



One Identity Manager 8.1.5

Administration Guide for Connecting to IBM Notes

Copyright 2021 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

One Identity Manager Administration Guide for Connecting to IBM Notes
Updated - 09 July 2021, 12:48
Version - 8.1.5

Contents

| | |
|--|-----------|
| Managing IBM Notes environments | 9 |
| Architecture overview | 9 |
| One Identity Manager users for managing IBM Notes | 11 |
| Setting up IBM Notes synchronization | 14 |
| Users and permissions for synchronizing with IBM Notes | 15 |
| Domino server configuration | 16 |
| Installing and configuring a gateway server | 16 |
| Copying the Notes certificate | 18 |
| Creating a custom Notes.ini | 19 |
| Installing and configuring the One Identity Manager Service | 19 |
| Creating an archive database for backing up employee documents | 22 |
| Creating a synchronization project for initial synchronization of a Notes domain | 23 |
| Displaying synchronization results | 29 |
| Customizing the synchronization configuration | 30 |
| How to configure IBM Notes synchronization | 31 |
| Configuring synchronization of several Notes domains | 32 |
| Updating schemas | 33 |
| Speeding up synchronization with revision filtering | 34 |
| Post-processing outstanding objects | 35 |
| Configuring the provisioning of memberships | 37 |
| Accelerating single object synchronization | 38 |
| Help for the analysis of synchronization issues | 39 |
| Disabling synchronization | 40 |
| Basic configuration data | 41 |
| Setting up account definitions | 42 |
| Creating an account definition | 43 |
| Master data for an account definition | 43 |
| Creating manage levels | 45 |
| Master data for manage levels | 47 |
| Creating a formatting rule for IT operating data | 48 |
| Collecting IT operating data | 49 |

| | |
|---|-----------|
| Modify IT operating data | 51 |
| Assigning account definitions to employees | 52 |
| Assigning account definitions to departments, cost centers, and locations | 53 |
| Assigning an account definition to business roles | 53 |
| Assigning account definitions to all employees | 54 |
| Assigning account definitions directly to employees | 54 |
| Assigning account definitions to system roles | 55 |
| Adding account definitions in the IT Shop | 55 |
| Assigning account definitions to a target system | 57 |
| Deleting an account definition | 57 |
| Password policies for Notes user accounts | 59 |
| Predefined password policies | 60 |
| Using password policies | 61 |
| Editing password policies | 63 |
| General master data for password policies | 63 |
| Policy settings | 64 |
| Character classes for passwords | 65 |
| Custom scripts for password requirements | 66 |
| Script for checking passwords | 66 |
| Script for generating a password | 67 |
| Password exclusion list | 69 |
| Checking a password | 69 |
| Testing password generation | 69 |
| Initial password for new Notes user accounts | 70 |
| Email notifications about login data | 71 |
| Editing a server | 72 |
| Master data for a Job server | 73 |
| Specifying server functions | 75 |
| Target system managers | 77 |
| Notes domains | 80 |
| General master data for a Notes domain | 80 |
| Specifying categories for inheriting Notes groups | 82 |
| How to edit a synchronization project | 82 |
| Notes certificates | 84 |

| | |
|---|-----------|
| General master data for Notes certificates | 84 |
| Notes certificates contact data | 85 |
| Additional tasks for managing Notes certificates | 86 |
| Overview of Notes certificates | 86 |
| Assigning owners | 86 |
| Assigning administrators | 87 |
| Post-processing newly loaded certificates | 88 |
| Notes certificate requests | 88 |
| Notes templates | 89 |
| Notes policies | 90 |
| Additional tasks for managing Notes policies | 91 |
| Displaying an overview of Notes policies | 91 |
| Assigning members to a Notes policy | 91 |
| Assigning owners to a Notes policy | 92 |
| Assigning administrators to a Notes policy | 92 |
| Notes policy settings | 93 |
| Notes user accounts | 95 |
| Linking user accounts to employees | 95 |
| Supported user account types | 96 |
| Entering master data for Notes user accounts | 100 |
| General master data of a Notes user account | 101 |
| Notes user account email system | 104 |
| Notes user account address data | 107 |
| Additional master data of a Notes user account | 107 |
| Administrative data for a Notes user account | 108 |
| Additional tasks for managing Notes user accounts | 110 |
| Displaying the Notes user accounts overview | 111 |
| Changing the manage level of user accounts | 111 |
| Assigning Notes groups directly to a Notes user account | 111 |
| Specifying document owners | 112 |
| Assigning owners | 114 |
| Assigning administrative documents | 114 |
| Assigning administrators | 116 |
| Maintaining excluded and additional lists | 117 |

| | |
|---|------------|
| Assigning extended properties | 118 |
| Automatic assignment of employees to user accounts | 118 |
| Editing search criteria for automatic employee assignment | 120 |
| Generating mailbox files | 123 |
| Saving user ID files | 124 |
| Restoring user ID files | 125 |
| ID vault | 125 |
| ID restore | 126 |
| Locking and unlocking Notes user accounts | 127 |
| Deleting and restoring Notes user accounts | 129 |
| Notes groups | 131 |
| General master data for Notes groups | 131 |
| Assigning Notes groups to Notes user accounts | 133 |
| Assigning Notes groups to departments, cost centers and locations | 134 |
| Assigning Notes groups to business roles | 135 |
| Assigning Notes user accounts directly to a Notes group | 136 |
| Adding Notes groups to system roles | 137 |
| Adding Notes groups to the IT Shop | 138 |
| Additional tasks for managing Notes groups | 139 |
| Displaying an overview of Notes groups | 139 |
| Assigning Notes mail-in databases to Notes groups | 140 |
| Assigning Notes servers to a Notes group | 140 |
| Adding Notes groups to Notes groups | 141 |
| Effectiveness of group memberships | 142 |
| Notes group inheritance based on categories | 144 |
| Assigning Notes groups as document owners | 146 |
| Assigning Notes groups as document administrators | 147 |
| Assigning owners to Notes groups | 149 |
| Assigning administrators to Notes groups | 150 |
| Assigning extended properties to Notes groups | 150 |
| Locking groups | 151 |
| Dynamic groups | 152 |
| Extension groups | 153 |
| Memberships in dynamic groups | 153 |
| Additional tasks for dynamic groups | 154 |

| | |
|--|------------|
| Assigning home servers | 154 |
| Editing the excluded list | 154 |
| Editing the inclusion list | 155 |
| Deleting Notes groups | 157 |
| Mail-in databases | 158 |
| Mail-in DB general master data | 158 |
| Additional tasks for mail-in databases | 159 |
| Overview of the mail-in DB | 159 |
| Assigning Notes groups to a mail-in DB | 159 |
| Assigning owners to a mail-in DB | 160 |
| Assigning administrators to a mail-in DB | 160 |
| Maintaining excluded and additional lists | 161 |
| Notes server | 163 |
| General master data for Notes servers | 163 |
| Notes server location data | 164 |
| Notes server security settings | 165 |
| Additional tasks for managing Notes servers | 166 |
| The Notes server overview | 166 |
| Assigning groups to Notes servers | 166 |
| Assigning mail servers to user accounts | 166 |
| Assigning owners to the server document | 167 |
| Assigning administrators to the server document | 167 |
| Specifying administrator access | 168 |
| Assigning administrators with full permissions | 168 |
| Assigning administrators | 169 |
| Assign database administrators | 170 |
| Assigning administrators with full remote console access | 171 |
| Assign view-only administrators | 171 |
| Assign system administrators | 172 |
| Assign restricted system administrators | 173 |
| Server permissions settings | 174 |
| Access servers | 174 |
| No access servers | 175 |
| Creating databases & templates | 176 |

| | |
|---|------------|
| Creating new replicas | 177 |
| Pass-through route | 178 |
| Pass-through destinations for routing | 179 |
| Cause calling with the passthru server | 180 |
| Destinations permitted for passthru servers | 181 |
| Signing or running unrestricted methods and operations | 181 |
| Running restricted LotusScript/Java agents | 182 |
| Running simple agents and formula agents | 183 |
| Maintaining excluded and additional lists | 184 |
| Using AdminP requests for handling IBM Notes processes | 185 |
| Automatic confirmation of AdminP requests | 185 |
| AdminP request master data | 186 |
| Reports about Notes domains | 188 |
| Overview of all assignments | 189 |
| Appendix: Configuration parameters for synchronizing a Notes domain | 191 |
| Appendix: Default project template for IBM Notes | 194 |
| About us | 196 |
| Contacting us | 196 |
| Technical support resources | 196 |
| Index | 197 |

Managing IBM Notes environments

IBM Notes 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 users 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 One Identity Manager, the necessary mailbox file is created.

