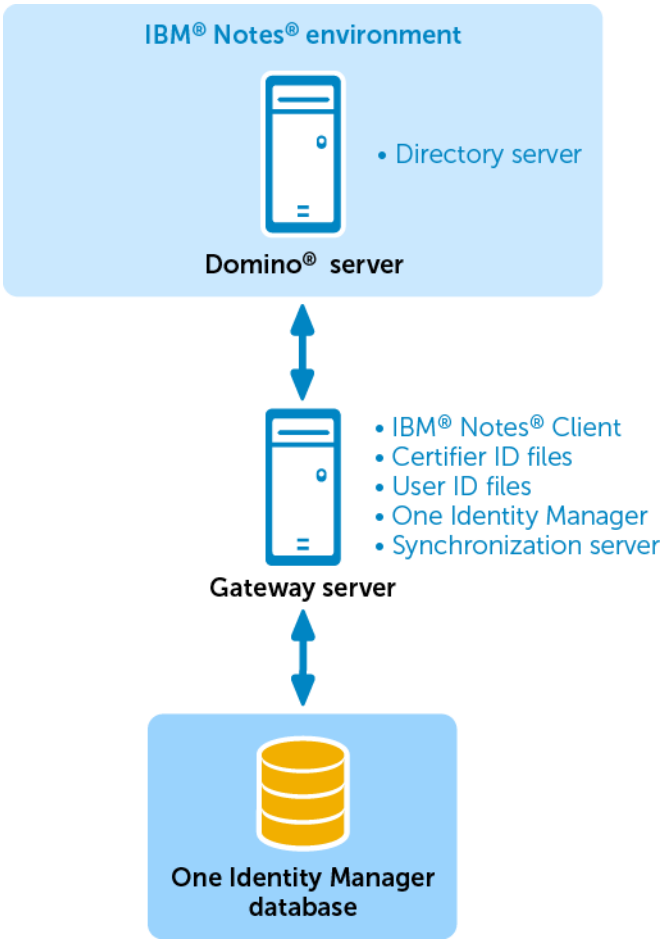
A server is defined within the One Identity Manager environment to execute all administrative task effecting the IBM® Notes® environment. This server is named the gateway server in the rest of this chapter. The gateway server takes over the function of synchronization server. It is not a productive Domino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

All IBM® Notes® connector actions are executed 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 a selected server with a good network connection to the gateway server. The IBM® Notes® connection requires access to the Domino Directory, preferably therefore, you should use a directory server.

For synchronization, provide an ID file with sufficient administrative permissions for accessing the productive IBM® Notes® 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 executes 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 IBM® Notes® client context using the IBM® Domino® COM library and processes all necessary function for exchanging data with the Domino server in it (access to Domino objects, running Notes agents, creating administrative processes (AdminP), error handling).

Figure 1: IBM® Notes® Connectors communication with IBM® Notes®



The objects in IBM® Notes® are mapped as following in the One Identity Manager database:

Table 1: Mapping object types from this IBM® Notes® installation in the One Identity Manager

IBM® Domino®	One Identity Manager
Domino server	Notes server
Domino domain	No direct mapping
	Notes domain Properties of Notes objects to assign them to different IBM® Notes® environments.

IBM® Domino®	One Identity Manager
User	Notes user account
Group	Notes group
Mail-in DB	Notes mail-in database
Notes certificate	Notes certificate
Template	Notes template
Policy	Notes policy

One Identity Manager Users for Managing an IBM® Notes® System

The following users are used for setting up and administration of an IBM® Notes® system.

Table 2: User

User	Task
Target system administrators	Target system administrators must be assigned to the application role **Target system | Administrators**. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | IBM® Notes®** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts, groups or container structures. • Prepare groups for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines 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	• 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, as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configures schedules as required.
Administrators for the IT Shop	Administrators must be assigned to the application role **Request & Fulfillment | IT Shop | Administrators**. Users with this application role: • Assign groups to IT Shop structures.
Administrators for organizations	Administrators must be assigned to the application role **Identity Management | Organizations | Administrators**. Users with this application role: • Assign groups to departments, cost centers and locations.
Business roles administrators	Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**. Users with this application role: • Assign groups to business roles.

2

Setting up IBM® Notes® Synchronization

One Identity Manager supports synchronization with IBM® Notes® environments in versions 8 and 9 of the IBM® Domino® Server and the IBM® Notes® Client version 8.5.3 or later.

To load IBM® Notes® objects into the One Identity Manager database

1. Prepare a user with sufficient permissions for synchronizing in IBM® Notes®.
2. One Identity Manager components for managing IBM® Notes® environments are available if the configuration parameter "TargetSystem\NDO" is set.
    - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
    - 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 IBM® Notes® are to be registered by the IBM® Notes® 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 IBM® Notes® on page 12
- Installing and Configuring a Gateway Server on page 14
- Creating a Synchronization Project for initial Synchronization of a Notes Domain on page 19
- General Master Data for Notes Certificates on page 62

Users and Permissions for Synchronizing with IBM® Notes®

The following users are involved in synchronizing One Identity Manager with IBM® Notes®.

Table 3: Users for Synchronization

User	Entitlements
One Identity Manager Service user account	The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited). The user account must belong to the group "Domain Users". The user account must have the extended access right "Log on as a service". The user account requires access rights to the internal web service. **NOTE:** If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights 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 the One Identity Manager. In the default installation the One Identity Manager is installed under: • `%ProgramFiles(x86)%\Dell` (on 32-bit operating systems) • `%ProgramFiles%\Dell` (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 • The role "UserCreator" in addition to the default roles • Administration access to the Domino server (server available for registering new user accounts and creating AdminP tasks) The access function "Editor" is also required for the following databases: • cert.log • admin4.nsf
User for accessing the One Identity Manager database	The default system user "Synchronization" is available to run synchronization over an application server.

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.
- Set `FT_MAX_SEARCH_RESULTS = 2147483000` in the file `Notes.ini`.

If you apply filters in the Domino Directory, a maximum of 5000 filtered values are returned. To obtain a complete result list of the elements which satisfy the filter condition, you must overwrite this value in the Domino server's `Notes.ini` file.

For more detailed information, see your IBM® Notes® documentation.

Installing and Configuring a Gateway Server

The gateway server administrates the functionality of the synchronization server. To set up a gateway server, a computer has to be available with the following software installed:

- Windows® operating system

  Following versions are supported:

  - Windows Server® 2008 (non-Itanium based 64-bit) Service Pack 2 or later
  - Windows Server® 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
  - Windows Server® 2012
  - Windows Server® 2012 R2
  - Windows Server® 2016
- Microsoft® .NET Framework version 4.5.2 or 4.6.1
- Windows® Installer (MSI service)
- IBM® Notes® Client version 8.5.3

  NOTE: A real installation must be run. IBM® Domino® COM class libraries are registered during installation. These require the IBM® Notes® connector.
- Write access to the IBM® Notes® client install directory and the One Identity Manager install directory.
- One Identity Manager Service, IBM® Notes® connector
  - Install One Identity Manager components with the installation wizard.
    1. Select the option **Select installation modules with existing database**.
    2. Select the machine role **Server | Job server | IBM® Notes®**.

Special requirements for synchronizing a IBM® Domino® 8.5. or 9 environment

The following versions of the IBM® Notes® and IBM® Domino® components are required for synchronizing a IBM® Domino® version 8.5 or 9 environment as a minimum.

- IBM® Domino® Server version 8.5.1 with Fix Pack 2 or later or version 9.0.1.
- IBM® Notes® Client version 8.5.3, Fix Pack 4

To set up a gateway server

1. Configure the IBM® Notes® client.

   For more information, see To configure the IBM® Notes® client on page 15.

2. Install the One Identity Manager Service and declare the gateway server as Job server in the One Identity Manager database. For more information, see Installing and Configuring the One Identity Manager Service on page 16.

To configure the IBM® Notes® client

1. Extend the PATH variable to include the default search path (installation directory) and the data directory (`<Installation directory>\data`).

   Enter the IBM® Notes® install path, that means the path where `Notes.exe` can be found, in the default search path for the operating system (PATH variable). Also add the path you selected for the Notes data directory when you installed the IBM® Notes® client, to the PATH variable.
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 IBM® 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 rights 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 IBM® 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.

Detailed information about this topic

- Copying the Notes Certificate on page 15
- Creating a Custom INI File on page 16

Copying the Notes Certificate

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 IBM® Notes® 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 detailed information about copying certificate documents, see your IBM® Notes® documentation.

Creating a Custom INI File

The `Notes.ini` file is created when you configure the IBM® Notes® client. This file contains different configuration information, which the IBM® Notes® connector needs to access the target system. Create a copy of this INI file and make it available to the IBM® Notes® 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 of the Notesdata directory (local directory).
KeyFileName	Path of the synchronization user's ID file (local directory).
KitType	Notes type: 1 = client, 2 = server.

Installing and Configuring the One Identity Manager Service

The gateway server takes over the synchronization server functionality. All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Entries which are necessary for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

NOTE: If the server running the synchronization does not have a connection to the One Identity Manager database, synchronization is aborted. Ensure that a direct connection to the One Identity Manager database is possible.

Use the Server Installer to install the One Identity Manager Service. This program executes the following steps.

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of 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 executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.

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

1. Start the program Server Installer on your administrative workstation.
2. Enter valid data for connecting to One Identity Manager on the **Database connection** page and click **Next**.
3. Specify on which server you want to install the One Identity Manager Service on the **Server properties** page.
   a. Select a job server in the **Server** menu.

      The view- OR -

      Click **Add** to add a new job server.

   b. Enter the following data for the Job server.

      Table 5: Job Servers Properties

Property	Description
Server	Name of the Job servers.
Queue	Name of queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Full server name	Full name of the server in DNS syntax. `Example:` <name of server>.<fully qualified domain name>

      NOTE: Use the **Advanced** option to edit other Job server properties. You can use the Designer to change properties at a later date.

4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.

   Select at least the following roles:

   - IBM® Notes®

5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

   The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.

   Select at least the following server functions:

   - IBM® Notes® connector

6. Check the One Identity Manager Service configuration on the **Service settings** page.

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

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on the **Select installation source** page.
10. Select the file with the private key on the page **Select private key file**.

    NOTE: This page is only displayed when the database is encrypted.

11. Enter the service's installation data on the **Service access** page.

    Table 6: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server*** • Enter the server name. - OR - • Select a entry from the list.
Service account	One Identity Manager Service user account data. ***To enter a user account for the One Identity Manager Service*** • Set the option **Local system account**. This starts the One Identity Manager Service under the account "NT AUTHORITY\SYSTEM". - OR - • Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** **Enable** Advanced • . • Enable the option **Current user**. This uses the user account of the current user. - OR - • Enter user account, password and password confirmation.

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: The One Identity Manager Service is entered with the name "Dell One Identity Manager Service" in the server's service administration.

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.

NOTE: The archive database is only required if the option **ID vault enabled** is not set and if the user ID files are supposed to be restored by One Identity Manager. For more information, see ID restore on page 99.

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

Table 7: 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 IBM® Notes® connector to access the archive database.

For more detailed information about adding the address book copy, see your IBM® Notes® 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 IBM® Notes®. The following describes the steps for initial configuration of a synchronization project.

After the initial set up 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.

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

Table 8: 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 a Custom INI File on page 16.
ID file password	Synchronization user's ID file password. The path of this ID file must be given in the custom INI file. The IBM® Notes® 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 IBM® Notes® on page 12.
Synchronization server	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Entries which are necessary for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The gateway server takes over the function of synchronization server. The One Identity Manager Service with the IBM® Notes® 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 9: Additional Properties for the Job Server** Property: Server Function — Value: IBM® Notes® connector Property: Machine role — Value: Server/Job server/IBM® Notes® For more information, see Installing and Configuring the One Identity Manager Service on page 16.

Data	Explanation
One Identity Manager Database Connection Data	SQL Server®: • Database server • Database • Database user and password • Specifies whether Windows® authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows® authentication. Oracle: • Species whether access is direct or through the Oracle client Which connection data is required, depends on how this option is set. • Database server • Oracle instance port • Service name • Oracle database user and password • Data source (TNS alias name from `TNSNames.ora`)
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 target system to do this. If you cannot start the Synchronization Editor directly on the gateway server, because of the firewall configuration, for example, 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 assumes the function of the remote connection server at the same time. 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 • IBM® Notes® 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 Dell One Identity Manager Target System Synchronization Reference Guide.

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

- In default mode
- Started from the launchpad

Additional settings can be made if the project wizard is run in expert mode or is started directly from the Synchronization Editor. Follow the project wizard instructions through these steps.

To set up initial synchronization project for a Notes domain.

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

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

2. Select the entry **IBM® Notes® target system type** . Click **Run**.

   This starts the Synchronization Editor's project wizard.

3. Specify how the One Identity Manager can access the target system on the **System access** page.
   - If you started the launch pad on the gateway server, do not change any settings.
   - If you started the launch pad on a workstation, connect remotely.

     In this case, set the option **Connect using remote connection server** and select, under **Job server**, the gateway server you want to use for the connection.

4. Enter the connection parameters required by the IBM® Notes® connector to log in on the target system on the page, **Configuration data for the IBM® Domino® directory**.

   Table 10: Domino Server Connection Configuration

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.
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 in **Verify connection settings**. Click on **Verify project**.

   The 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 this option is not set, target system objects are deleted directly through the IBM® Notes® connector.
   - Click **Finish**, to end the system connection wizard and return to the project wizard.

7. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.

> **NOTE:** Reenter all the connection data if you are not working with an encrypted One Identity Manager database and no synchronization project has been saved yet in the database. 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. Specify how system access should work on the page **Restrict target system access**. You have the following options:

Table 11: Specifying Target System Access

Option	Meaning
Read-only access to target system	Specifies whether a synchronization workflow should be set up to initially load 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 in synchronization direction "One Identity Manager".
Changes are also made to the target system	Specifies whether a provisioning workflow should be set up in addition to the synchronization workflow to initially load the target system. The provisioning workflow displays the following characteristics: • Synchronization in the direction of the "target system" • Processing methods are only defined in the synchronization steps in synchronization direction "target system". • Synchronization steps are only created for such schema classes whose schema types have write access.

10. Select the synchronization server to execute synchronization on the **Synchronization server** page.

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

    - Click to add a new job server.
    - Enter a name for the job server and the full server name conforming to DNS syntax.
    - Click **OK**.

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

      > **NOTE:** Ensure that this server is set up as the synchronization server after saving the synchronization project.

11. Click **Finish** to complete the project wizard.

    This creates and allocates a default schedule for regular synchronization.

    The synchronization project is created, saved and enabled immediately.

> **NOTE:** If the synchronization project is not going to be executed immediately, disable the option **Activate and save the new synchronization project automatically**.
>
> In this case, save the synchronization project manually before closing the Synchronization Editor.

> **NOTE:** The target system connection data is saved in a variable set, which you can change in the Synchronization Editor under **Configuration | Variables** if necessary.

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the category **Configuration | Target system**.
2. To configure the synchronization log for the database connection, select the category **Configuration | One Identity Manager connection**.
3. Select **General** view and click **Configure...**.
4. Select the **Synchronization log** view and set **Create synchronization log**.
5. Enable the data to be logged.

   > **NOTE:** Certain content create a lot of log data.
   >
   > The synchronization log should only contain the data necessary for error analysis and other evaluations.

6. Click **OK**.

To synchronize on a regular basis

1. Select the category **Configuration | Start configuration**.
2. Select a start up configuration in the document view and click **Edit schedule...**.
3. Edit the schedule properties.
4. To enable the schedule, click **Activate**.
5. Click **OK**.

To start initial synchronization manually

1. Select the category **Configuration | Start configuration**.
2. Select a start up configuration in the document view and click **Execute**.
3. Confirm the security prompt with **Yes**.

NOTE: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the domain at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
    a. Select the category **IBM® Notes® | User accounts | Linked but not configured | <Domain>**.
    b. Select the task **Assign account definition to linked accounts**.

Detailed information about this topic

- Dell One Identity Manager Target System Synchronization Reference Guide

Related Topics

- Installing and Configuring a Gateway Server on page 14
- Users and Permissions for Synchronizing with IBM® Notes® on page 12
- Show Synchronization Results on page 25
- Customizing Synchronization Configuration on page 26
- Speeding Up Synchronization with Revision Filtering on page 29
- Using AdminP Requests for Handling IBM® Notes® Processes on page 148
- Appendix: Default Project Template for IBM® Notes® on page 156
- Setting Up Account Definitions on page 35
- Automatic Assignment of Employees to User Accounts on page 92

Show 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. Open the synchronization project in the Synchronization Editor.
2. Select the category **Logs**.
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 on it.

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

To display a provisioning log.

1. Select the category **Logs**.
2. Click  in the navigation view toolbar.

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

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

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

Synchronization logs are stored for a fixed length of time. The retention period is set in the configuration parameter "DPR\Journal\LifeTime". By default, synchronization logs are stored for 30 days and then deleted.

To modify the retention period for synchronization logs

- Edit the value of the configuration parameter "DPR\Journal\LifeTime" in the Designer. Enter a retention period in days.

Customizing Synchronization Configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization of an Notes domain. You can use this 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 IBM® Notes® environment.

You must customize the synchronization configuration in order to compare the IBM® Notes® database with the regularly and to synchronize changes.

- Create a workflow with the direction of synchronization "target system" to use One Identity Manager as the master system for synchronization.
- To specify which Notes objects and database object 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 which contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes or processing methods, for example.
- Use variables to set up a synchronization project which can be used for several 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.

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

- The moment another synchronization is started with the same start up configuration, the running synchronization process is stopped and given the status, "Frozen". An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Plan your start times carefully. If possible, specify your start times so that synchronization does not overlap.

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

Detailed information about this topic

- How to Configure IBM® Notes® Synchronization on page 27
- Configuring Synchronization of Several Notes Domains on page 28
- Updating Schemas on page 28

How to Configure IBM® Notes® Synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of Notes objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). You also require a workflow with synchronization in the direction of the "target system" to use One Identity Manager as the master system for synchronization.

To create a synchronization configuration for synchronizing IBM® Notes®

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This adds a workflow for synchronizing in the direction of the target system.
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 28

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.

To customize a synchronization project for synchronizing another domain

1. Set up a synchronization user with sufficient permissions in the other domain.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other domain. Use the wizards to attach a base object.
    - Select the IBM® Notes® connector in the wizard and declare the connection parameter. The connection parameters are saved in a special variable set.

      A start up configuration is created, which uses the new 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 IBM® Notes® Synchronization on page 27
- Users and Permissions for Synchronizing with IBM® Notes® on page 12

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 loading 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 compressing 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:
  - Activating the synchronization project
  - Synchronization project initial save
  - Compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target system**.

   - OR -
   Select the category

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

   This reloads the schema data.

To edit a mapping

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

   Opens the Mapping Editor. For more detailed information about editing mappings, see Dell 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.

IBM® Notes® supports revision filtering. The Notes document's last change date is used as revision counter. Each synchronization saves its last execution date as the revision in the One Identity Manager database (table `DPRRevisionStore`, column `Value`). 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 changed after this point are included with the next synchronization.

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

To permit revision filtering on a workflow

- Open the synchronization project in the Synchronization Editor.
- Edit the workflow properties. Select the entry **Use revision filter** from **Revision filtering**.

To permit revision filtering for a start up configuration

- Open the synchronization project in the Synchronization Editor.
- Edit the start configuration properties. Select the entry **Use revision filter** from **Revision filtering**.

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

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

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.

Objects marked as outstanding:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Must be post-processed separately in One Identity Manager.

Start target system synchronization to do this.

To post-process outstanding objects

1. Select the category **IBM® Notes® | Target system synchronization: IBM® Notes®**.

   All tables assigned to the target system type IBM® Notes® as synchronization tables are displayed in the navigation view.

2. Select the table whose outstanding objects you want to edit in the navigation view.

   This opens the target system synchronization form. All objects are shown here that are marked as outstanding.

   TIP:

   To display object properties of an outstanding object

   a. Select the object on the target system synchronization form.

   b. Open the context menu and click **Show object**.

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

Table 12: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted in the One Identity Manager. Deferred deletion is not taken into account. The "outstanding" label is removed from the object. Indirect memberships cannot be deleted.
	Publicize	The object is added in the target system. The "outstanding" label is removed from the object. The method triggers the event "HandleOutstanding". 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 from the object.

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

NOTE: By default, the selected objects are processed in parallel, which speeds up execution of 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

- Deactivate in the form toolbar.

You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization.

1. Select the category **IBM® Notes® | Basic configuration data | Target system types**.
2. Select the target system type in the result list IBM® Notes®.
3. Select **Assign synchronization tables** in the task view.
4. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
5. Save the changes.
6. Select **Configure tables for publishing**.
7. Select custom tables whose outstanding objects can be published in the target system and set the option **Publishable**.
8. Save the changes.

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 option **Connection is read only** must no be set for the target system connection.

Configuring Memberships Provisioning

Memberships, for example, 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 will probably be overwritten. This behavior can occur under the following conditions:

- Memberships are saved in the target system as an object property in list form.
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; 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. Start the Manager.
2. Select the category **IBM® Notes® | Basic configuration data | Target system types**.
3. Select the target system type in the result list.
4. Select the task **Configure the table for publishing**.
5. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - The option can only be set for assignment tables whose base table has a column `XDateSubItem`.
    - Assignment tables, which are grouped together in a virtual schema property in the mapping, must be labeled identically.
6. Click **Enable merging**.
7. Save the changes.

For each assignment table labeled like this, the changes made in the One Identity Manager are saved in a separate table. 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 the members list does not get entirely overwritten.

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.

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

Help for Analyzing Synchronization Issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance. The report contains information such as:

- Consistency check results
- Revision filter settings
- Scope applied
- Analysis of the synchronization buffer
- Object access times in the One Identity Manager database and in the target system

To generate a synchronization analysis report

1. Open the synchronization project in the Synchronization Editor.
2. Select the menu **Help | Generate synchronization analysis report** and answer the security prompt with **Yes**.

   The report may take a few minutes to generate. It is displayed in a separate window.
3. Print the report or save it in one of the available output formats.

Deactivating Synchronization

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

To prevent regular synchronization

- 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 loaded synchronization project

1. Select **General** on the start page.
2. Click **Deactivate project**.

Detailed information about this topic

- Creating a Synchronization Project for initial Synchronization of a Notes Domain on page 19

3

Basic configuration data

To manage an IBM® Notes® environment in One Identity Manager, the following data is relevant.

- Configuration parameter

  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. You can find an overview of all configuration parameters in the category **Base data | Configuration parameters** in the Designer.

  For more information, see Appendix: Configuration Parameters for Synchronization with a Notes Domain on page 152.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

  For more information, see Setting Up Account Definitions on page 35.

- Initial Password for New User Accounts

  You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used or a randomly generated initial password can be issued.

  For more information, see Initial Password for New Notes User Accounts on page 49.

- Email notifications about login data

  When a new user account is created, the login data are send to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.

  For more information, see Email Notifications about Login Data on page 51.

- Target System Types

  Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.

  For more information, see Post-Processing Outstanding Objects on page 30.

- Target System Managers

  A default application role exists for the target system manager in the One Identity Manager. Assign this application to employees who are authorized to edit the domains in One Identity Manager.

  Define other application roles, if you want to limit target system managers' access permissions to individual domains. The application roles must be added under the default application role.

  For more information, see Target System Managers on page 57.

- Server

  Servers must know your server functionality in order to handle IBM® Notes® specific processes in One Identity Manager. That includes the gateway server, for example.

  For more information, see Editing a Server on page 53.

Setting Up Account Definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

The data for the user accounts in the respective target system comes from the basic employee data. 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 (template processing). 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.

For more details about the basics, see the Dell One Identity Manager Target System Base Module Administration Guide.

The following steps are required to implement an account definition:

- Creating an Account Definition
- Setting Up Manage Levels
- Creating a Formatting Rule for IT Operating Data
- Determining IT Operating Data
- Assigning Account Definitions to Employees
- (Optional) Assigning Account Definitions to a Target System

Creating an Account Definition

To create a new account definition

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions.**
2. Select an account definition in the result list. Select **Change master data** in the task view.

   - OR -

Click  in the result list toolbar.

3. Enter the account definition's master data.
4. Save the changes.

Master Data for an Account Definition

Enter the following data for an account definition:

Table 13: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema which maps user accounts.
Target System	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. Leave empty for IBM® Notes® domains.
Description	Spare text box 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 account definition assignments to employees. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more information, see the Dell One Identity Manager Risk Assessment Administration Guide.
Service item	Service item through which you can request the account definition 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 ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can still be directly assigned 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 ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.

Property	Description
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. **IMPORTANT**: Only set this option 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. Disable this option to remove automatic assignment of the account definition to all 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 disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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 disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition if permanently disabled	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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 . Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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.

Setting Up Manage Levels

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.

The One Identity Manager supplies a default configuration for manage levels:

- unmanaged

  User accounts with a manage level of “Unmanaged” become linked to an employee but do not inherit any other 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 a manage level of “Full managed” inherit specific properties from the assigned employee.

NOTE: The manage levels “Full managed” and “Unmanaged” are evaluated in the 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 detailed information about manage levels, see the Dell 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 assign manage levels to an account definition

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level** in the task view.
4. Assign manage levels in **Add assignments**.

   - OR -

   Remove assignments to manage levels in **Remove assignments**.
5. Save the changes.

IMPORTANT: The manage level "Unmanaged" is assigned automatically when an account definition is assigned and cannot be removed.

To edit a manage level

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Manage levels**.
2. Select the manage level in the result list.Select **Change master data** in the task view.

   - OR -

   Click  in the result list toolbar.
3. Edit the manage level's master data.
4. Save the changes.

To assign an account definition to a manage level

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Manage levels**.
2. Select a manage level in the result list.
3. Select **Assign account definitions**.
4. Assign user account definitions in **Add assignments**.

   - OR -

   Remove assignments to account definitions in **Remove assignments**.
5. Save the changes.

Master Data for a Manage Level

Enter the following data for a manage level.

Table 14: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.
Description	Spare text box 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 always — Data is always updated Only initially — Data is only initially determined.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.

Property	Description
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled 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 locked user accounts retain their group memberships.

Creating a Formatting Rule 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 automatic creating and modifying of user accounts for an employee in the target system.

- IBM® Notes® Server
- IBM® Notes® certificate
- Mailbox template
- Groups can be inherited
- Identity
- Privileged user account

To create a mapping rule for IT operating data

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Edit IT operating data mapping** in the task view.

4. Enter the following data:

Table 15: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
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:** Only use the primary business role if the Business Roles Module is ins talled. • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
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 user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\NDO\Accounts\MailTemplateDefaultValues" .