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

Architecture overview

In One Identity Manager, the image of part of an operational IBM Notes system is mapped to a Notes domain. 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 performs the function of the

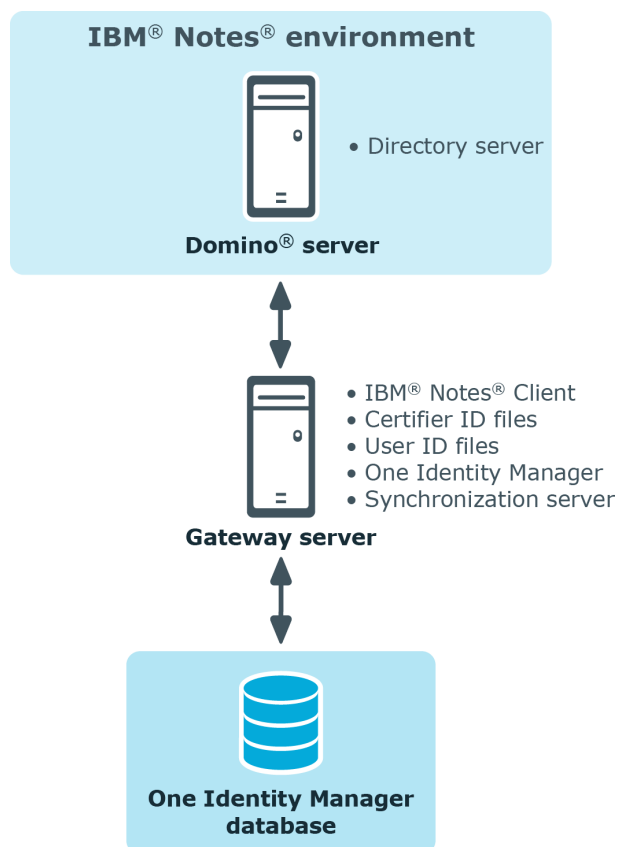
synchronization server. It is not a productive Domino server. An IBM Notes client, the One Identity Manager Service, and the IBM Notes connector are installed on the gateway server.

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 an 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 follows 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. |
| 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 IBM Notes

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

Table 2: Users

| User | Tasks |
|------------------------------|---|
| Target system administrators | <p>Target system administrators must be assigned to the Target systems Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Administer application roles for individual target system types.• Specify the target system manager.• Set up other application roles for target system managers if required.• Specify which application roles for target system managers are mutually exclusive. |

| User | Tasks |
|-------------------------------------|---|
| | <ul style="list-style-type: none"> • Authorize other employees to be target system administrators. • Do not assume any administrative tasks within the target system. |
| Target system managers | <p>Target system managers must be assigned to the Target systems IBM Notes application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other identity than the Primary identity. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required. |
| One Identity Manager administrators | <ul style="list-style-type: none"> • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required. |
| Administrators for the IT Shop | <p>Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role.</p> <p>Users with this application role:</p> |

| User | Tasks |
|----------------------------------|---|
| | <ul style="list-style-type: none"> Assign groups to IT Shop structures. |
| Administrators for organizations | <p>Administrators must be assigned to the Identity Management Organizations Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> Assign groups to departments, cost centers, and locations. |
| Business roles administrators | <p>Administrators must be assigned to the Identity Management Business roles Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> Assign groups to business roles. |

Setting up IBM Notes synchronization

One Identity Manager supports synchronization with IBM Notes in the following versions:

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

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

1. In IBM Notes, prepare a user with sufficient permissions for synchronization.
2. One Identity Manager components for managing IBM Notes environments are available if "TargetSystem | NDO" is set.
 - In the Designer, check if the configuration parameter is set. 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 15
- [Installing and configuring a gateway server](#) on page 16
- [Creating a synchronization project for initial synchronization of a Notes domain](#)

on page 23

- [General master data for Notes certificates](#) on page 84

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 | Permissions |
|---|--|
| One Identity Manager Service user account | <p>The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files.</p> <p>The user account must belong to the Domain users group.</p> <p>The user account must have the Login as a service extended user permissions.</p> <p>The user account requires access permissions to the internal web service.</p> <p>NOTE: If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none">• %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)• %ProgramFiles%\One Identity (on 64-bit operating systems) |
| User for accessing the target system (synchronization user) | <p>The user who accesses the system required sufficient administrative permissions to the Domino Directory (names.nsf). The minimum requirements are:</p> <ul style="list-style-type: none">• "Editor" access function on the primary Domino directory• Permissions for deleting documents |

| User | Permissions |
|--|---|
| | <ul style="list-style-type: none"> • "UserCreator" in addition to the default permissions • Remote console access • Administrative access to a Domino server (server on which new user can be registered and AdminP tasks created) <p>"Editor" is also required for the following databases:</p> <ul style="list-style-type: none"> • certlog.nsf • admin4.nsf |
| User for accessing the One Identity Manager database | The Synchronization default system user is provided to execute synchronization with 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.
- In the file Notes.ini, set FT_MAX_SEARCH_RESULTS = 2147483000.

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

For more 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
- The following versions are supported:
- Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
 - Windows Server 2012
 - Windows Server 2012 R2

- Windows Server 2016
 - Windows Server 2019
 - Microsoft .NET Framework Version 4.7.2 or later
- NOTE:** Take the target system manufacturer's recommendations into account.
- Windows Installer
 - IBM Notes Client version 8.5.3 or 10.0 or HCL Notes Client version 11.0.1
- NOTE:**
- Run the installation in single-user mode.
 - You must run a proper installation. IBM Domino COM class libraries are registered during installation. This requires 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 **Select installation modules with existing database** option.
 2. Select the **Server | Job server | IBM Notes** machine role.

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

The following versions of the IBM Domino and IBM Notes components are required for synchronizing an 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 in version 8.5.3, Fix Pack 4 or IBM Notes client version 10.0

To set up a gateway server

1. Configure the IBM Notes client.
For more information, see [To configure the IBM Notes client](#) on page 17.
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 19.

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 insert the path selected for the Notes data directory during installation of the IBM Notes client for the PATH variables.

2. Specify the directory for the ID files repository (<Installation directory>\data\IDS\<Name of the domain>).
3. Ensure the synchronization user's user ID file is available.

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

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

Set up all certifier ID files for registering users on the gateway server. Certifier ID files with multiple passwords are not supported.
5. Start the 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 permissions can be checked by calculating a new user with the ID file as a test.
6. Copy the Domino Directory certificate documents into the user account's personal address book for synchronization.
7. Check whether the certification log certlog.nsf exists.
8. Create a custom INI file.

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

NOTE:

- If you did not install the 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.
- If you are using IBM Notes client version 10.0, change the path to Notes.ini. Depending on the installation, this file can be saved in the user profile directory.

Detailed information about this topic

- [Copying the Notes certificate](#) on page 18
- [Creating a custom Notes.ini](#) on page 19

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 Notes.ini

When you configure the IBM Notes client, a Notes.ini file is created. This file contains configuration information that 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: Required parameters in the custom Notes.ini

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

Installing and configuring the One Identity Manager Service

The gateway server performs the function of the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager. All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.

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

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

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

- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

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

NOTE: The program performs a 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 remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

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

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

- a. Select a Job server from the **Server** menu.