5. Save the changes.

Determining IT Operating Data

In order for an employee to create user accounts with the manage level “Full managed”, the necessary IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. 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 client A. Specify the property "Department" in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

To specify IT operating data

1. Select the role in the category **Organizations** or **Business roles**.
2. Select **Edit IT operating data mapping** in the task view.
3. Enter the following data:

Table 16: IT Operating Data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	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 text box. b. Select the table under **Table**, which maps the target system or the table `TSBAccountDef` for an account definition. c. Select the concrete target system or concrete account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. Columns using the script template `TSB_ITDataFromOrg` in their template are listed. For more detailed information, see the Dell One Identity Manager Target System Base Module Administration Guide.
Value	Concrete value which is assigned to the user account property.

4. Save the changes.

Modifying IT Operating Data

If IT operating data changes, you must transfer these 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 the effect of a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the database in the case of each affected column in each affected database.

Prerequisites

- The IT operating data of a department, cost center, business roleor a location was changed.

  The view- 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, business role or to a primary location changes, the templates are automatically executed.

To execute the template

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

Old value	Current value of the object property.
New value	Value applied to the object property after modifying the IT operating data.
Selection	Specifies whether the modification is applied 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 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. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

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. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (department, cost center, location or business role).

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

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

   Remove the organizations from **Remove assignments**.
5. Save the changes.

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

   Remove business roles in **Remove assignments**.
5. Save the changes.

Assigning Account Definitions to all Employees

To assign an account definition to all employees

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.

3. Select **Change master data** in the task view.
4. Set the option **Automatic assignment to employees** on the **General** tab.

   IMPORTANT: Only set this option 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.
5. Save the changes.

The account definition is assigned to every employee that is not marked as external. New employees automatically obtain this account definition as soon as they are added. The assignment is calculated by the DBQueue Processor.

NOTE: Disable the option **Automatic assignment to employees** to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees** in the task view.
4. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
5. Save the changes.

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove assignments to system roles in **Remove assignments**.
5. Save the changes.

Adding Account Definitions in the IT Shop

A 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.
- If the account definition is only assigned to employees using IT Shop assignments, you must also set the option **Only for use in IT Shop**. 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

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the account definition to the IT Shop shelf in **Add assignments**
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the account definition from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

1. Select the category **IBM® Notes® | Basic configuration data | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.

5. Click **OK**.

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

For more detailed information about request from company resources through the IT Shop, see the Dell One Identity Manager IT Shop Administration Guide.

Related Topics

- Master Data for an Account Definition on page 36
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 44
- Assigning Account Definitions to Business Roles on page 44
- Assigning Account Definitions Directly to Employees on page 45
- Assigning Account Definitions to System Roles on page 45

Assigning Account Definitions to a Target System

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

- 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 (state "Linked") 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. Select the domain in the category **IBM® Notes® | Domains**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

Deleting an Account Definition

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

NOTE: If an account definition is deleted, the user accounts arising from this account definition are deleted.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Change master data** in the task view.
    d. Disable the option **Automatic assignment to employees** on the **General tab**.
    e. Save the changes.
2. Remove direct assignments of the account definition to employees.
    a. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign to employees** in the task view.
    d. Remove employees from **Remove assignments**.
    e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
    a. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign organizations**.
    d. Remove the account definition's assignments to departments, cost centers and locations in **Remove assignments**.
    e. Save the changes.
4. Remove the account definition's assignments to business roles.
    a. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign business roles** in the task view.

        Remove business roles from **Remove assignments**.
    d. 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, see the .Dell One Identity Manager IT Shop Administration Guide
6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
    a. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.

c. Select **Change master data** in the task view.

d. Remove the account definition from the **Required resource** menu.

e. Save the changes.

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

a. Select the domain in the category **IBM® Notes® | Domains**.

b. Select **Change master data** in the task view.

c. Remove the assigned account definitions on the **General** tab.

d. Save the changes.

8. Delete the account definition.

a. Select the category **IBM® Notes® | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Click , to delete the account definition.

Initial Password for New Notes User Accounts

Table 17: Configuration Parameters for Formatting Initial Passwords for User Accounts

Configuration parameter	Meaning
QER\Person\CentralPasswordHistoryLength	This configuration parameter specifies whether the password history is created. The given value corresponds to the number of unique new passwords that have to be used before an old one can be reused. The employee's central password is tested.
QER\Person\UseCentralPassword	The employee’s central password is automatically mapped to the employee’s user account in all permitted target systems.

Configuration parameter	Meaning
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permanently stored. If the parameter is not set, the central password is only to publicize the target system and is subsequently deleted from the One Identity Manager database.
TargetSystem\NDO\Accounts\InitialPassword	This configuration parameter contains the initial password for creating user accounts. If no password if given when the user account is added, the initial password in the configuration parameter is used.
TargetSystem\NDO\Accounts\InitialRandomPassword	A random generated password is generated when a new user account is added.
TargetSystem\NDO\Accounts\InitialRandomPassword\Character	The random generated password should contain at least one letter [a..z].
TargetSystem\NDO\Accounts\InitialRandomPassword\Length	Specifies how many characters the random generated password has.
TargetSystem\NDO\Accounts\InitialRandomPassword\Numeric	Specifies if the random generated password should contain at least one number [0...9].
TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo	Specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\NDO\DefaultAddress".
TargetSystem\NDO\Accounts\InitialRandomPassword\SpecialCharacter	Specifies whether at least one special character should be included in the random generated password.
TargetSystem\NDO\Accounts\InitialRandomPassword\UpperCase	At least one capital letter must be included in the random generated password [A-Z].
TargetSystem\NDO\MinPasswordLength	Specifies the minimum password length that is set in all newly calculated Notes ID files.

You have the following possible options for issuing an initial password for a new Notes user account.

1. The employee’s central password is mapped to the user account password.
    - Set the configuration parameter "QER\Person\UseCentralPassword" in the Designer.

      If the configuration parameter "QER\Person\UseCentralPassword“ is set, the employee's central password is automatically mapped to an employee's user account in each of the target systems.
    - Use the configuration parameter “QER\Person\UseCentralPassword\PermanentStore” in the Designer to specify whether an employee’s central password is permanently saved in the One Identity Manager database or only until the password has been published in the target system.
    - Set the configuration parameter "QER\Person\UseCentralPassword" in the Designer. This configuration parameter controls the password history. The given value corresponds to the number of unique new passwords that have to be used before an old one can be reused. The employee's central password is tested.
2. A fixed password is automatically entered when the user account is created.
    - Set the configuration parameter "TargetSystem\NDO\Accounts\InitialPassword" and enter the initial password.

      Take into account the minimum password length defined in the configuration parameter "TargetSystem\NDO\MinPasswordLength".

      TIP: To encrypt the password, set the option **Encrypted** for the configuration parameter "TargetSystem\NDO\Accounts\InitialPassword".
3. A random generated password is generated when a new user account is added.
    - Set the configuration parameter "TargetSystem\NDO\UserDefaults\InitialRandomPassword" and its child configuration parameters.

      Use the child parameters to specify the character sets that the password needs to contain and the email address to which the password should be sent.

Related Topics

- Email Notifications about Login Data on page 51

Email Notifications about Login Data

Table 18: Configuration Parameters for Notifications about Login Data

Configuration parameter	Meaning
TargetSystem\ NDO\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. It must contain at least those character sets set in the configuration subparameters.
TargetSystem\NDO \Accounts\InitialRandomPassword\SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee’s manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\NDO\DefaultAddress".

Configuration parameter	Meaning
TargetSystem\NDO\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account).
TargetSystem\NDO\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password).
TargetSystem\NDO\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.

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, which 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.

To use email notifications about login data

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the .Dell One Identity Manager Configuration Guide
2. Enable the configuration parameter "Common\MailNotification\DefaultSender" in the Designer and enter the email address for sending the notification.
3. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the .Dell One Identity Manager Identity Management Base Module Administration Guide
4. Ensure that a language culture can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed information, see the .Dell 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. Set the configuration parameter "TargetSystem\NDO\Accounts\InitialRandomPassword" in the Designer.
2. Set the configuration parameter "TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo" in the Designer and enter the message recipient as value.
3. Set the configuration parameter "TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in the Designer.

   By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.
4. Set the configuration parameter "TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in the Designer.

   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: Change the value of the configuration parameter in order to use custom mail templates for these mails.

Editing a Server

In order to handle IBM® Notes® 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:

- Create an entry for the Job server in the Designer.
- Select an entry for the Job server in the category **Manager | Basic configuration data | Server** in the IBM® Notes® and edit the Job server master 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 Service must be installed, configured and started in order for a server to execute its function in the One Identity Manager network. Proceed as follows in the Dell One Identity Manager Installation Guide.

To edit a Job server and its functions

1. Select the category **IBM® Notes® | Basic configuration data | Server**.
2. Select the Job server entry in the result list.
3. Select **Change master data** in the task view.
4. Edit the Job server's master data.
5. Select **Assign server functions** in the task view and specify server functionality.
6. Save the changes.

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Job server**.

Detailed information about this topic

- Master Data for a Job Server on page 53
- Specifying Server Functions on page 55

Related Topics

- Installing and Configuring the One Identity Manager Service on page 16

Master Data for a Job Server

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Job server**.

Table 19: Job Server Properties

Property	Meaning
Server	Job server name.

Property	Meaning
Full server name	Full server name in accordance with DNS syntax. Example: `<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 properties **Server is cluster** and **Server belongs to cluster** 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. Only the methods “Robocopy” and “Rsync” are currently supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication then takes place between servers with a Windows® operating system using "Robocopy" and between servers with the Linux® operating system using "rsync". If the operating systems of the source and destination servers differ, it is important that the right copy method is 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 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. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. 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. Permitted values are "Win32", "Windows", "Linux" and "Unix". If the input is empty, "Win32" is assumed.

Property	Meaning
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 procedure `QBM_PJobQueueLoad` 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 program "Job Queue Info".
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 being executed.
Server Function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying Server Functions on page 55

Specifying Server Functions

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.

NOTE: More server functions may be available depending on which modules are installed.

Table 20: 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 controller are considered to be member servers.
Printer server	Server which acts as a print server.

Server Function	Remark
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
IBM® Notes® gateway server	Gateway server for synchronizing the One Identity Manager with IBM® Notes®.
IBM® Notes® connector	Server on which the IBM® Notes® connector is installed. This server executes synchronization with the target system IBM® Notes®.
Master SQL server	Server for processing database queries. The server is already entered during initial database schema installation.
Native database connector	The 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 executes synchronization with the target system One Identity Manager.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	The primary domain controller (not for SMB-Based Target Systems).
Profile Server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for running synchronization with an SMB-based target system.
SMTP host	Server from which the One Identity Manager Service sends email notifications. Prerequisite for sending mails using the One Identity Manager Service is SMTP host configuration.
SQL Processing enabled (for load balancing)	The server can run DBQueue Processor SQL tasks (for load balancing). Assign this function to Job servers that do not have the server function Master SQL Server. The system distributes the generated processes through this Job server in addition to the Master SQL Server.
Default report server	Server on which reports are generated.
Windows PowerShell® connector	The server can run Windows PowerShell® version 3.0 or later.

Related Topics

- Master Data for a Job Server on page 53

Target System Managers

For more detailed information about implementing and editing application roles, see Dell One Identity Manager Identity Management Base Module Administration Guide.

Implementing Application Roles for Target System Managers

1. The One Identity Manager administrator assigns employees to be target system managers.
2. These target system managers add employees to the default application role for target system managers.

   The default application role target system managers are entitled to edit all domains in the One Identity Manager.
3. Target system managers can authorize more employees as target system managers, within their scope of responsibilities and create other child application roles and assign individual domains.

Table 21: Default Application Roles for Target System Managers

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | IBM® Notes®** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts, groups or container structures. • Prepare groups for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines 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 One Identity Manager administrator (application role **Base role \| Administrators**)
2. Select the category **One Identity Manager Administration \| Target systems \| Administrators**.
3. Select **Assign employees** in the task view.
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 yourself into the Manager as target system administrator (application role **Target systems \| Administrator**).
2. Select the category **One Identity Manager Administration \| Target systems \| IBM® Notes®**.

3. Select **Assign employees** in the task view.
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. Login to the Manager as target system manager.
2. Select the application role in the category **IBM® Notes® | Basic configuration data | Target system managers** .
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To define target system managers for individual domains

1. Login to the Manager as target system manager.
2. Select the category **IBM® Notes® | Domains**.
3. Select the domain in the result list.
4. Select **Change master data** in the task view.
5. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

   Click  next to the **Target system manager** menu to create a new application role.

   - Enter the application role name and assign the parent application role **Target system | IBM® Notes®**.
   - Click **OK** to add the new application role.
6. Save the changes.
7. Assign the application role to employees, who are authorized to edit the domain in One Identity Manager.

Related Topics

- One Identity Manager Users for Managing an IBM® Notes® System on page 10
- General Master Data for a Notes Domain on page 59

4

Notes Domains

A One Identity Manager domain in IBM® Notes® corresponds to a the image of a specific area in IBM® Notes®, for example a productive environment. Using this construction, which is far more stringently handled in the One Identity Manager than in IBM® Notes®, it is possible to manage several productive IBM® Notes® environments in parallel with a One Identity Manager database. Even if a user's relation to his domain is not maintained in IBM® Notes®, 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.

To edit master data for a domain

1. Select the category **IBM® Notes® | Domains**.
2. Select the domain in the result list.
3. Select **Change master data** in the task view.
4. Edit the domain's master data.
5. Save the changes.

General Master Data for a Notes Domain

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

Table 22: General Master Data for 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. These account definitions are used if automatic assignment of employees to user account is used for this domain resulting in administered user accounts (state "Linked configured"). The account definition's default manage level is applied. User accounts are only linked to the employee (state "Linked") if no account definition is given. This is the case on initial synchronization, for example.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>Target System Managers</td><td>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.</td></tr>
<tr><td>Synchronized by</td><td>Type of synchronization through which data is synchronized between the domain and One Identity Manager.
Table 23: Permitted Values
<table>
<tr><th>Value</th><th>Synchronization by</th><th>Provisioning by</th></tr>
<tr><td>One Identity Manager</td><td>IBM® Notes® connector</td><td>IBM® Notes® connector</td></tr>
<tr><td>FIM</td><td>Microsoft® Forefront® Identity Manager</td><td>Microsoft® Forefront® Identity Manager</td></tr>
<tr><td>No synchronization</td><td>None</td><td>None</td></tr>
</table>
NOTE: You can only specify the synchronization type, if you add a new domain. No changes can be made after saving.
"One Identity Manager" is used when you create a domain with the Synchronization Editor.
NOTE: If you select “No synchronization” you can define custom processes to exchange data between One Identity Manager and the target system.</td></tr>
<tr><td>User ID file path</td><td>Path of the gateway server used for creating new user ID files. This data is only required if the configuration parameter "TargetSystem\NDO\StoreIDInAddressbook" is not set.</td></tr>
<tr><td>Description</td><td>Spare text box for additional explanation.</td></tr>
<tr><td>ID vault enabled</td><td>Specifies whether IBM® Notes® ID vault function is used to restore user ID files.</td></tr>
</table>

Related Topics

- Setting Up Account Definitions on page 35
- Assigning Account Definitions to a Target System on page 47
- Target System Managers on page 57
- Recovering User ID Files on page 98

Specifying Categories for Inheriting Notes Groups

In One Identity Manager, groups can be selectively inherited by user accounts. For this, groups and user accounts are divided into categories. The categories can be freely selected and are specified by a template.

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. Enter your categories for the target system dependent groups in the group table. Each table contains the category items “Position1” to “Position31”.

To define a category

1. Select the category **IBM® Notes® | Domains**.
2. Select the domain in the result list.
3. Select **Change master data** in the task view.
4. Change to the **Categories** tab.
5. Expand the respective base node of the user account or group table.
6. Click  to enable category.
7. Enter a name for the user account and group categories in the current language.
8. Save the changes.

Detailed information about this topic

- Notes Group Inheritance Based on Categories on page 114

How to Edit a Synchronization Project

Synchronization projects, in which a domain is already used as a base object, can also be opened using 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. Select the category **IBM® Notes® | Domains**.
2. Select the domain in the result list. Select **Change master data** in the task view.
3. Select **Edit synchronization project...** from the task view.

Related Topics

- Customizing Synchronization Configuration on page 26

5

Notes Certificates

Certificates are loaded into the One Identity Manager database through synchronization, so they can be referenced when new user accounts are added. User accounts, which 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, the One Identity Manager cannot determine the certificate and therefore cannot allocate it to the user account.

To edit a certificate

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list. Select **Change master data** in the task view.
3. Enter the required data on the master data form.
4. Save the changes.

Detailed information about this topic

- General Master Data for Notes Certificates on page 62

General Master Data for Notes Certificates

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

Table 24: General Master Data for 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.

Property	Description
Mailbox file	Path to the certifier's mailbox file.
ID file name (incl. 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 option **CA process possible** is not set.
Password and password confirmation	Password of the certifier's ID file. This data is only required if the option **CA process possible** is not set.
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 option **CA process possible** is set.
CA database name	Name or path of the CA database file. This data is only required if the option **CA process possible** is set.
Expiry date	Certificate expiry date.
certificate type	Type of certificate.

Notes Certificates Contact Data

Enter the certifier's contact data on the **Contact** tab.

Table 25: 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	Spare text box for additional explanation.

Additional Tasks for Managing Notes Certificates

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Notes Certificates

To obtain an overview of a certificate

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Notes certificate overview** in the task view.

Assigning Owners

Specify which user accounts and groups are entered as certificate document owners.

To specify user accounts as owners of a certificate

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign owner** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as owners of a certificate

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign owner** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Administrators

Specify which user accounts and groups are allowed to administrate the certificate document.

To specify user accounts as administrators for a certificate

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign administrators** in the task view.

4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators for a certificate

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Post-Processing Newly Loaded Certificates

To add new users with One Identity Manager or to recertify existing users, copy the new certificate regularly in the synchronization user's personal address book.

To use new certificates for registering user accounts

1. Copy the certificates from the Domino Directory in the synchronization user's personal address book.

   For more information, see Copying the Notes Certificate on page 15.
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 master data in One Identity Manager. This data is only required for certificates that are not used by the CA process.

   For more information, see General Master Data for Notes Certificates on page 62.

Notes Certificate Requests

Certificate requests are mapped in the 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. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list. Select **Notes certificate overview** in the task view.

3. Select a certificate request on the form element **Notes certificate requests**.
4. Select **Change master data** in the task view.

Table 26: Notes Certificate Request Master Data

Property	Description
Object	Name of the certified object.
CA certificate	Name of the certificate to use for certification.
Issuer	Name of the official certifier.
Certificate	Unique certificate identifier.
Notes domain	Certificate request's domain.
State of request	Current state of the certificate request.

6

Notes Templates

To allow the IBM® Notes® 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. You will find Notes templates in One Identity Manager for this purpose.

To edit a template's master data

1. Select the category **IBM® Notes® | Notes templates**.
2. Select the template in the result list. Select **Change master data** in the task view.
3. Enter the required data on the master data form.
4. Save the changes.

Table 27: Notes Template Master Data

Property	Description
Notes template	Template name.
Notes domain	Domain in which to apply the template.
File Name	Name of the template file.

7

Notes Policies

You can use policies to specify settings to apply to Notes users and groups. Policies and policy settings can be loaded into the One Identity Manager database and assigned to user accounts by synchronization. The policies can be assigned to user accounts and groups as members, owners or administrators.

To display policy master data

1. Select the category **IBM® Notes® | Notes policies**.
2. Select the policy from the result list. Select **Change master data** in the task view.

Table 28: Notes Policy Master 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.
Notes 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.

Related Topics

- Notes Policy Settings on page 71

Additional Tasks for Managing Notes Policies

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Notes Policies

To obtain an overview of a policy

1. Select the category **IBM® Notes® | Policies**.
2. Select the policy in the result list.
3. Select **Notes policy overview** in the task view.

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. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign members** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To assign groups to a policy

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign members** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
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. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign owner** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as owner

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign owner** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
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. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators

1. Select the category **IBM® Notes® | Certificates**.
2. Select a certificate in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Notes Policy Settings

The policy settings mapped in One Identity Manager are those used in synchronized Notes policies.

To display policy settings master data

1. Select the category **IBM® Notes® | Notes policies**.
2. Select a policy in the result list. Select **Change master data** in the task view.
3. Select an assigned policy setting and open the context menu.
4. Click **Go to assigned object**.
5. Select **Change master data** in the task view.

Table 29: Master Data of a Notes Policy Setting

Property	Description
Full name	Full name of the policy setting.
Description	Describes the policy setting.
Setting type	Type of policy setting.
Notes domain	Policy setting domain.

Related Topics

- Notes Policies on page 68

8

Notes user accounts

Use the One Identity Manager to manage users and employee documents in IBM® Notes®. 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

- Linking User Accounts to Employees on page 72
- Supported User Account Types on page 73
- Entering Master Data for Notes User Accounts on page 76

Linking User Accounts to Employees

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems. One Identity Manager provides the possibility to manage 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, the One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.

- Employees and user accounts can be entered manually and assigned to each other.
- Employees can automatically obtain their account definitions using user account resources. If an employee does not 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 mechanism followed by process handling.

When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.

> **NOTE:** If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, primary location or a primary cost center.

- An existing employee is automatically assigned when a user account is added or a new employee is created if necessary. In this case, employee master data is created on the basis of the existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. This method, however, is not the One Identity Manager default method. Define criteria for finding employees for automatic employee assignment.

Related Topics

- Entering Master Data for Notes User Accounts on page 76
- Setting Up Account Definitions on page 35
- Automatic Assignment of Employees to User Accounts on page 92
- For more detailed information about employee handling and administration, see the Dell One Identity Manager Target System Base Module Administration Guide.

Supported User Account Types

Different types of user accounts, such as default user accounts, administrative user accounts or service accounts, can be mapped in One Identity Manager. The following properties are used for mapping different user account types.

- Identity (column `IdentityType`)

  The identity describes the type of user account.

  Table 30: Identities of user accounts

Identity	Description	Value in "IdentityType" Column
Primary identity	Default user account of an employee.	Primary
Organizational identity	Secondary user account used for various roles within the organization, f. ex. In sub-agreements with other functional areas.	Organizational
Personalized admin identity	User account with administration rights used by one person.	Admin
Sponsored identity	User account used for example for training purposes.	Sponsored
Shared identity	User account with administration rights used by several people.	Shared

Identity	Description	Value in "IdentityType" Column
Service identity	Service account.	Service

- Privileged user account (column `IsPrivilegedAccount`)

  Use this option to flag user accounts with special, privileged permissions. This includes administrative user accounts or service accounts, for example. This option is not used to flag default user accounts.

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.

The One Identity Manager supplies a default configuration for manage levels:

- unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other 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 a manage level of "Full managed" inherit specific properties from the assigned employee.

NOTE: The manage levels "Full managed" and "Unmanaged" are evaluated in the 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.

To create default user accounts

1. Create an account definition and assign the manage level "Unmanaged" or "Full managed" to it.
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.

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

   - Use the default value "1" in the formatting rule for the column `IsGroupAccount` and set the option **Always use default value**.

- Use the default value "primary" in the formatting rule for the column `IdentityType` and set the option **Always use default value**.

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

   In order for an employee to create user accounts with the manage level “Full managed”, the necessary IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. 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.

5. Assign the account definition 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. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

Administrative User Accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are normally predefined in the target system and have fixed identifiers and login names, for example, "Administrator".

Administrative user accounts are loaded through synchronization into the One Identity Manager. To assign a manager to administrative user accounts, assign an employee to the user account in One Identity Manager.

Privileged User Accounts

Privileged user accounts are used to provide employees with additional privileges.

To create a privileged user account

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 properties for privileged user accounts being overwritten, set the property **IT operating data overwrites** for the manage level, to the value "Only initially". In this case, the properties are populated just once when the user accounts is created.
3. 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.
4. Create a formatting rule for IT operating data.

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center,

location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

- Use the default value "1" in the formatting rule for the column `IsPrivilegedAccount` and set the option **Always use default value**.
- You can also specify a formatting rule for the column `IdentityType`. The column owns different permitted values, which represent user accounts.
- To prevent privileged user accounts inheriting default user groups, define a template for the column `IsGroupAccount` with the default value "0" and set the option **Always use default value**.

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.

NOTE: You can automatically label administrative user accounts as privileged user accounts. To do this, set the schedule "Mark selected user accounts as privileged" in the Designer.

The criteria used to label user accounts as privileged are defined as extensions to the view definition (ViewAddOn) on the table `TSBVAccountIsPrivDetectRule` (table type "Union"). The evaluation is done in the script `TSB_SetIsPrivilegedAccount`. The user accounts are marked with the property **Privileged user account** (`IsPrivilegedAccount`).

NOTE: Specify a formatting rule for a naming schema if it is required by the company for privileged user account login names.

Entering Master Data for Notes User Accounts

A user account can be linked to an employee in the 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 master data described in the following is mapped through templates from employee master data.

NOTE: If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, primary location or a primary cost center.

To edit master data for a user account

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list and run the task **Change master data**.

   - OR-

   Click  in the result list toolbar.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list and run **Assign Notes user accounts** from the task view.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic

- General Master Data for a Notes User Account on page 77
- Additional Master Data for Notes User Accounts on page 82
- Notes User Account Email System on page 80
- Notes User Account Address Data on page 82
- Administrative Data for a Notes User Account on page 83

Related Topics

- Setting Up Account Definitions on page 35
- Supported User Account Types on page 73
- Linking User Accounts to Employees on page 72

General Master Data for a Notes User Account

Table 31: Configuration Parameters for Setting up User Accounts

Configuration parameter	Active Meaning
QER\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is set, values can be entered and calculated for the risk index.

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

Table 32: General Master Data for 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 use automatic employee assignment, an associated employee is created and entered into the user account when the user account is saved.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The 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. To create the user account manually through an account definition, enter an employee in the **Employee** box. You can select all the account definitions assigned to this employee and through which no user account has been created for this employee.
Manage level	User account's manage level. 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.
Organizational unit	Additional organization unit belonging to the user account.
Full name	Full name of the user account. Full name is made up of the first name, last name, certificate and organizational unit.
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.

Property	Description
Generational affix	User's generational affix, for example "Junior".
Alternative name	Alternative name in the user's native language. This can be used to display and search for names in IBM® Notes®. The alternative name has to linked to one of the user account's alternative language.
Alternative language	Alternative language for the alternative names.
Email system	Type of email system used by the user. "1 - Notes" is entered by default. The other input fields shown on the master data form depend on the type of email system selected.
Risk index (calculated)	Maximum risk index values for all assigned groups. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information, see the .Dell One Identity Manager Risk Assessment Administration Guide
Notes category	Categories for the inheritance of groups by the user account. Select one or more categories from the menu. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories.
User account is disabled	Specifies whether the user account is blocked from logging in to the domain.
Identity	User account's identity type **Table 33: Permitted values for the identity.** **Value** / **Description** 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 admin identity — User account with administrative permissions, used by one employee. Sponsored identity — User account that is used for training purposes, for example. Shared identity — User account with administrative permissions, used by several employees. Service identity — Service account.
Privileged user account	Specifies whether this is a privileged user account.