- OR -

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

- b. Enter the following data for the Job server.

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

Syntax:

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

NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with the Designer.

4. On the **Machine roles** page, select **IBM Notes**.
5. On the **Server functions** page, select **IBM Notes connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

- For a direct connection to the database:
 - a. Select **Process collection | sqlprovider**.
 - b. Click the **Connection parameter** entry, then click the **Edit** button.
 - c. Enter the connection data for the One Identity Manager database.
 - For a connection to the application server:
 - a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
 - b. Click the **Connection parameter** entry, then click the **Edit** button.
 - c. Enter the connection data for the application server.
 - d. Click the **Authentication data** entry and click the **Edit** button.
 - e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
7. To configure remote installations, click **Next**.
 8. Confirm the security prompt with **Yes**.
 9. On the **Select installation source** page, select the directory with the install files.
 10. On the **Select private key file** page, select the file with the private key.

NOTE: This page is only displayed when the database is encrypted.
 11. On the **Service access** page, enter the service's installation data.
 - **Computer:** Name or IP address of the server that the service is installed and started on.
 - **Service account:** User account data for the One Identity Manager Service.
 - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.
 - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.
 - **Installation account:** Data for the administrative user account to install the service.
 - To use the current user's account, set the **Current user** option.
 - To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.

- To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.
12. Click **Next** to start installing the service.
Installation of the service occurs automatically and may take some time.
 13. Click **Finish** on the last page of the Server Installer.
NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Creating an archive database for backing up employee documents

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

INFORMATION: The archive database is only required if the **ID vault enabled** option is disabled for the domain and if user ID files are supposed to be restored by One Identity Manager. For more information, see [ID restore](#) on page 126.

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

Table 5: 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 environment. The following describes the steps for initial configuration of a synchronization project.

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

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

Table 6: 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 Notes.ini on page 19. |
| ID file password | <p>Synchronization user's ID file password. The path of this ID file must be given in the custom INI file.</p> <p>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 15.</p> |
| synchronization server | <p>All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>The gateway server performs the function of the synchronization server. The One Identity Manager Service with the IBM Notes connector must be installed on the synchronization server.</p> <p>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.</p> |

| Data | Explanation |
|---|--|
| Table 7: Additional properties for the Job server | |
| Property | Value |
| Server function | IBM Notes connector |
| Machine role | Server/Job server/IBM Notes |
| For more information, see Installing and configuring the One Identity Manager Service on page 19. | |
| One Identity Manager database connection data | <ul style="list-style-type: none"> • Database server • Database • SQL Server login and password • Specifies whether integrated 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. |
| Remote connection server | <p>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If the Synchronization Editor cannot be started directly on the gateway server, you can set up a remote connection.</p> <p>To use a remote connection</p> <ol style="list-style-type: none"> 1. Provide a workstation on which the Synchronization Editor is installed. 2. Install the RemoteConnectPlugin on the gateway server. Thus the gateway server simultaneously assumes the function of the remote connection server. <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • <code>[[[Undefined variable ProductVarSet.TargetSystemDomino]]]</code> connector is installed |

| Data | Explanation |
|------|---|
| | 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 <i>One Identity Manager Target System Synchronization Reference Guide</i> . |

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

- Executed in default mode
- Started from the Launchpad

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

To set up an initial synchronization project for a Notes domain

1. Start the Launchpad on the gateway server and log in to the One Identity Manager database.
NOTE: If synchronization is executed by an application server, connect the database through the application server.
2. Select the **Target system type IBM Notes** entry and click **Start**.
This starts the Synchronization Editor's project wizard.
3. On the **System access** page, specify how One Identity Manager can access the target system.
 - If you started the Launchpad on the gateway server, do not change any settings.
 - If you started the Launchpad on the gateway server, do not change any settings.

Enable the **Connect using remote connection server** option and select the gateway server to use for the connection under **Job server**.
4. On the **Configuration data for the IBM Domino directory** page, enter the connection parameters required by the IBM Notes connector to log in on the target system.

Table 8: Connection data for the Domino server

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

| Property | Description |
|------------------|---|
| server | 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 on the **Verify connection settings** page. Click on **Verify project**.

One Identity Manager tries to connect to the target system.

6. You can configure additional settings on the **Configuration settings** page.
 - To delete Notes objects using AdminP processes, enable **Delete objects using AdminP processes**. If the option is disabled, the objects are deleted directly in the system by the IBM Notes connector.
 - Click **Finish**, to end the system connection wizard and return to the project wizard.
7. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not shown if a synchronization project already exists.
8. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
9. On the **Restrict target system access** page, specify how system access should work. You have the following options:


Table 9: Specify target system access

| Option | Meaning |
|------------------------------------|---|
| Read-only access to target system. | <p>Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization is in the direction of One Identity Manager. • Processing methods in the synchronization steps are only defined for synchronization in the direction of |

| Option | Meaning |
|--|--|
| One Identity Manager. | |
| Read/write access to target system. Provisioning available. | <p>Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization is in the direction of the Target system. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the Target system. • Synchronization steps are only created for such schema classes whose schema types have write access. |

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

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

- 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 a Job server for the target system in the One Identity Manager database.

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

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

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

The synchronization project is created, saved, and enabled immediately.

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

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

NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually

before closing the Synchronization Editor.

NOTE: The connection data for the target system is saved in a variable set and can be modified in the **Configuration | Variables** category in the Synchronization Editor.

To configure the content of the synchronization log

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

NOTE: Some content generates a particularly large volume of log data. The synchronization log should only contain data required for troubleshooting and other analyses.

7. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Start up configurations** category.
3. Select a start up configuration in the document view and click **Execute**.
4. Confirm the security prompt with **Yes**.

NOTE:

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

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

To select user accounts through account definitions

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

Detailed information about this topic

- [One Identity Manager Target System Synchronization Reference Guide](#)

Related topics


- [Installing and configuring a gateway server](#) on page 16
- [Users and permissions for synchronizing with IBM Notes](#) on page 15
- [Displaying synchronization results](#) on page 29
- [Customizing the synchronization configuration](#) on page 30
- [Speeding up synchronization with revision filtering](#) on page 34
- [Using AdminP requests for handling IBM Notes processes](#) on page 185
- [Default project template for IBM Notes](#) on page 194
- [Setting up account definitions](#) on page 42
- [Automatic assignment of employees to user accounts](#) on page 118

Displaying synchronization results


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

To display a synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.

3. Click  in the navigation view toolbar.
Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.
3. Click  in the navigation view toolbar.
Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the provisioning is shown as a report. You can save the report.

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Customizing the synchronization configuration

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

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

- To use One Identity Manager as the master system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- To specify which Notes objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.

- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing methods, for example.
- Use variables to set up a synchronization project for synchronizing different domains. Store a connection parameter as a variable for logging in to the domain.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

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

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

Detailed information about this topic

- [How to configure IBM Notes synchronization](#) on page 31
- [Configuring synchronization of several Notes domains](#) on page 32
- [Updating schemas](#) on page 33

How to configure IBM Notes synchronization

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

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 creates a workflow with **Target system** as its synchronization direction.
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 32

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 domains. Use the wizard to attach a base object.
 - In the wizard, select the IBM Notes connector and declare the connection parameters. The connection parameters are saved in a special variable set.
A start up configuration is created that uses the newly created variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related topics

- [How to configure IBM Notes synchronization](#) on page 31
- [Users and permissions for synchronizing with IBM Notes](#) on page 15

Updating schemas

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

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

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

- A schema was changed by:
 - Changes to a target system schema
 - Customizations to the One Identity Manager schema
 - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
 - Enabling the synchronization project
 - Saving the synchronization project for the first time
 - Compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Target system** category.
- OR -
Select the **Configuration | One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.
Opens the Mapping Editor. For more detailed information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Speeding up synchronization with revision filtering

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

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

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

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

For more detailed information about revision filtering, see the 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.

Outstanding objects:

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

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

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select the **IBM Notes | Target system synchronization: IBM Notes** category.