Property	Description
Groups can be inherited	Specifies whether the user account groups can inherit through the employee. If this option is set, the user account inherits groups through hierarchical roles or 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

- Setting Up Account Definitions on page 35
- Linking User Accounts to Employees on page 72
- Supported User Account Types on page 73
- Notes User Account Email System on page 80
- Specifying Categories for Inheriting Notes Groups on page 60
- Locking and Unlocking Notes User Accounts on page 100

Notes User Account Email System

Table 34: Configuration Parameters for Creating a Mailbox File

Configuration parameter	Active Meaning
TargetSystem\NDO\CreateMailDB	This configuration parameter specifies whether the mailbox is created after or while the Notes user is registering with the target system. If the configuration parameter is set, the mailbox is created during registration. This uses the template of the Notes server on which the user is registered. If the configuration parameter is not set (default), the mailbox is created after the Notes user has registered. This uses the template given in the user account or in the configuration parameter "TargetSystem\NDO\DefTemplatePath".
TargetSystem\NDO\DefTemplatePath	Template for adding the mailbox on a Notes server.
TargetSystem\NDO\MailFilePath	Directory on the mail server, in which the user account's mailbox files are stored.

Select the email system that the user uses from the **Email system** menu on the general master 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 will be 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 name are required for the selected email system. Enter the data necessary to create the mailbox file.

Table 35: 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 option **Has Notes mailbox files** 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 the configuration parameter "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 configuration parameter "TargetSystem\NDO\MailFilePath". To use another directory, edit the value of this configuration parameter in the Designer.
NOTES POP or IMAP	Mailbox display name	Display name of the mailbox. This is made up by template, of the first and last names to which "Mailbox" is appended.
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 IBM® Notes® 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 option **Has Notes mailbox files** are available.
X.400	X.400 address	User's mail address in X.400 format (including domain name).

Detailed information about this topic

- Generating Mailbox Files on page 96

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 master data depending on the manage level of the user account.

Additional Master Data for 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

- Configure and enable the schedule "Load Designer user mail file sizes" in the IBM® Notes®.

  For more detailed information about configuring schedules, see the Dell One Identity Manager Configuration Guide.

Table 36: Additional Master Data for Notes User Accounts

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.
Sametime server	Notes server used as a Sametime server. Enter a Sametime server for user accounts, which use the IBM® Notes® Sametime function.
Calendar domain	Domain, which applies if the user account uses another calendar and schedule functionality.
Website	The user's website.
Comment	Spare text box for additional explanation.

Administrative Data for a Notes User Account

Enter the administrative data of a user account on the **Admininstration** tab.

Table 37: 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. **NOTE:** Policy settings basically replace all the user account settings.

Property	Description	
Password check type	Specifies how users must authenticate themselves on the server. Password check types are:	
	0 - don't check:Password not checked	The user must not provide a password to log in on the server. The user must not provide a password to log in on the server.
	1 - check:	Password checked The user must provide a password to log in to the server.
	2 - Lockout ID:	ID is locked The user cannot log in on any server in the domain which checks passwords.
	When a new user is added the password check type "0 - don't check" is entered 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. Depending on the configuration parameter "Person\UseCentralPassword" the employee's central password can be mapped to the user account's password. If you use an initial password for the user accounts, it is automatically entered when a user account is created.	
Change password on next login	Specifies whether the user account password must be changed on the next login.	

Property	Description
Notes client license	License type of the Notes client. The license type determines the range of user access. Possible license types are: • 0 - IBM® Notes® • 1 - IBM® Notes® Mail • 2 - IBM® Notes® Desktop • 3 - IBM® Notes® Designer • 4 - IBM® Notes® Administration • 5 - IBM® iNotes®/Domino® CAL The license type "0 -IBM® Notes® " is entered by default when a new user account is added.
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 IBM® Notes® and other systems, for example Active Directory®.
ID expires	User ID file's expiry date. The expiry date is calculated using a template. User ID file for enabled user accounts, which will expire in less that 10 days can be extended by 2 years. ***To extend the expiry date*** • Configure and set the schedule "Automatically extend IBM® Notes® ID expiry data" in the Designer. For more detailed information about configuring schedules, see the Dell One Identity Manager Configuration Guide.

Related Topics

- Notes server on page 128
- Initial Password for New Notes User Accounts on page 49

Additional Tasks for Managing Notes User Accounts

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Notes User Accounts

To obtain an overview of a user account

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Notes user account overview** in the task view.

Changing the Manage Level of a User Account

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. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Select the manage level in the **Manage level** menu on the tab **General**.
5. Save the changes.

Related Topics

- General Master Data for a Notes User Account on page 77

Assigning Notes Groups Directly to Notes User Accounts

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, like 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 the user account.

To assign groups directly to user accounts

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**. To filter the groups, select a domain in **Notes domains**.

   The view- OR -

   Remove groups from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Notes Groups to Notes User Accounts on page 105

Specifying Document Owners

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 an owner for user accounts

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify an owner for groups

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Group** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To specify an owner for mail-in databases

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Mail-in DB** tab.
5. Assign mail-in databases in **Add assignments**.

   - OR -

   Remove the mail-in database in **Remove assignments**.
6. Save the changes.

To specify an owner for certificates

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Certificate** tab.
5. Assign certificates in **Add assignments**.

   - OR -

   Remove certificates in **Remove assignments**.
6. Save the changes.

To specify an owner for server documents

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Server document** tab.
5. Assign the server documents in **Add assignments**.

   - OR -

   Remove server documents in **Remove assignments**.
6. Save the changes.

Assigning Owners

Specify which user accounts and groups are allowed to edit the selected user account.

To specify user accounts as owner

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign owner** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as owner

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign owner** in the task view.

4. Select the **Group** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Administrable Documents

Specify which documents the user account should administrate. You can only assign documents belonging to the same domain as the user account.

To specify the user account administrator

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify an administrator for groups

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Group** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To specify an administrator for mail-in databases

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Mail-in DB** tab.
5. Assign mail-in databases in **Add assignments**.

   - OR -

Remove the mail-in database in **Remove assignments**.

6. Save the changes.

To specify an administrator for certificates

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Certificate** tab.
5. Assign certificates in **Add assignments**.

   - OR -

   Remove certificates in **Remove assignments**.
6. Save the changes.

To specify an administrator for servers

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Server** tab.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

To specify an administrator for server documents

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Server document** tab.
5. Assign the server documents in **Add assignments**.

   - OR -

   Remove server documents in **Remove assignments**.
6. Save the changes.

Assigning Administrators

Specify which user accounts and groups are allowed to administrate the selected user account.

To specify user accounts as administrators

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrators** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrators** in the task view.
4. Select the **Groups** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Maintaining Additional and Excluded Lists

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. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Maintain excluded and additional** in the task view.
4. Select the **Additional** tab.
5. Assign the groups in whose additional list the user account is to be a member in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To add a user account to a dynamic group's excluded list

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Maintain excluded and additional** in the task view.

4. Select the **Excluded** tab.
5. Assign the groups in whose excluded list the user account is to be a member in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Extended Properties

Extended properties are meta objects that cannot be mapped directly in the One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a user account

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties in **Remove assignments**.
5. Save the changes.

For more detailed information about setting up extended properties, see the Dell One Identity Manager Identity Management Base Module Administration Guide.

Automatic Assignment of Employees to User Accounts

Table 38: Configuration Parameters for Synchronizing a Notes Domain

Configuration parameter	Meaning
TargetSystem\NDO\PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\NDO\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\NDO\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern.

When you add a user account, an existing employee can be assigned automatically or added if necessary. In the process, the employee master data is created based for existing user master data. This mechanism can follow

on after a new user account has been created 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 assignment 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 the task **Change master data** to assign employees to administrative user account for the respective user account.

Run the following tasks to assign employees automatically.

- If employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\NDO\PersonAutoFullsync" in the Designer and select the required mode.
- If employees can be assigned by user accounts outside synchronization, set the parameter "TargetSystem\NDO\PersonAutoDefault" in the Designer and select the required mode.
- Specify the user accounts in the configuration parameter "TargetSystem\NDO\PersonExcludeList" which must not be assigned automatically to employees.

  Example:

  ```
  Administrator
  ```

- Assign an account definition to the domain. Ensure the manage level to be used is entered as 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: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the domain at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
   a. Select the category **IBM® Notes® | User accounts | Linked but not configured | <Domain>**.
   b. Select the task **Assign account definition to linked accounts**.

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

Related Topics

- Creating an Account Definition on page 35
- Assigning Account Definitions to a Target System on page 47
- Editing Search Criteria for Automatic Employee Assignment on page 94

Editing Search Criteria for Automatic Employee Assignment

Criteria for employee assignment are defined in the domain. In this case, 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 criteria are written in XML notation in the column "Search criteria for automatic employee assignment" (`AccountToPersonMatchingRule`) of 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: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given 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.

It is not recommended to make assignment to administrative user accounts based on search criteria. Use the task **Change master data** to assign employees to administrative user account for the respective user account.

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.

To define employee assignment criteria for a Notes domain

1. Select the category **IBM® Notes® | Domains**.
2. Select the domain in the result list.
3. Select **Define search criteria for employee assignment** in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 39: Default Search Criteria for User Accounts

Apply to	Column on Employee	Column on 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.

Direct Assignment of Employees to User Accounts Based on a Suggestion List

You can create a suggestion list in the "Assignments" view for assignments of employees to user accounts based on the search criteria. User accounts are grouped in different views for this.

Table 40: 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.

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

To apply search criteria to user accounts

- 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.

To assign employees directly over a suggestion list

1. Click **Suggested assignments**.
   a. Click **Select** for all user accounts to be assigned to the suggested employee. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

      The selected user accounts are assigned to the employees found using the search criteria.

   - OR -

2. Click **No employee assignment**.
   a. Click **Select employee...** for the user account to which you want to assign the employee. Select an employee from the menu.
   b. Click **Select** for all user accounts to which you want to assign the selected employees. Multi-select is possible.
   c. Click **Assign selected**.
   d. Confirm the security prompt with **Yes**.

      This assigns the selected user accounts to the employees shown in the "Employee" column.

To remove assignments

1. Click **Assigned user accounts**.
    a. Click **Select** for all user accounts whose employee assignment you want to remove. Multi-select is possible.
    b. Click **Delete selected**.
    c. Confirm the security prompt with **Yes**.

       The assigned employees are deleted from the selected user accounts.

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

Related Topics

- Automatic Assignment of Employees to User Accounts on page 92

Generating Mailbox Files

Table 41: Configuration Parameters for Creating a Mailbox File

Configuration parameter	Active Meaning
TargetSystem\NDO\CreateMailDB	This configuration parameter specifies whether the mailbox is created after or while the Notes user is registering with the target system. If the configuration parameter is set, the mailbox is created during registration. This uses the template of the Notes server on which the user is registered. If the configuration parameter is not set (default), the mailbox is created after the Notes user has registered. This uses the template given in the user account or in the configuration parameter "TargetSystem\NDO\DefTemplatePath".
TargetSystem\NDO\DefTemplatePath	Template for adding the mailbox on a Notes server.
TargetSystem\NDO\MailFilePath	Directory on the mail server, in which the user account's mailbox files are stored.

If and in what way mailboxes are created in IBM® Notes® depends on the user account data and the configuration parameter settings. The mailbox path and file name must be supplied with the user account in order to create a mailbox. If this information is missing, the mailbox file cannot be created.

The configuration parameter "TargetSystem\NDO\CreateMailDB" is not set (default)

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 user account, the template given in the configuration parameter "TargetSystem\NDO\DefTemplatePath" is used. The template must exist on the gateway server.

The configuration parameter "TargetSystem\NDO\CreateMailDB" is set.

If it is necessary to create the mailbox during the Notes user's registration, set the configuration parameter "TargetSystem\NDO\CreateMailDB". In this case, the template of the Notes server's on which the user is

registered is used.

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.

Only set this configuration parameter to prevent the IBM® Notes® connector from accessing the mailboxes.

Related Topics

- Notes User Account Email System on page 80
- Additional Master Data for Notes User Accounts on page 82

Saving User ID Files

Table 42: Configuration Parameters for Creating a Mailbox File

Configuration parameter	Meaning
TargetSystem\NDO\StoreIDInAddressbook	This configuration parameter control the behavior of ID files for new user accounts. If the configuration parameter is set, the ID files are attached to the employee document. If this configuration parameter is no set, the ID file is stored on the gateway server.

The IBM® Notes® connector requires the information about where the ID files for the new user accounts ahould be stored in the IBM® Notes® environment. User ID files can be added to the employee document as an attachment or stored on the gateway server. Set the desired behavior in the configuration parameter "argetSystem\NDO\StoreIDInAddressbook". Enter the path for saving the User ID files if they are going to be stored on the on the gateway server.

By default, the IBM® Notes® connector uses the path stored in the domain. If a default path is not given, you can add the path to the user accounts' mail servers.

NOTE: If there is no path given either in the domain or the mail server, use the default IBM® Notes® connector path, which is stored with the variable `UserIDFilesDefaultPath` in the synchronization project. If you want to change the variable value, customize the synchronization configuration. For more detailed information about variables and variable sets, see the Dell One Identity Manager Target System Synchronization Reference Guide.

To specify the user ID file location on the gateway server

1. Disable the configuration parameter "TargetSystem\NDO\StoreIDInAddressbook" in the Designer.
2. Edit the domain's master data in the Manager and enter the user ID files path.

Detailed information about this topic

- General Master Data for a Notes Domain on page 59
- General Master Data for Notes Servers on page 128
- Notes User Account Email System on page 80

Recovering 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 IBM® Domino® version 8.5, IBM® Notes® provides the ID vault function to do this.

The 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 IBM® 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!

ID vault

The ID Vault is a IBM® Domino® database that stores copies of user ID files. This allows IBM® Notes® to be able to restore user ID files and to reset user account passwords. The One Identity Manager provides a process for resetting the passwords in the ID vault.

Prerequisites

- The Domino server, which communicates with the gateway server, is also the ID vault server.
- There are executing permissions defined for agents for the synchronization user account. For more information, see Running Restricted LotusScript®/Java Agents on page 145.
- ID vault database permissions for the synchronization user account are set: access function "Manager" and role "Auditor". For more detailed information, see your IBM® Notes® documentation.
- Permissions for restoring passwords of the synchronization administrative user account and the ID vault server are set. For more detailed information, see your IBM® Notes® documentation.

To use the ID vault

1. Select the category **IBM® Notes® | Domains**.
2. Select the domain you want to use for the ID vault in the result list and run **Change master data** in the task view.
3. Set the option **ID vault enabled**.

   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 IBM® Notes®, 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 the IBM® Notes® environment the One Identity Manager saves the initial password in the One Identity Manager database (`NotesUser.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 the One Identity Manager. The initial password for all other user accounts has to be transferred to the One Identity Manager database with a customized process.

To reset a user account password

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **ID restore** in the task view.

This task starts the process `NDO_NDOUser_PWReset_from_Vault`. The password from the user ID file saved in ID Vault is replaced by the initial password from the One Identity Manager database by this process. If the user is logged into the IBM® 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 IBM® Notes® client is started the next time. If the user is not logged into the IBM® 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.

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. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **ID restore** in the task view.

   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.
   - Updates the restored employee documents with 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 19

Locking and Unlocking Notes User Accounts

Table 43: Configuration Parameters for Locking/Unlocking User Accounts

Configuration parameter	Meaning
TargetSystem\NDO\MailBoxAnonymPre	Prefix for user account anonymity.
QER\Person\TemporaryDeactivation	This configuration parameter specifies whether user accounts for an employee are locked if the employee is temporarily or permanently disabled.

A user is considered to be locked in IBM® Notes® 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 permissions type "Not access server" 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 permissions type “Not access server” 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. User accounts with the manage level “Full managed” are disabled depending on the account definition settings. For user accounts with another manage level, modify the column template `NDOUser.AccountDisabled` accordingly.

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 configuration parameter “QER\Person\TemporaryDeactivation”.

- If the configuration parameter is set, the employee’s user accounts are locked if 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 a user account when the configuration parameter is disabled

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To lock a user account, which is not linked to an employee

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
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 configuration parameter "TargetSystem\NDO\MailBoxAnonymPre" is checked if the user is made anonymous.

To unlock a user account

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Disable the option **Account is disabled** 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

- Denied Access Groups on page 121

Related Topics

- Setting Up Account Definitions on page 35
- Setting Up Manage Levels on page 37

Deleting Notes User Accounts

If a user account is deleted in One Identity Manager, it is initially marked for deletion. The user account is therefore locked. Depending on the deferred deletion setting, the user account is either deleted immediately from the address books and One Identity Manager database or at a later date.

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 created through this account definition, is deleted.

To delete a user account

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Click  to delete the user account.
4. Confirm the security prompt with **Yes**.

To restore user account

1. Select the category **IBM® Notes® | User accounts**.
2. Select the user account in the result list.
3. Click  in the result list toolbar.

Configuring Deferred Deletion

By default, user accounts are finally deleted from the database after 30 days.The user accounts are initially disabled. You can reenable the user accounts until deferred deletion is run. After deferred deletion is run, the user account are deleted from the database and cannot be restored anymore. You can configure an alternative deletion delay on the table `NDOUser` in the Designer.

Related Topics

- Locking and Unlocking Notes User Accounts on page 100

9

Notes groups

Users, mail-in databases, groups and servers can be grouped together into Notes groups. IBM® Notes® divides groups into different group types. The groups type specifies the group's intended purpose and whether the group is visible in the Domino Directory.

To edit group master data

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list. Select **Change master data** in the task view.

   - OR -

   Click  in the result list toolbar.
3. Edit the group's master data.
4. Save the changes.

Detailed information about this topic

- General Master Data for Notes Groups on page 103

General Master Data for Notes Groups

Table 44: Configuration Parameters for Setting up User Accounts

Configuration parameter	Active Meaning
QER\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is set, values can be entered and calculated for the risk index.

Enter the following data for groups.

Table 45: General Master Data for a Notes Group

Property	Description
Group	Name of the group.
Display name	Display name of the group.

Property	Description
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. Enter a value between 0 and 1. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information, see the Dell One Identity Manager Risk Assessment Administration Guide.
Notes category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Use this menu to allocate one or more categories to the group. For more detailed information, see the Dell One Identity Manager Target System Base Module Administration Guide.
Import dynamic members	Method for specifying members of a dynamic group. Select "Home server" if the group members are determined dynamically from the home server members. Excluded and additional lists are synchronized for this group. Select "none" if the group is not dynamic.
Description	Spare text box 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. This group can be requested by staff through the Web Portal and granted through a defined approval process. The group can still be assigned directly to hierarchical roles. For more detailed information, see the Dell One Identity Manager IT Shop Administration Guide.

Property	Description
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted through a defined approval process. The group may not be assigned directly to hierarchical roles.
Dynamic group	Specifies whether this is a dynamic group. This option is set depending on the setting of property "Import dynamic members".

Detailed information about this topic

- Extension Groups on page 122
- Specifying Categories for Inheriting Notes Groups on page 60
- Dynamic Groups on page 122
- Denied Access Groups on page 121

Assigning Notes Groups to Notes User Accounts

Groups can be assigned directly or indirectly to employees. In the case of indirect assignment, employees and 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 hierarchical roles and that employee owns a user account, this user account is added to the group. Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and groups is permitted for role classes (department, cost center, location or business role).
- User accounts are marked with the option **Groups can be inherited**.
- User accounts and groups belong to the same domain.

Furthermore, groups can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that groups can be assigned through IT Shop requests. All groups are assigned to this shop can be requested by the customers. Requested groups are assigned to the employees after approval is granted.

For more detailed information about inheriting company resources, see the Dell One Identity Manager Identity Management Base Module Administration Guide.

Detailed information about this topic

- Assigning Notes Groups to Departments, Cost Centers and Locations on page 106
- Assigning Notes Groups to Business Roles on page 107
- Assigning Notes User Accounts directly to an Notes Group on page 107
- Adding Notes Groups to System Roles on page 108
- Adding Notes Groups to the IT Shop on page 109

Assigning Notes Groups to Departments, Cost Centers and Locations

Assign groups to departments, cost centers and locations in order to assign user accounts to them through these organizations.

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

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

   Remove the organizations from **Remove assignments**.
5. Save the changes.

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

1. Select the category **Organizations | Departments**.

   The view- OR -

   Select the category **Organizations | Cost centers**.

   The view- OR -

   Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign Notes groups**.
4. Assign groups in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Notes Groups to Business Roles on page 107
- Assigning Notes User Accounts directly to an Notes Group on page 107
- Adding Notes Groups to System Roles on page 108
- Adding Notes Groups to the IT Shop on page 109
- One Identity Manager Users for Managing an IBM® Notes® System on page 10

Assigning Notes Groups to Business Roles

Installed Module: Business Roles Module

You assign groups to business roles in order to assign them to user accounts over business roles.

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

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

   Remove business roles from **Remove assignments**.
5. Save the changes.

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

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign Notes groups**.
4. Assign groups in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Notes Groups to Departments, Cost Centers and Locations on page 106
- Assigning Notes User Accounts directly to an Notes Group on page 107
- Adding Notes Groups to System Roles on page 108
- Adding Notes Groups to the IT Shop on page 109
- One Identity Manager Users for Managing an IBM® Notes® System on page 10

Assigning Notes User Accounts directly to an 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 a group directly to user accounts

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign members** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**. To filter the user accounts in the list, select a domain in **Notes domains**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning Notes Groups Directly to Notes User Accounts on page 86
- Assigning Notes Groups to Departments, Cost Centers and Locations on page 106
- Assigning Notes Groups to Business Roles on page 107
- Adding Notes Groups to System Roles on page 108
- Adding Notes Groups to the IT Shop on page 109
- Assigning Owners to Notes Groups on page 119
- Assigning Administrators to Notes Groups on page 120

Adding Notes Groups to System Roles

Installed Modules: System Roles Module

Use this task to add a group to system roles. If you assign a system role to employees, all the employees' user accounts inherit the group.

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

To assign a group to system roles

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove system roles from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Notes Groups to Departments, Cost Centers and Locations on page 106
- Assigning Notes Groups to Business Roles on page 107
- Assigning Notes User Accounts directly to an Notes Group on page 107
- Adding Notes Groups to the IT Shop on page 109

Adding Notes Groups to the IT Shop

Once a group has been assigned 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 must be labeled with the option **IT Shop**.
- The group must be assigned to a service item.
- The group must be labeled with the option **Only use in IT Shop** if the group can only be assigned to employees through IT Shop requests. Direct assignment to hierarchical roles may not be possible.

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

To add a group to the IT Shop

1. Select the category **IBM® Notes® | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Notes groups** (role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the group to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove a group from individual IT Shop shelves.

1. Select the category **IBM® Notes® | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Notes groups** (role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the group from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove a group from all IT Shop shelves.

1. Select the category **IBM® Notes® | Groups** (non role-based login).

   - OR -

Select the category **Entitlements | Notes groups** (role-based login).

2. Select the group in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   This removes the group from all One Identity Manager Service shelves. All requests and assignment requests with this group are canceled in the process.

For more detailed information about request from company resources through the IT Shop, see the Dell One Identity Manager IT Shop Administration Guide.

Related Topics

- General Master Data for Notes Groups on page 103
- Assigning Notes Groups to Departments, Cost Centers and Locations on page 106
- Assigning Notes Groups to Business Roles on page 107
- Assigning Notes User Accounts directly to an Notes Group on page 107
- Adding Notes Groups to System Roles on page 108

Additional Tasks for Managing Notes Groups

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Notes Groups

To obtain an overview of a group

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Notes group overview** in the task view.

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. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign members** in the task view.
4. Select the **Mail-in DB** tab.
5. Assign mail-in databases in **Add assignments**. To filter the mail-in databases in the list, select a domain in **Notes domains**.

   - OR -

   Remove the mail-in database in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning Notes User Accounts directly to an Notes Group on page 107
- Assigning Notes Servers to a Notes Group on page 111
- Adding Notes Groups to Notes Groups on page 111

Assigning Notes Servers to a Notes Group

You can assign Notes servers directly to a group.

To assign servers to a group

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign members** in the task view.
4. Select the **Server** tab.
5. Assign the servers in **Add assignments**. To filter the server in the list, select a domain in **Notes domains**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning Notes User Accounts directly to an Notes Group on page 107
- Assigning Notes Mail-In Databases to Notes Groups on page 110
- Adding Notes Groups to Notes Groups on page 111

Adding Notes Groups to Notes Groups

You can assign parent or child groups to a Notes group.

To assign child groups

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign members** in the task view.
4. Select the **Groups** tab.
5. Assign child groups in **Add assignments**. To filter the groups, select a domain in **Notes domains**.

   - OR -

   Remove child groups in **Remove assignments**.
6. Save the changes.

To assign parent groups

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign parent groups**.
4. Assign parent groups in **Add assignments**. To filter the groups, select a domain in **Notes domains**.

   - OR -

   Remove parent groups in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Notes User Accounts directly to an Notes Group on page 107
- Assigning Notes Servers to a Notes Group on page 111
- Assigning Notes Mail-In Databases to Notes Groups on page 110

Effectiveness of Group Memberships

Table 46: Configuration Parameter for Conditional Inheritance

Configuration parameter	Active Meaning
QER\Structures\Inherite\GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. Changes to the parameter require recompiling the database.

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 directly, indirectly or by IT Shop request at any time. 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.

The effect of the assignments is mapped in the tables `NDOUserInGroup` and `BaseTreeHasNDOGroup` through the column `XIsInEffect`.

Example of the effect of group memberships

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

Clara Harris has a user account in this domain. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her 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 47: Specifying excluded groups (table `NDOGroupExclusion`)

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

Table 48: Effective Assignments

Employee	Member in Role	Effective Group
Ben King	Marketing	Group A
Jan Bloggs	Marketing, finance	Group B
Clara Harris	Marketing, finance, control group	Group C
Jenny Basset	Marketing, control group	Group A, Group C

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

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

Table 49: Excluded groups and effective assignments

Employee	Member in Role	Assigned Group	Excluded Group	Effective Group
Jenny Basset	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

- The configuration parameter “QER\Inherite\GroupExclusion” is enabled.
- The mutually exclusive groups belong to the same domain

To exclude a group

1. Select the category **IBM® Notes® | Groups**.
2. Select a group in the result list.
3. Select **Exclude groups** in the task view.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.

   - OR -

   Remove the conflicting groups that are no longer mutually exclusive in **Remove assignments**.
5. Save the changes.

Notes Group Inheritance Based on Categories

In One Identity Manager, groups can be selectively inherited by user accounts. For this, groups and user accounts are divided into categories. The categories can be freely selected and are specified by a template. 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. Enter your categories for the target system dependent groups in the group table. Each table contains the category items “Position1” to “Position31”.