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

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was executed. The **No log available** entry can mean the following:

- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted from the target system.
The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.
- An object that contains a member list has been deleted from the target system.




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

TIP:

To display object properties of an outstanding object

- 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 on one of the following icons in the form toolbar to execute the respective method.

Table 10: Methods for handling outstanding objects

| Icon | Method | Description |
|---|---------|---|
|  | Delete | The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. The Outstanding label is removed from the object. Indirect memberships cannot be deleted. |
|  | Publish | The object is added to the target system. The Outstanding label is removed from the object. The method triggers the HandleOutstanding event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: <ul style="list-style-type: none">• The table containing the object can be published.• The target system connector has write access to the target system. |
|  | Reset | The Outstanding label is removed for the object. |

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

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

- In the form's toolbar, click  to disable bulk processing.

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

To add custom tables to target system synchronization

1. In the Manager, select the **IBM Notes | Basic configuration data | Target system types** category.

2. In the result list, select the **IBM Notes** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

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

Configuring the provisioning of memberships

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

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

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


To allow separate provisioning of memberships

1. In the Manager, select the **IBM Notes | Basic configuration data | Target system types** category.
2. In the result list, select the **IBM Notes** target system type.
3. Select the **Configure tables for publishing** task.

4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
 - This option can only be enabled for assignment tables that have a base table with an XDateSubItem column.
 - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Merge mode**.
6. Save the changes.

For each assignment table labeled like this, the changes made in 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 not the entire members list.

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

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

To restore the default condition

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

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

Accelerating single object synchronization

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

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

NOTE: You should not implement load balancing for single object synchronization on a permanent basis. Parallel processing of object might result in dependencies not being

resolved because referenced objects from another Job server have not been completely processed.

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
 - Assign the **IBM Notes connector** server function to the Job server.

All Job servers must access the same Notes domain as the synchronization server for the respective base object.

2. In the Synchronization Editor, assign a custom server function to the base object.

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

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

For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Manager, assign this server function to all the Job servers that will be processing single object synchronization for the base object.

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- [Editing a server](#) on page 72

Help for the analysis of synchronization issues

You can generate a report for analyzing problems that arise during synchronization, inadequate performance for example. The report contains information such as:

- Consistency check results
- Revision filter settings

- Scope applied
- Analysis of the data store
- 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 **Help | Generate synchronization analysis report** menu item and click **Yes** in the security prompt.
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.

Disabling synchronization

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

To prevent regular synchronization

1. Open the synchronization project in the Synchronization Editor.
2. Select the start up configuration and deactivate the configured schedule.

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

1. Open the synchronization project in the Synchronization Editor.
2. Select the **General** view on the start page.
3. Click **Deactivate project**.

Detailed information about this topic

- [Creating a synchronization project for initial synchronization of a Notes domain](#) on page 23

Basic configuration data

To manage an IBM Notes environment in One Identity Manager, the following basic 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. In the Designer, you can find an overview of all configuration parameters in the **Base data | General | Configuration parameters** category.

For more information, see [Configuration parameters for synchronizing a Notes domain](#) on page 191.

- 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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

For more information, see [Setting up account definitions](#) on page 42.

- Password policy

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

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

For more information, see [Password policies for Notes user accounts](#) on page 59.

- 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 70.

- Email notifications about credentials

When a new user account is created, the login data are sent 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 71.

- 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 35.

- Target system managers

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

Define additional application roles if you want to limit the edit permissions for target system managers to individual domains. The application roles must be added under the default application role.

For more information, see [Target system managers](#) on page 77.

- 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 72.

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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

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

data required for user accounts included in the default installation. You can customize templates as required.


For detailed information about account definitions, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- [Creating an account definition](#)
- [Creating manage levels](#)
- [Creating a formatting rule for IT operating data](#)
- [Collecting 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. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list. Select the **Change master data** task.
-OR-
Click  in the result list.
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 11: Master data for an account definition

| Property | Description |
|--------------------|---|
| Account definition | Account definition name. |
| User account table | Table in the One Identity Manager schema that maps user accounts. |
| Target system | Target system to which the account definition applies. |

| Property | Description |
|-----------------------------------|---|
| Required account definition | Required account definition. 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 | Text field for additional explanation. |
| Manage level (initial) | Manage level to use by default when you add new user accounts. |
| Risk index | Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> . |
| 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 also be assigned directly to employees and roles outside the IT Shop. |
| Only for use in IT Shop | Specifies whether the account definition can only be requested through the IT Shop. The account definition can be 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. |
| 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 | Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user |

| Property | Description |
|---|--|
| permanently disabled | 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 on deferred deletion | Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account 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. |

Creating 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.

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged:** User accounts with the **Unmanaged** manage level are linked to the employee but they do not inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed:** User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

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

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

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For detailed information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

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

To assign manage levels to an account definition

1. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage levels.
- OR -
In the **Remove assignments** pane, remove the manage levels.
5. Save the changes.

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

To edit a manage level

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

- OR -

Click  in the result list.

3. Edit the manage level's master data.
4. Save the changes.

Master data for manage levels

Enter the following data for a manage level.

Table 12: Master data for manage levels

| Property | Description |
|--|---|
| Manage level | Name of the manage level. |
| Description | Text field for additional explanation. |
| IT operating data overwrites | Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <ul style="list-style-type: none">• Never: Data is not updated.• Always: Data is always updated.• Only initially: Data is only determined at the start. |
| 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. |
| 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 disabled 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 automatically creating user accounts for an employee in the target system and modifying them.

- 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. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.

3. Select the **Edit IT operating data mapping** task and enter the following data.

Table 13: Mapping rule for IT operating data

| Property | Description |
|-----------------------------------|--|
| Column | User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the <i>One Identity Manager Target System Base Module Administration Guide</i> . |
| Source | <p>Specifies which roles to use in order to find the user account properties. You have the following options:</p> <ul style="list-style-type: none">• Primary department• Primary location• Primary cost center• Primary business roles <p>NOTE: Only use the primary business role if the Business Roles Module is installed.</p> <ul style="list-style-type: none">• Empty <p>If you select a role, you must specify a default value and set the Always use default value option.</p> |
| 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. The Employee - new user account with default properties created mail template is used. To change the mail template, adjust the TargetSystem NDO Accounts MailTemplateDefaultValues configuration parameter. |

4. Save the changes.

Collecting IT operating data

To create user accounts with the **Full managed** manage level, the required IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the business roles, departments, locations, or cost centers. An employee is assigned a primary business role, primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from

these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example

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

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. Specify the "Department" property 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 of department A for the domain A. This IT operating data is used for standard user accounts. In addition, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.

3. Click **Add** and enter the following data.

Table 14: IT operating data

| Property | Description |
|------------|--|
| Effects on | <p>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.</p> <p>To specify an application scope</p> <ol style="list-style-type: none">a. Click ➔ next to the field.b. Under Table, select the table that maps the target system for select the TSBAccountDef table or an account definition.c. Select the specific target system or account definition under Effects on.d. Click OK. |
| Column | <p>User account property for which the value is set.</p> <p>In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the <i>One Identity Manager Target System Base Module Administration Guide</i>.</p> |
| Value | <p>Concrete value which is assigned to the user account property.</p> |

4. Save the changes.

Modify IT operating data

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

Prerequisites

- The IT operating data of a department, a cost center, a business role, or a location have been changed.
- OR -
- The default values in the IT operating data template were modified for an account definition.

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

To execute the template

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

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

Old value: Current value of the object property.

New value: Value that the object property would have following modification of the IT operating data.

Selection: Specifies whether or not the new value is transferred 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. Department managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or added directly to the IT Shop as products.

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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 assignment of an account definition is removed, the user account that was created from this account definition is deleted.

For detailed information about preparing role classes to be assigned, see the *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. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

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

Assigning an account definition to business roles

Installed modules: Business Roles Module


To add account definitions to hierarchical roles

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

4. In the **Add assignments** pane, assign business roles.

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

To remove an assignment

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

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, enable the **Automatic assignment to employees** option.