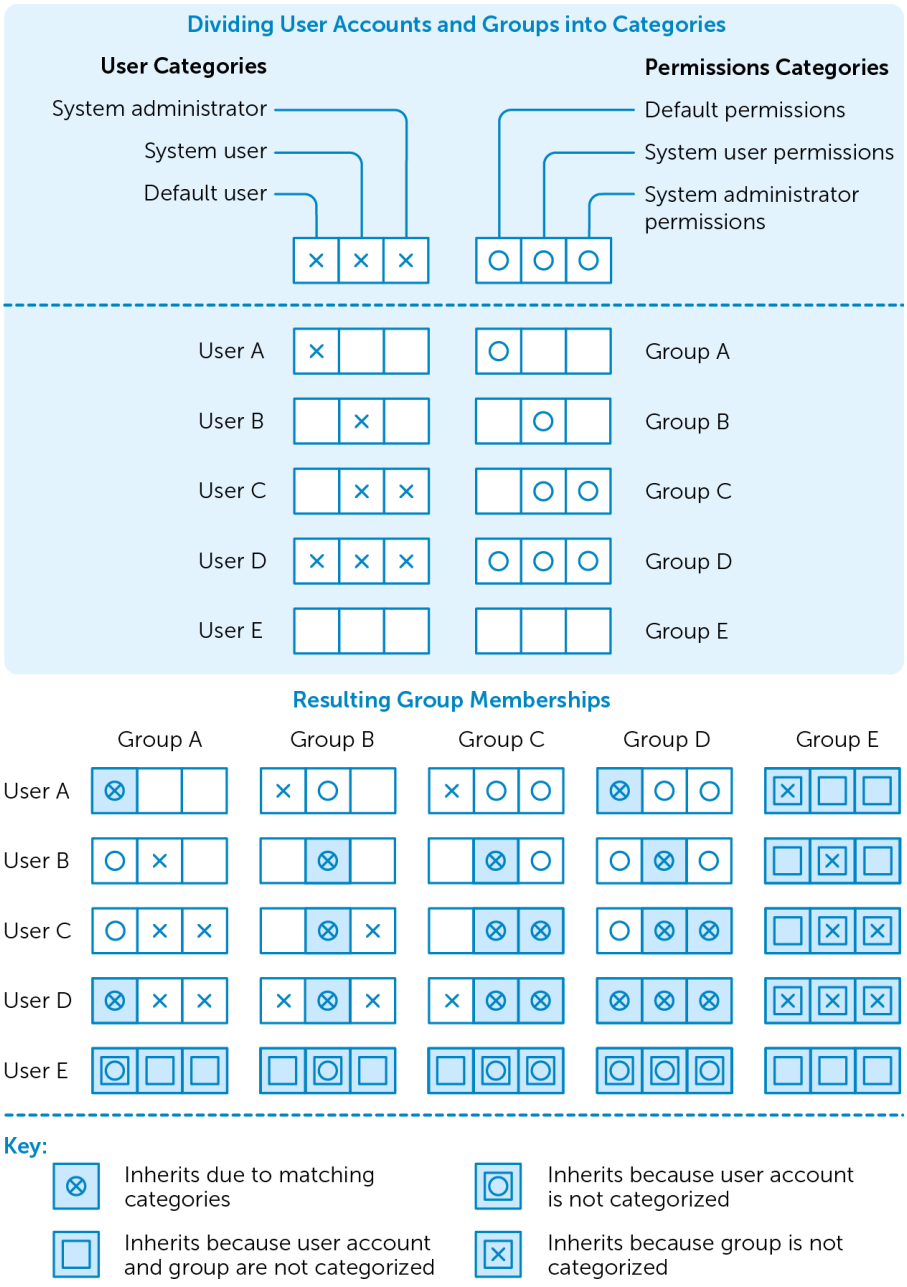
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the 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 50: Category Examples

Category Position	Categories for User Accounts	Categories for Groups
1	Default user	Default permissions
2	System user	System user permissions
3	System administrator	System administrator permissions

Figure 2: Example of inheriting through categories.



To use inheritance through categories

- Define categories in the domain.
- Assign categories to user accounts through their master data.
- Assign categories to groups through their master data.

Related Topics

- Specifying Categories for Inheriting Notes Groups on page 60
- General Master Data for a Notes User Account on page 77
- General Master Data for Notes Groups on page 103

Assigning 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. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify a group as group owner

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Groups** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To specify a group as mail-in database owner

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Mail-in DB** tab.
5. Assign mail-in databases in **Add assignments**.

   - OR -

   Remove the mail-in database in **Remove assignments**.

6. Save the changes.

To specify a group as certificate owner

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Certificate** tab.
5. Assign certificates in **Add assignments**.

   - OR -

   Remove certificates in **Remove assignments**.
6. Save the changes.

To specify a group as server owner

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select the **Assign document owner** in the task view.
4. Select the **Server** tab.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Assigning 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. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify a group as administrator for groups

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Groups** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To specify a group as administrator for mail-in databases

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Mail-in DB** tab.
5. Assign mail-in databases in **Add assignments**.

   - OR -

   Remove the mail-in database in **Remove assignments**.
6. Save the changes.

To specify a group as administrator for certificates

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Certificate** tab.
5. Assign certificates in **Add assignments**.

   - OR -

   Remove certificates in **Remove assignments**.
6. Save the changes.

To specify a group as administrator for server documents

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Server document** tab.
5. Assign the server documents in **Add assignments**.

   - OR -

Remove server documents in **Remove assignments**.

6. Save the changes.

To specify a group as administrator for servers

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrable documents** in the task view.
4. Select the **Server** tab.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
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. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign owner** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as owner of a group

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign owner** in the task view.
4. Select the **Groups** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
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. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrators** in the task view.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators for groups

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign administrators** in the task view.
4. Select the **Groups** tab.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Extended Properties to an Notes Group

Extended properties are meta objects that cannot be mapped directly in the One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a group

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties in **Remove assignments**.
5. Save the changes.

For more detailed information about setting up extended properties, see the Dell One Identity Manager Identity Management Base Module Administration Guide.

Denied Access Groups

Table 51: Configuration Parameter for Setting Up Denied Access Groups

Configuration parameter	Meaning
TargetSystem\NDO\DenyAccessGroups	Denied access groups are used when a Notes user account is disabled.
TargetSystem\NDO\DenyAccessGroups\Memberlimit	This configuration parameter contains 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	This configuration parameter contains the prefix used for formatting the name of a denied access group.

A user is considered to be locked in IBM® Notes® 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 permissions type "Not access server" 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 permissions type “Not access server” 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 with the group type “Deny list only” and automatically stores it on each server with the permissions type “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 the option **Denied access group>**.

To change the prefix of an denied access group.

1. Edit the value of the configuration parameter "TargetSystem\NDO\DenyAccessGroups\Prefix" in the Designer.
2. Enter the prefix to use 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

- Edit the value of the configuration parameter "TargetSystem\NDO\DenyAccessGroups\Memberlimit" in the Designer.

TIP: The denied access groups are found using the script `VI_Notes_GetOrCreateRestrictGroup` then added. If denied access groups already exist in IBM® Notes®, they are handled like normal groups.

To use these groups for the locking process in One Identity Manager

1. Set the option **Denied access group** for this group.
2. Modify the prefix in the configuration parameter "TargetSystem\NDO\DenyAccessGroups\Prefix", if necessary.
3. Modify the script `VI_Notes_GetOrCreateRestrictGroup` according to your requirements.

Dynamic Groups

Since IBM® 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 the method "Home server" is selected in the property "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 organization cannot be assigned to dynamic groups. Inheritance exclusion cannot be specified. Dynamic groups cannot be requested in the IT Shop.

Extension Groups

IBM® Notes® adds so called extension groups if the maximum number of members in a group has been reached. These extension groups are loaded into the One Identity Manager database by synchronization and cannot be edited. The connection to the dynamic group is created using the property **Parent Notes groups** (column `UID_NotesGroupParent`). 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 the IBM® Notes® 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 member of Notes group
- Are assigned to an excluded list
- Are assigned to an excluded list as member of 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 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 IBM® Notes® environment such that changes to effective memberships are promptly transferred to the One Identity Manager database.
>
> For more detailed information about editing synchronization schedules, see the Dell One Identity Manager Target System Synchronization Reference Guide.

Additional Tasks for Dynamic Groups

To maintain memberships in dynamic groups, you can apply the following tasks to dynamic groups. The task **Assign member** is not available.

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. Select the category **IBM® Notes® | Groups**.
2. Select the dynamic group in the result list.
3. Select **Assign home server** in the task view.
4. Assign the servers in **Add assignments**. To filter the server in the list, select a domain in **Notes domains**.

   - OR -

   Remove servers in **Remove assignments**.
5. Save the changes.

Editing the Excluded List

Use the excluded list to specify which user accounts you want to exclude from membership in a dynamic group.

To edit the excluded list of a dynamic group

1. Select the category **IBM® Notes® | Groups**.
2. Select the dynamic group in the result list.
3. Select **Edit additional list** in the task view.

4. To add user accounts to the excluded list, select the tab **User accounts**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. To add group to the excluded list, select the tab **Groups**.
7. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
8. Save the changes.

Editing the Additional List

Use the additional list to specify which user accounts you want to additionally include in membership in a dynamic group.

To edit the additional list of a dynamic group

1. Select the category **IBM® Notes® | Groups**.
2. Select the dynamic group in the result list.
3. Select **Edit additional list** in the task view.
4. To add user accounts to the additional list, select the tab **User accounts**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. To add user accounts to the additional list, select the tab **Groups**.
7. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
8. Save the changes.

Deleting Notes Groups

To delete a group

1. Select the category **IBM® Notes® | Groups**.
2. Select the group in the result list.
3. Click  to delete the group.
4. Confirm the security prompt with **Yes**.

The group is deleted completely from the One Identity Manager database and from IBM® Notes®.

10

Mail-In Databases

To edit mail-in database master data

1. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list. Select **Change master data** in the task view.

   - OR -

   Click  in the result list toolbar.
3. Edit the mail-in database's master data.
4. Save the changes.

Mail-In Database General Master Data

Enter the following data for mail-in databases:

Table 52: General Master 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 in format mailfile@organization.domain.
File Name	File name and path for the mail-in database relative to the Domino directory.
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	Spare text box for additional explanation.

Additional Tasks for Mail-In Databases

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of the Mail-In Database

To obtain an overview of a mail-in database

1. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list.
3. Select **Notes mail-in database overview** in the task view.

Assigning Notes Groups to Mail-In Databases

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. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**. To filter the groups, select a domain in **Notes domains**.

   - OR -

   Remove groups in **Remove assignments**.
5. Save the changes.

Assigning Owners to 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. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list.
3. Select **Assign owner** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.

6. Save the changes.

To specify groups as owner

1. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list.
3. Select **Assign owner** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Administrators to 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. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators

1. Select the category **IBM® Notes® | Mail-in DB**.
2. Select a mail-in database in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

11

Notes server

In One Identity Manager all servers declared in the Domino Directory are mapped as Notes servers.

To edit an Notes server's master data

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list. Select **Change master data** in the task view.
3. Enter the required data on the master data form.
4. Save the changes.

General Master Data for Notes Servers

Table 53: Configuration Parameters for Handling New User ID Files

Configuration parameter	Meaning
TargetSystem\NDO\StoreIDInAddressbook	This configuration parameter control the behavior of ID files for new user accounts. If the configuration parameter is set, the ID files are attached to the employee document. If this configuration parameter is no set, the ID file is stored on the gateway server.

Enter the following general master data for Notes servers.

Table 54: General Master Data for 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.
User ID file path	Path of the gateway server used for creating new user ID files. This data is only required if the configuration parameter "TargetSystem\NDO\StoreIDInAddressbook" is not set.
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 is only required when the option **Has Notes mailbox files** is set.

Property	Description
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.
Start 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 execution 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.

Notes Server Location Data

Edit location data for Notes servers on the **Location** tab.

Table 55: Location Data for a Notes Servers

Property	Description
Phone number	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.
Pass-through server	Pass-through server used at the server's location. Corresponds to the home server.

You can find more location information on the **Contact** tab.

Table 56: Contact data for a Notes Server

Property	Description
Location	Server's location.
Department	Server's department.
Comment	Spare text box for additional explanation.
Detailed description	Spare text box for additional explanation.

Security Settings for Notes Servers

Edit a server's security settings on the **Security** tab.

Table 57: Security Settings for a Notes Server

Property	Description
Compare public keys with keys in Domino Directory	Specifies whether public keys must be checked for all users and servers, once they have logged in to the server.
Permit anonymous connections	Specifies whether users and servers without valid certificates can log in to the server.
Examine passwords with Notes IDs	Specifies whether user ID file passwords are checked when the users log in to the server.

Additional Tasks for Managing Notes Servers

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

The Notes Server Overview

To obtain an overview of a Notes server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Notes server overview**.

Assigning Groups to Notes Servers

You can add servers to a group as members.

To add a Notes server to a group

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
5. Save the changes.

Assigning Mail Servers to 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`). This task is only available if the option **Has Notes mailbox files** is set.

To assign Notes servers directly to user accounts

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
5. Save the changes.

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. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign document owner** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as owners of a server document

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign document owner** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Administrators to Server Documents

Specify which user accounts and groups are allowed to administrate the server document.

To specify user accounts as administrators for a server document

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign document administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators for a server document

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign document administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Specifying Administrator Access

You can limit administrator's access rights in IBM® Notes®, whereby you issue access rights only at specific access levels. You can, for example, specify database administrators or issues full permissions to individual administrators.

Assigning Administrators with full Permissions

Assign user accounts and groups that are to have full access on servers.

To specify user accounts as full access administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign full access administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as full access administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign full access administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Administrators

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 administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning Database Administrators on page 134
- Assigning Administrators with Full Remote Console Access on page 135

Assigning Database Administrators

Assign the user accounts and groups to administrate databases on servers.