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 **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. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign to employees** task.
4. In the **Add assignments** pane, add employees.

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

To remove an assignment

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

Assigning account definitions to system roles

Installed modules: System Roles Module


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

To add account definitions to a system role

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

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

To remove an assignment

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

Adding account definitions in the IT Shop

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

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

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

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

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

To add an account definition to the IT Shop

1. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements | Account definitions** (role-based login) category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements | Account definitions** (role-based login) category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from all IT Shop shelves

1. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements | Account definitions** (role-based login) category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related topics

- [Master data for an account definition on page 43](#)
- [Assigning account definitions to departments, cost centers, and locations on page 53](#)
- [Assigning an account definition to business roles on page 53](#)
- [Assigning account definitions directly to employees on page 54](#)
- [Assigning account definitions to system roles on page 55](#)

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 (**Linked configured** state):

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

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

To assign the account definition to a target system

1. In the Manager, select the domain in the **IBM Notes | Domains** category.
2. Select the **Change master data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
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.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change master data** task.

- d. On the **General** tab, disable the **Automatic assignment to employees** option.
 - e. Save the changes.
2. Remove direct assignments of the account definition to employees.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign to employees** task.
 - d. In the **Remove assignments** pane, remove the employees.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign organizations** task.
 - d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.
 - e. Save the changes.
4. Remove the account definition's assignments to business roles.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign business roles** task.

In the **Remove assignments** pane, remove the business roles.
 - 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 about unsubscribing requests, see the *One Identity Manager Web Portal User Guide*.

To remove an account definition from all IT Shop shelves


- a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

- OR -

In the Manager, select the **Entitlements | Account definitions** (role-based login) category.
- b. Select an account definition in the result list.

- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

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

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change master data** task.
 - d. From the **Required account definition** menu, remove the account definition.
 - e. Save the changes.
7. Remove the account definition's assignments to target systems.
 - a. In the Manager, select the domain in the **IBM Notes | Domains** category.
 - b. Select the **Change master data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
8. Delete the account definition.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Account definitions | Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Click  to delete an account definition.

Password policies for Notes user accounts

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

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

Detailed information about this topic

- [Predefined password policies](#) on page 60
- [Using password policies](#) on page 61
- [Editing password policies](#) on page 63
- [Custom scripts for password requirements](#) on page 66
- [Password exclusion list](#) on page 69
- [Checking a password](#) on page 69
- [Testing password generation](#) on page 69

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.1.5, the configuration parameter settings for forming passwords are passed on to the target system-specific password policies.

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

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

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

Using password policies

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

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

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

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

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

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

To reassign a password policy

1. In the Manager, select the **IBM Notes | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.

- Click **Add** in the **Assignments** section and enter the following data.

Table 15: Assigning a password policy

| Property | Description |
|-----------------|---|
| Apply to | <p>Application scope of the password policy.</p> <p>To specify an application scope</p> <ol style="list-style-type: none">Click ➔ next to the field.Select one of the following references under Table:<ul style="list-style-type: none">The table that contains the base objects of synchronization.To apply the password policy based on the account definition, select the TSBAccountDef table.To apply the password policy based on the manage level, select the TSBBehavior table.Under Apply to, select the table that contains the base objects.<ul style="list-style-type: none">If you have selected the table containing the base objects of synchronization, next select the specific target system.If you have selected the TSBAccountDef table, next select the specific account definition.If you have selected the TSBBehavior table, next select the specific manage level.Click OK. |
| Password column | The password column's identifier. |
| Password policy | The identifier of the password policy to be used. |


- Save the changes.

To change a password policy's assignment

- In the Manager, select the **IBM Notes | Basic configuration data | Password policies** category.
- Select the password policy in the result list.
- Select the **Assign objects** task.
- In the **Assignments** pane, select the assignment you want to change.
- From the **Password Policies** menu, select the new password policy you want to apply.
- Save the changes.

Editing password policies

To edit a password policy

1. In the Manager, select the **IBM Notes | Basic configuration data | Password policies** category.
2. Select the password policy in the result list and select **Change master data**.
- OR -
Click  in the result list.
3. Edit the password policy's master data.
4. Save the changes.




Detailed information about this topic

- [General master data for password policies](#) on page 63
- [Policy settings](#) on page 64
- [Character classes for passwords](#) on page 65
- [Custom scripts for password requirements](#) on page 66

General master data for password policies

Enter the following master data for a password policy.

Table 16: Master data for a password policy

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

Policy settings

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

Table 17: Policy settings

| Property | Meaning |
|---------------------------|--|
| Initial password | Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated. |
| Password confirmation | Reconfirm password. |
| Minimum Length | Minimum length of the password. Specify the number of characters a password must have. |
| Max. length | Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is 256 . |
| Max. errors | <p>Maximum number of errors. Set the number of invalid passwords attempts. Only taken into account when logging in to One Identity Manager.</p> <p>This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager.</p> <p>You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more detailed information, see the <i>One Identity Manager Web Portal User Guide</i>.</p> |
| Validity period | Maximum age of the password. Enter the length of time a password can be used before it expires. |
| Password history | Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored. |
| Minimum password strength | Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1 , 2 , 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity. |
| Name properties denied | Specifies whether name properties are permitted in the |

| Property | Meaning |
|----------|---|
| | password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the Contains name properties for password check option is set. In the Designer, adjust this option in the column definition. For more detailed information, see the <i>One Identity Manager Configuration Guide</i> . |

Character classes for passwords

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

Table 18: Character classes for passwords

| Property | Meaning |
|---|--|
| Min. number letters | Specifies the minimum number of alphabetical characters the password must contain. |
| Min. number lowercase | Specifies the minimum number of lowercase letters the password must contain. |
| Min. number uppercase | Specifies the minimum number of uppercase letters the password must contain. |
| Min. number digits | Specifies the minimum number of digits the password must contain. |
| Min. number special characters | Specifies the minimum number of special characters the password must contain. |
| Permitted special characters | List of permitted special characters. |
| Max. identical characters in total | Specifies the maximum number of identical characters that can be present in the password in total. |
| Max. identical characters in succession | Specifies the maximum number of identical character that can be repeated after each other. |
| Denied special | List of special characters that are not permitted. |

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

Custom scripts for password requirements

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

Detailed information about this topic

- [Script for checking passwords](#) on page 66
- [Script for generating a password](#) on page 67

Script for checking passwords

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example of a script that checks a password

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

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

To use a custom script for checking a password

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

Related topics

- [Script for generating a password](#) on page 67

Script for generating a password

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

The script replaces the ? and ! characters at the beginning of random passwords with _.

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

```
    Dim pwd = spwd.ToInsecureArray()  
    ' replace invalid characters at first position  
    If pwd.Length>0  
        If pwd(0)="?" Or pwd(0)="!"  
            spwd.SetAt(0, CChar("_"))  
        End If  
    End If
```

```
End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **IBM Notes | Basic configuration data | Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change master data** task.
 - d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
 - e. Save the changes.

Related topics

- [Script for checking passwords](#) on page 66

Password exclusion list

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

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

To add a term to the restricted list

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

Checking a password

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

To check if a password conforms to the password policy

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

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

Testing password generation

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

To generate a password that conforms to the password policy

1. In the Manager, select the **IBM Notes | Basic configuration data | Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change master data** task.

4. Select the **Test** tab.
5. Click **Generate**.

This generates and displays a password.

Initial password for new Notes user accounts

Table 19: Configuration parameters for formatting initial passwords for user accounts

| Configuration parameter | Meaning |
|---|---|
| QER Person UseCentralPassword | This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated. |
| QER Person UseCentralPassword PermanentStore | This configuration parameter controls the storage period for central passwords. If the configuration parameter is enabled, the central password is stored in the One Identity Manager database and is used for new users. If the configuration parameter is disabled, the central password is deleted from the One Identity Manager database following publishing to the existing user accounts. The central password is not available for new user accounts. |
| TargetSystem NDO Accounts InitialRandomPassword | This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy. |
| TargetSystem NDO MinPasswordLength | Specifies the minimum password length that is set in all newly calculated Notes ID files. |

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

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
 - In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword** configuration parameter.

- Apply target system specific password policies and define the character sets that the password must contain.
- Specify which employee will receive the initial password by email.
- Use the employee's central password. The employee's central password is mapped to the user account password. For detailed information about an employee's central password, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- [Password policies for Notes user accounts](#) on page 59
- [Email notifications about login data](#) on page 71

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text in a mail template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

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

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

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

To send initial login data by email

1. In the Designer, set the **TargetSystem | NDO | Accounts | InitialRandomPassword** configuration parameter.

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

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

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

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

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:

- In the Designer, create an entry for the Job server in the **Base Data | Installation | Job server** category. For detailed information, see *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **IBM Notes | Basic configuration data | Server** category and edit the Job server master data category.

Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

NOTE: One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

To edit a Job server and its functions

1. In the Manager, select the **IBM Notes | Basic configuration data | Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change master data** task.
4. Edit the Job server's master data.

5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- [Master data for a Job server](#) on page 73
- [Specifying server functions](#) on page 75

Related topics

- [Installing and configuring the One Identity Manager Service](#) on page 19

Master data for a Job server

NOTE: All editing options are also available in the Designer under **Base Data | Installation | Job server**.

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

Table 20: Job server properties

| Property | Meaning |
|------------------------------|---|
| Server | Job server name. |
| Full server name | Full server name in accordance with DNS syntax. Example: <Name of server>.<Fully qualified domain name> |
| Server is cluster | Specifies whether the server maps a cluster. |
| Server belongs to cluster | Cluster to which the server belongs. NOTE: The Server is cluster and Server belongs to cluster properties are mutually exclusive. |
| IP address (IPv6) | Internet protocol version 6 (IPv6) server address. |
| IP address (IPv4) | Internet protocol version 4 (IPv4) server address. |
| Copy process (source server) | Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported. |

| Property | Meaning |
|--|---|
| | If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is 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 | <p>Name of the executing server. The name of the server that exists physically and where the processes are handled.</p> <p>This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.</p> |
| 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 this exact 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. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used. |
| Service account data | One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server. |
| One Identity Manager Service installed | <p>Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.</p> <p>The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.</p> |
| Stop One | 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 |

| Property | Meaning |
|------------------------------|---|
| Identity Manager Service | process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> . |
| No automatic software update | Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set. |
| Software update running | Specifies whether a software update is currently running. |
| Last fetch time | Last time the process was collected. |
| Last timeout check | The time of the last check for loaded process steps with a dispatch value that exceeds the one in the Common Jobservice LoadedJobsTimeOut configuration parameter. |
| Server function | Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function. |

Related topics

- [Specifying server functions](#) on page 75

Specifying server functions

| NOTE: All editing options are also available in the Designer under **Base Data | Installation | Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

Table 21: Permitted server functions

| Server function | Remark |
|-------------------|---|
| CSV connector | Server on which the CSV connector for synchronization is installed. |
| Domain controller | The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers. |

| Server function | Remark |
|---|---|
| Printer server | Server that acts as a print server. |
| Generic server | Server for generic synchronization with a custom target system. |
| Home server | Server for adding home directories for user accounts. |
| IBM Notes gateway server | Gateway server for synchronizing One Identity Manager with IBM Notes. |
| IBM Notes connector | Server on which the IBM Notes connector is installed. This server synchronizes the IBM Notes target system. |
| Update server | <p>This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks.</p> <p>The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.</p> |
| SQL processing server | <p>It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.</p> <p>Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.</p> |
| CSV script server | This server can process CSV files using the ScriptComponent process component. |
| Native database connector | This server can connect to an ADO.Net database. |
| One Identity Manager database connector | Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system. |
| One Identity Manager Service installed | Server on which a One Identity Manager Service is installed. |
| Primary domain controller | Primary domain controller. |
| Profile server | Server for setting up profile directories for user accounts. |
| SAM synchronization | Server for running synchronization with an SMB-based target system. |

| Server function | Remark |
|------------------------------|---|
| Server | |
| SMTP host | Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration. |
| Default report server | Server on which reports are generated. |
| Windows PowerShell connector | The server can run Windows PowerShell version 3.0 or later. |

Related topics

- [Master data for a Job server](#) on page 73

Target system managers

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

Define additional application roles if you want to limit the edit permissions for target system managers to individual domains. The application roles must be added under the default application role.

For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.
Target system managers with the default application role are authorized to edit all the domains in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual domains.

Table 22: Default application roles for target system managers

| User | Tasks |
|------------------------|--|
| Target system managers | <p>Target system managers must be assigned to the Target systems IBM Notes application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects like user accounts or groups.• Edit password policies for the target system.• Prepare groups to add to the IT Shop.• Can add employees who have an other identity than the Primary identity.• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.• Edit the synchronization's target system types and outstanding objects.• Authorize other employees within their area of responsibility as target system managers and create child application roles if required. |

To initially specify employees to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)
2. Select the **One Identity Manager Administration | Target systems | Administrators** category.
3. Select the **Assign employees** task.
4. Assign the employee you want and save the changes.

To add the first employees to the default application as target system managers

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration | Target systems | IBM Notes** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

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

To specify target system managers for individual domains

1. Log in to the Manager as a target system manager.
2. Select the **IBM Notes | Domains** category.
3. Select the domain in the result list.
4. Select the **Change master data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

- OR -

Next to the **Target system manager** menu, click  to create a new application role.

- a. Enter the application role name and assign the **Target systems | IBM Notes** parent application role.
 - b. Click **OK** to add the new application role.
6. Save the changes.
 7. Assign employees to this application role who are permitted to edit the domain in One Identity Manager.

Related topics

- [One Identity Manager users for managing IBM Notes](#) on page 11
- [General master data for a Notes domain](#) on page 80

Notes domains

In One Identity Manager, a domain corresponds to the image of a specific area in IBM Notes, such as an operational IBM Notes system. Using this construction, which is far more stringently handled in One Identity Manager than in IBM Notes, it is possible to manage several productive IBM Notes environments in parallel using a One Identity Manager database. Even if a user's relation to their 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 **IBM Notes | Domains** category.
2. Select the domain in the result list.
3. Select the **Change master data** task.
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 23: 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 account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts |


| Property | Description |
|------------------------|---|
| (initial) | <p>is used for this domain and if user accounts are to be created that are already managed (Linked configured). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the employee (Linked state) if no account definition is given. This is the case on initial synchronization, for example.</p> |
| Target system managers | <p>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.</p> <p>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.</p> |
| Synchronized by | <p>Type of synchronization through which data is synchronized between the domain and One Identity Manager. You can no longer change the synchronization type once objects for these domains are present in One Identity Manager.</p> <p>If you create a domain with the Synchronization Editor, One Identity Manager is used.</p> |