To specify user accounts as database administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign database administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as database administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign database administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning Administrators with Full Remote Console Access

Assign user accounts and groups that are allowed to use the remote console to execute commands on this server. That includes permissions and entitlements of an administrator with read-only access.

To specify user accounts as remote console administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign full remote console administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as remote console administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign full remote console administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning Read-only Administrators on page 135

Assigning Read-only Administrators

Assign user accounts and groups that are only allowed to use the remote console to execute commands supplying system information.

To specify user accounts as administrators with read access

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign view only administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

Remove user accounts in **Remove assignments**.

6. Save the changes.

To specify groups as administrators with read access

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign view only administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Assigning System Administrators

Assign the user accounts and groups that can execute any operating system commands on the server.

To specify user accounts as system administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign system administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as system administrators

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign system administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning Restricted System Administrators on page 137

Assigning Restricted System Administrators

Assign the user accounts and groups that can only execute restricted operating system commands on the server.

To specify user accounts as administrators with restrictions

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign restricted system administrators** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To specify groups as administrators with restrictions

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Assign restricted system administrators** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Assigning System Administrators on page 136

Server Permissions Settings

In the server document, access lists are defined that specify what access is given to users, groups or servers for different purposes.

The Access Server

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 **Not access server** in the task view. For more information, see Not Access Server on page 138.

To explicitly ensure server access to user accounts

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Access server** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To explicitly ensure server access to groups

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Access server** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To explicitly ensure server access to servers

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Access server** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Not Access Server

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 The Access Server on page 137.

To deny user accounts access to the server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.

3. Select **Deny server access** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To deny groups access to the server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Deny server access** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To deny servers access to the server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Deny server access** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

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. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Create databases & templates** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

Remove user accounts in **Remove assignments**.

6. Save the changes.

To allow groups to create databases and templates

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Create databases & templates** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To allow servers to create databases and templates

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Create databases & templates** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Creating New Copies

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. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Create new replicas** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to create replicas

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Create new replicas** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To allow servers to create replicas

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Create new replicas** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Routing through Servers

The given user accounts, groups and servers use the server as pass-through servers without taking server access into account. If there are no user accounts, groups or servers assigned, the server cannot be used as a pass-through server.

Servers must be set up as pass-through destinations for assignments to take effect. For more information, see Passthru Destinations for Routing on page 142.

To allow user accounts to use the server as pass-through server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Route through Server** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to use the server as pass-through server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Route through Server** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To allow servers to use the server as pass-through server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Route through Server** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Passthru Destinations for Routing

The given user accounts, groups and servers can access the server using pass-through servers. Server access must also be set up on this server for user accounts, groups and servers.

If there are no user accounts, groups or servers assigned, the server cannot be used as a pass-through destination.

To allow user accounts to use the server as pass-through destination

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Access this server** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to use the server as pass-through destination

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Access this server** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To allow servers to use the server as pass-through destination

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Access this server** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Cause Calling with the Passthru Server

The given user accounts, groups and servers can access other servers by using this pass-through server as a modem. If no user accounts, groups and servers are assigned, dial up is not permitted.

Servers must be set up as pass-through destinations for assignments to take effect. For more information, see Passthru Destinations for Routing on page 142.

To allow user accounts to use the passthru server for placing calls

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Cause calling** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to use the passthru server for placing calls

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Cause calling** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

To allow servers to use the passthru server for placing calls

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Cause calling** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign the servers in **Add assignments**.

   - OR -

   Remove servers in **Remove assignments**.
6. Save the changes.

Destinations Permitted for Passthru Servers

The pass-through server allows you to enter the destination servers that can be reached through this pass-through server. If no destination server is given, all servers given as pass-through destinations, can be accessed.

Servers must be set up as pass-through destinations for assignments to take effect. For more information, see Passthru Destinations for Routing on page 142.

To specify the destination server for a pass-through server

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Destinations allowed** in the task view.
4. Select the table "Notes server" in **Table**.
5. Assign target servers in **Add assignments**.

   - OR -

   Remove target servers in **Remove assignments**.
6. Save the changes.

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

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Run or sign unrestricted methods and operations** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to run unrestricted methods and operations

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Run or sign unrestricted methods and operations** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Running Restricted LotusScript®/Java Agents on page 145
- Running Simple Agents and Formula Agents on page 146

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

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Run restricted LotusScript®/Java agents** in the task view.
4. Select the table "Notes user accounts" in **Table**.

5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to run restricted LotusScript®/Java agents

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Run restricted LotusScript®/Java agents** in the task view.
4. Select the table "Notes groups" in **Table**.
5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Signing or Running Unrestricted Methods and Operations on page 145

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

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Run simple and formula agents** in the task view.
4. Select the table "Notes user accounts" in **Table**.
5. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts in **Remove assignments**.
6. Save the changes.

To allow groups to run simple agents and formula agents

1. Select the category **IBM® Notes® | Notes server**.
2. Select the server in the result list.
3. Select **Run simple and formula agents** in the task view.
4. Select the table "Notes groups" in **Table**.

5. Assign groups in **Add assignments**.

   - OR -

   Remove groups in **Remove assignments**.
6. Save the changes.

Related Topics

- Signing or Running Unrestricted Methods and Operations on page 145

12

Using AdminP Requests for Handling IBM® Notes® Processes

IBM® Notes® contains an asynchronous mechanism for processing various internal tasks. For example, if the name of a user changes, 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 executing Notes server creates a response document and if necessary a follow-up request.

AdminP requests are used by certain One Identity Manager processes, 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 executing Notes server?
- How often does the AdminP server task run on the executing Notes server?
- Which type of request is it?

Automatic Confirmation of 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 the One Identity Manager. Prerequisite for this is regular synchronization of the Admin4 database.

To confirm pending AdminP requests regularly

- Configure and set the schedule "IBM® Notes® automatic AdminP request confirmation" in the Designer.

For more detailed information about editing schedules, see the Dell One Identity Manager Configuration Guide.

Confirmation of the following requests has currently been implemented:

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

AdminP Request Master Data

Properties of synchronized AdminP requests are displayed in the Manager.

To display the master data of a request document

- Select the category **IBM® Notes® | Hierarchical view | <domain> | Administration requests | <filter> | <object> | <action>**.

Table 58: Master Data of an AdminP request document

Property	Description
Action	Action to be executed by the AdminP request.
Executing server	Server to execute the request.
Target	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 master data of an response document

1. Select the category **IBM® Notes® | Hierarchical view | <domain> | Administration requests | <filter> | <object> | <action>**.
2. Select the response document in the result list.

Table 59: Master Data of an AdminP response document

Property	Description
Action	Action that was executed by the AdminP request.
request document	Unique ID for the associated request document
Target	Name of the object that was processed.
Author	Name of the AdminP request author.
Executing server	Server that executed 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.

13

Reports about Notes Domains

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 Notes domains.

Table 60: Reports for the Target System

Report	Description
Overview of all assignments (domain)	This report find all roles containing employees with at least one user account in the selected domain.
Overview of all assignments (certificate)	The report shows all roles containing employees whose Notes user account was created with the selected certificate.
Overview of all assignments (group)	This report finds all roles containing employees with the selected group.
Show orphaned user accounts	This report shows all user accounts in the domain, which are not assigned to an employee. The report contains group memberships and risk assessment.
Show unused user accounts	This report shows all user accounts in the domain, which have not been used in the last few months. The report contains group memberships and risk assessment.
Show entitlement drifts	This report shows all groups in the domain that are the result of manual operations in the target system rather than using the One Identity Manager.
Show user accounts with an above average number of system entitlements	This report contains all user accounts in the domain with an above average number of group memberships.
Show employees with multiple user accounts	This report shows all employees with more than one Notes user account in the domain. The report contains a risk assessment.
IBM® 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 category **My One Identity Manager | Target system overviews**.
Data quality summary for IBM® Notes® user accounts	This report contains different evaluations of user account data quality in all Notes domains. You can find the report in the category **My |** Data quality analysisOne Identity Manager.

Overview of all Assignments

The report "Overview of all Assignments" is displayed for certain objects, for example, permissions, 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 employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

- 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, all roles are determined in which there are employees with this group.
- If the report is created for a compliance rule, all roles are determined in which there are employees with 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 report **Overview of all assignments**.
- Use the **Used by** button in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are 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. In the report's toolbar, click to open the legend.
- 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 employee for tracking. This creates a new business role to which the employees are assigned.

Figure 3: Toolbar for Report "Overview of all assignments"

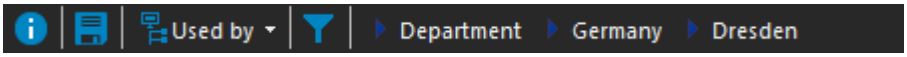


Table 61: Meaning of Icons in the Report Toolbar

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.

A

Appendix: Configuration Parameters for Synchronization with a Notes Domain

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 62: Configuration Parameters for Synchronizing a Notes Domain

Configuration parameter	Meaning if Set
TargetSystem\NDO	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system IBM® Notes®. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\NDO\Accounts	Parameter for configuring Notes user account data.
TargetSystem\NDO\Accounts\InitialPassword	This configuration parameter contains the initial password for creating user accounts. If no password if given when the user account is added, the initial password in the configuration parameter is used. This is necessary if a user account is added in the target system and the target system demands a minimum password length which is greater than 0. Note the minimum password length for the initial password.
TargetSystem\NDO\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. It must contain at least those character sets set in the configuration subparameters.
TargetSystem\NDO\Accounts\InitialRandomPassword\ Character	This configuration parameter specifies whether the random password must contain at least one letter [a-z].
TargetSystem\NDO\Accounts\InitialRandomPassword\ Length	This configuration parameter specifies how many characters the random password must contain.

Configuration parameter	Meaning if Set
TargetSystem\NDO\Accounts\InitialRandomPassword\Numeric	This configuration parameter specifies whether the random password must contain at least one numeric [0-10].
TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo	Specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/role, employee's manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\NDO\DefaultAddress".
TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account).
TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password).
TargetSystem\NDO\Accounts\InitialRandomPassword\SpecialCharacter	This configuration parameter specifies whether the random password must contain at least one special character.
TargetSystem\NDO\Accounts\InitialRandomPassword\UpperCase	This configuration parameter specifies whether the random password must contain at least one capital letter [A-Z].
TargetSystem\NDO\Accounts\MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account.
TargetSystem\NDO\BuildShortnameFullSync	This configuration parameter specifies whether short names are created for employee documents during synchronization, which do not have short names in IBM® Notes®. If this parameter is set, short names are created. If the parameter is set, short names are created.If not, user accounts without a short name cannot be added to the One Identity Manager database.

Configuration parameter	Meaning if Set
TargetSystem\NDO\CreateMailDB	This configuration parameter specifies whether the mailbox is created after or while the Notes user is registering with the target system. If the configuration parameter is set, the mailbox is created during registration. This uses the template of the Notes server on which the user is registered. If the configuration parameter is not set (default), the mailbox is created after the Notes user has registered. This uses the template given in the user account or in the configuration parameter "TargetSystem\NDO\DefTemplatePath".
TargetSystem\NDO\DefaultAddress	The configuration parameter contains the recipient's default email address for sending 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\IsNorthAmerican	Specifies whether the newly created ID files are compatible with the American (US) and Canadian IBM® Notes® version. If this parameter is set, all new user ID files are calculated with North American encryption strength.
TargetSystem\NDO\IsOperational	This configuration parameter specifies whether the target system access is tested before the action takes place. If the parameter is set, the system is tested for availability before the action takes place. The configuration parameter works for both synchronization and for when changes to Notes objects are published in real-time in the IBM® Notes® environment.
TargetSystem\NDO\MailBoxAnonymPre	Prefix for user account anonymity.
TargetSystem\NDO\MailFilePath	Directory on the mail server, in which the user account's mailbox files are stored.

Configuration parameter	Meaning if Set
TargetSystem\NDO\MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. 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\MinPasswordLength	Specifies the minimum password length that is set in all newly calculated user ID files.
TargetSystem\NDO\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\NDO\PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\NDO\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern.
TargetSystem\NDO\RedoDelay	This configuration parameter specifies the delay time after which an uncompleted modification on a target system object is repeated. The input is in minutes.
TargetSystem\NDO\StoreIDInAddressbook	This configuration parameter control the behavior of ID files for new user accounts. If the configuration parameter is set, the ID files are attached to the employee document. If this configuration parameter is no set, the ID file is stored on the gateway server.
TargetSystem\NDO\TempNetworkPath	Temporary directory in which newly created ID files and personal address books are stored.
TargetSystem\NDO\UpdateAddressbook	If the configuration is set, entries in the Domino Directory are added when new user ID files are created.
TargetSystem\NDO\UserType	This configuration parameter specifies the type of user, which results from registering.
TargetSystem\NDO\VerifyUpdates	This configuration parameter specifies whether modified properties are checked by updating. If this parameter is set, the objects in the target system are verified after every update.

B

Appendix: Default Project Template for IBM® Notes®

A default project template ensures that all required information is added in the 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 template uses mappings for the following schema types.

Table 63: Mapping Notes schema types to tables in the One Identity Manager schema.

Schema type in IBM® Notes®	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
PolicySecurity	NDOPolicySetting
PolicySetup	NDOPolicySetting
Server	NDOServer
Template	NDOTemplate

About Dell

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

Contacting Dell

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

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.quest.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

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

Index

E

G

I

J

L

M

N

O

P

R

S

T

U