Table 24: Permitted values

| Value | Synchronization by | Provisioned by |
|----------------------|---------------------|---------------------|
| One Identity Manager | IBM Notes connector | IBM Notes connector |
| No synchronization | none | none |

NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.

| | |
|-------------------|--|
| User ID file path | Path of the gateway server used for creating new user ID files. This data is only required if the TargetSystem NDO StoreIDInAddressbook configuration parameter is not set. |
| Description | Text field for additional explanation. |
| ID vault enabled | Specifies whether IBM Notes ID vault function is used to restore user ID files. |

Related topics


- [Setting up account definitions](#) on page 42
- [Assigning account definitions to a target system](#) on page 57

- [Target system managers](#) on page 77
- [Restoring user ID files](#) on page 125

Specifying categories for inheriting Notes groups

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table enter your categories for the target system-dependent groups. Each table contains the **Position 1** to **Position 31** category positions.

To define a category

1. In the Manager, select the domain in the **IBM Notes | Domains** category.
2. Select the **Change master data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- [Notes group inheritance based on categories](#) on page 144

How to edit a synchronization project

Synchronization projects in which a domain is already used as a base object can also be opened in the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor:

1. Select the **IBM Notes | Domains** category.
2. Select the domain in the result list. Select the **Change master data** task.
3. Select the **Edit synchronization project...** task.

Related topics

- [Customizing the synchronization configuration](#) on page 30

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 that are added with One Identity Manager contain a reference to the certificate in use. This means you can recover their ID files with this certificate at anytime. The certificate is the deciding factor for mapping more user account properties when managing user accounts with account definitions.

You can only synchronize Domino Directory certificates. If a user in the target system has been created with an external certificate, One Identity Manager cannot determine the certificate and therefore cannot allocate it to the user account.

To edit a certificate

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list. Select the **Change master data** task.
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 84

General master data for Notes certificates

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

Table 25: General master data for a Notes certificate

| Property | Description |
|-----------|-------------------------------|
| Full name | Full name of the certificate. |

| Property | Description |
|------------------------------------|--|
| Parent certifier | Unique ID for the parent certifier. Enter the name of the issuer of the certificate. |
| Notes domain | Unique domain name. |
| Notes server | Notes server on which the certifier's mailboxes are stored. |
| Mailbox file | Path to the certifier's mailbox file. |
| ID file name (including path) | Name and path of the certificate's ID file. If user accounts should be registered with the certificate, enter the full path of the certifier's ID file. The directory to save the ID file in, must be reachable by the gateway server. This data is only required if the CA process possible option is disabled. |
| Password and password confirmation | Password of the certifier's ID file. This data is only required if the CA process possible option is disabled. |
| CA process possible | Specifies whether the CA process is used for certifying user accounts. If this option is not set, a certifier ID file is required for certification. |
| CA database server | Server which provides the CA database for this certificate. This data is only required if the CA process possible option is enabled. |
| CA database name | Name or path of the CA database file. This data is only required if the CA process possible option is enabled. |
| Due date | Certificate expiry date. |
| Certificate type | Type of certificate. |

Notes certificates contact data

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

Table 26: Notes certifier's contact data

| Property | Description |
|------------|-------------------------|
| Company | Certifier's company. |
| Department | Certifier's department. |

| Property | Description |
|---------------|--|
| Location | Certifier's location. |
| Email address | Certifier's email address. |
| Phone, office | Certifier's office telephone number. |
| Comment | Text field for additional explanation. |

Additional tasks for managing Notes certificates

After you have entered the master data, you can run the following tasks.

Overview of Notes certificates

To obtain an overview of a certificate

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

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 **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as owners of a certificate

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove the groups.
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 **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators for a certificate

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove the groups.
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 to the synchronization user's personal address book on a regular basis.

To use new certificates for registering user accounts

1. Copy the certificates from the Domino Directory in the synchronization user's personal address book.
For more information, see [Copying the Notes certificate](#) on page 18.
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 84.

Notes certificate requests

Certificate requests are mapped in One Identity Manager for all documents that were certified using the CA process. All certificate requests for a certificate are displayed on the certificate's overview form.

To display a certificate request's properties

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list. Select the **Notes certificate overview** task.
3. Select a certificate request on the **Notes certificate requests** form element.
4. Select the **Change master data** task.

Table 27: Notes certificate request master data

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

Notes templates

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 One Identity Manager templates in Notes for this purpose.

To edit a template's master data

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

Table 28: 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. |

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 **IBM Notes | Policies** category.
2. Select the policy in the result list. Select the **Change master data** task.

Table 29: 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. |
| 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 93

Additional tasks for managing Notes policies

After you have entered the master data, you can run the following tasks.

Displaying an overview of Notes policies

To obtain an overview of a policy

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

Assigning members to a Notes policy

Assign the user accounts and groups to which the policy will apply.

To assign user accounts to a policy

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign members** task.
4. Select "Notes user accounts" in the **Table** field.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To assign groups to a policy

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

4. Select "Notes groups" in the **Table** field.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove the groups.
6. Save the changes.

Assigning owners to a Notes policy

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 **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign owner** task.
4. Select "Notes user accounts" in the **Table** field.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as owner

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign owner** task.
4. Select "Notes groups" in the **Table** field.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove the groups.
6. Save the changes.

Assigning administrators to a Notes policy

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 **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign administrators** task.
4. Select "Notes user accounts" in the **Table** field.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators

1. Select the **IBM Notes | Certificates** category.
2. Select a certificate in the result list.
3. Select the **Assign administrators** task.
4. Select "Notes groups" in the **Table** field.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove the groups.
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 **IBM Notes | Policies** category.
2. Select a policy in the result list. Select the **Change master data** task.
3. Select an assigned policy setting and open the context menu.
4. Click **Go to assigned object**.
5. Select the **Change master data** task.

Table 30: 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 90

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 95
- [Supported user account types](#) on page 96
- [Entering master data for Notes user accounts](#) on page 100

Linking user accounts to employees

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

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

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a Notes domain, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

Employee documents can also be created through account definitions.

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

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

Related topics

- [Entering master data for Notes user accounts](#) on page 100
- [Setting up account definitions](#) on page 42
- [Automatic assignment of employees to user accounts](#) on page 118
- For more detailed information about employee handling and administration, see the 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, service accounts, or privileged user accounts, can be mapped in One Identity Manager.

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

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

Table 31: Identities of user accounts

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

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

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

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

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

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

- Privileged user account

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

Default user accounts

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

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

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

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

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

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

5. Assign the account definition to employees.

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

Administrative user accounts

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

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

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

You can label administrative user accounts as a **Personalized administrator identity** or as a **Shared identity**. Proceed as follows to provide the employees who use this user account with the required permissions.

- Personalized admin identity
 1. Use the `UID_Person` column to link the user account with an employee.
Use an employee with the same identity or create a new employee.
 2. Assign this employee to hierarchical roles.
- Shared identity
 1. Assign all employees with usage authorization to the user account.
 2. Link the user account to a dummy employee using the `UID_Person` column.
Use an employee with the same identity or create a new employee.
 3. Assign this dummy employee to hierarchical roles.

The dummy employee provides the user account with its permissions.

Privileged user accounts

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

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

To create privileged users through account definitions

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

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

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

- In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
- You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.

- To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the IsGroupAccount column with a default value of **0** and set the **Always use default value** option.
5. Enter the effective IT operating data for the target system.
Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
 6. Assign the account definition directly to employees who work with privileged user accounts.
When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, create the template according to which the login names are formed.


Entering master data for Notes user accounts

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

To create a user account

1. In the Manager, select the **IBM Notes | User accounts** category.
2. Click  in the result list.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

1. In the Manager, select the **IBM Notes | User accounts** category.
2. Select the user account in the result list and run the **Change master data** task.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

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

Detailed information about this topic

- [General master data of a Notes user account](#) on page 101
- [Additional master data of a Notes user account](#) on page 107
- [Notes user account email system](#) on page 104
- [Notes user account address data](#) on page 107
- [Administrative data for a Notes user account](#) on page 108

Related topics

- [Setting up account definitions](#) on page 42
- [Supported user account types](#) on page 96
- [Linking user accounts to employees](#) on page 95

General master data of a Notes user account


Table 32: Configuration parameters for risk assessment of user accounts

| Configuration parameter | Effect when set |
|--------------------------------|--|
| QER CalculateRiskIndex | <p>Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database.</p> <p>If the parameter is enabled, values for the risk index can be entered and calculated.</p> |

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

Table 33: General master data of a Notes user account

| Property | Description |
|-----------------|--|
| Employee | Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create |

| Property | Description |
|--------------------|--|
| | <p>the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account.</p> <p>You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.</p> |
| Account definition | <p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account master data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p>NOTE: The account definition cannot be changed once the user account has been saved.</p> <p>Employee documents can also be created through account definitions.</p> |
| Manage level | <p>Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.</p> |
| 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 | <p>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.</p> <p>If a certificate is not assigned when a new user account is saved, the certificate cannot be assigned later.</p> <p>If a certificate is assigned when a new user account is saved, the certificate cannot be removed later.</p> |

| Property | Description |
|--------------------------|--|
| Organizational unit | Additional organization unit belonging to the user account. |
| Display name | User account display name. The display name is made up of the full name or the first and last names. |
| Title | User's title. |
| Generational affix | User's generational affix, for example, "Junior". |
| Alternative language | Alternative language for the alternative names. |
| Alternative name | Alternative name in the user's 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. |
| 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 value of all assigned groups. The property is only visible if the QER CalculateRiskIndex configuration parameter is set. For detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> . |
| Category | Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu. |
| User account is disabled | Specifies whether the user account is blocked from logging in to the domain. |
| Identity | User account's identity type Permitted values are: <ul style="list-style-type: none"> • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account that is used for a specific purpose, such as training. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this |

| Property | Description |
|-------------------------|---|
| | <p>user account.</p> <ul style="list-style-type: none"> • Service identity: Service account. |
| Privileged user account | Specifies whether this is a privileged user account. |
| Groups can be inherited | <p>Specifies whether the user account can inherit groups through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests.</p> <ul style="list-style-type: none"> • 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 42
- [Linking user accounts to employees](#) on page 95
- [Supported user account types](#) on page 96
- [Notes user account email system](#) on page 104
- [Specifying categories for inheriting Notes groups](#) on page 82
- [Locking and unlocking Notes user accounts](#) on page 127

Notes user account email system

Table 34: Configuration parameters for creating a mailbox file

| Configuration parameter | Effect when set |
|-----------------------------------|--|
| TargetSystem NDO CreateMailDB | <p>This configuration parameter specifies whether the mailbox file is created after or during registration of the Notes user in 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.</p> <p>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 "TargetSystem NDO DefTemplatePath".</p> |

| Configuration parameter | Effect when set |
|--------------------------------------|---|
| 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 Has Notes mailbox files option are available. |
| Notes | Mailbox template | <p>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.</p> <p>The data can be determined with the employee's IT operating data. If you do not enter a template, the template entered in "TargetSystem NDO DefTemplatePath" is used.</p> |
| Notes | Mailbox | Name and path of the mailbox file. These are created using |

| Email system | Property | Description |
|---|-----------------------|---|
| POP or IMAP | file | 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: <ul style="list-style-type: none"> • 0 - Notes • 1 - Notes and Internet Mail • 2 - Internet Mail |
| 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 Has Notes mailbox files option are |

| Email system | Property | Description |
|--------------|---------------|--|
| | | 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 123

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 of a Notes user account

Enter the additional data for a user account on the **Miscellaneous** tab. This data is mainly for the mailbox file and message forwarding. You can find the size of a user account's mailbox on regular basis using a scheduled process plan. Prerequisite for this is that you enter the correct mail server data and the mailbox file path on the **General** tab.

To find out the size of the user account's mailbox file

- In Designer, configure and enable the **Load IBM Notes mail file sizes for NOTES users** schedule.

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

Table 36: Additional master data of a Notes user account

| Property | Description |
|--------------------|---|
| Size [KB] | Logical size of the mailbox file. |
| Physical size [KB] | Physical size of the mailbox file. |
| Max. size [KB] | Maximum permitted size of the mailbox. |
| Warn at [KB] | When this threshold is exceeded, users are sent an email. |

| Property | Description |
|---|--|
| Internet password/Password confirmation | The user's internet password. Web users must use this password for authentication on a Domino web server. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements. |
| Sametime server | Notes server used as a sametime server. Enter a sametime server for user accounts, which use the IBM Notes sametime function. |
| Calendar domain | The domain that applies if the user account uses different calendar and schedule functionality. |
| Website | The user's website. |
| Comment | Text field for additional explanation. |

Related topics

- [Password policies for Notes user accounts](#) on page 59

Administrative data for a Notes user account

Enter the administrative data of a user account on the **Administration** 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. | | | | |
| Password check type | Specifies how users must authenticate themselves on the server. Password check types are: <table> <tr> <td>0 - don't check: :Password not checked</td><td>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.</td></tr> <tr> <td>1 - check:</td><td>Password checked</td></tr> </table> | 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 |
| 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 | | | | |

| Property | Description |
|------------------------------------|--|
| | <p>The user must provide a password to log in to the server.</p> <p>2 - Lockout ID: ID is locked</p> <p>The user cannot log in on any server in the domain that checks passwords.</p> <p>When a new user account is created, the 0 - don't check password check type is applied by default.</p> |
| 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 | <p>Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>If you use an initial password for the user accounts, it is automatically entered when a user account is created.</p> <p>The password is deleted from the database after publishing to the target system.</p> <p>No password is required for purely employee documents.</p> <p>NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.</p> |
| Change password at next login | Specifies whether the user account password must be changed on the next login. |
| Notes client license | <p>License type of the Notes client. The license type determines the range of user access. Possible license types are:</p> <ul style="list-style-type: none"> • 0 - IBM Notes • 1 - IBM Notes Mail |

| Property | Description |
|---|---|
| | <ul style="list-style-type: none"> • 2 - IBM Notes Desktop • 3 - IBM Notes Designer • 4 - IBM Notes Administration • 5 - IBM iNotes®/Domino® CAL <p>When a new user account is created, the 0 - IBM Notes license type is applied by default.</p> |
| 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, such as Active Directory. |
| Full name | Full name of the user account. Full name is made up of the first name, last name, certificate, and organizational unit. |
| ID expires | <p>User ID file's expiry date. The expiry date is calculated using a template. User ID file for enabled user accounts that will expire in less than 10 days can be extended by two years.</p> <p>To extend the expiry date</p> <ul style="list-style-type: none"> • In the Designer, configure and enable the Automatically extend IBM Notes ID expiry data schedule. <p>For more detailed information about configuring schedules, see the <i>One Identity Manager Operational Guide</i>.</p> |

Related topics

- [Notes server](#) on page 163
- [Password policies for Notes user accounts](#) on page 59
- [Initial password for new Notes user accounts](#) on page 70

Additional tasks for managing Notes user accounts

After you have entered the master data, you can run the following tasks.

Displaying the Notes user accounts overview

To obtain an overview of a user account

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

Changing the manage level of user accounts

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

To change the manage level for a user account

1. In the Manager, select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

Related topics

- [General master data of a Notes user account](#) on page 101

Assigning Notes groups directly to a Notes user account

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

To react quickly to special requests, you can assign groups directly to the user account.


To assign groups directly to user accounts

1. In the Manager, select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups** task.

4. In the **Add assignments** pane, assign groups. To filter the groups, select a domain in the **Notes Domains** input field.

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

To remove an assignment

- Select the group and double-click .

5. Save the changes.

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

Related topics

- [Assigning Notes groups to Notes user accounts](#) on page 133
- [Maintaining excluded and additional lists](#) on page 117
- [Memberships in dynamic groups](#) on page 153

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 **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify an owner for groups

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

5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
6. Save the changes.

To specify an owner for mail-in databases

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.
 - OR -In the **Remove assignments** pane, remove mail-in databases.
6. Save the changes.

To specify an owner for certificates

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.
 - OR -In the **Remove assignments** pane, remove the certificates.
6. Save the changes.

To specify an owner for server documents

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign document owner** task.
4. Select the **Server document** tab.
5. In the **Add assignments** pane, assign the server documents.
 - OR -In the **Remove assignments** pane, remove the server documents.
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 **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as owner

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign owner** task.
4. Select the **Group** tab.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove the groups.
6. Save the changes.

Assigning administrative 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 **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts.
- OR -

In the **Remove assignments** pane, remove user accounts.

6. Save the changes.

To specify an administrator for groups

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

- OR -

In the **Remove assignments** pane, remove groups.

6. Save the changes.

To specify an administrator for mail-in databases

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

- OR -

In the **Remove assignments** pane, remove mail-in databases.

6. Save the changes.

To specify an administrator for certificates

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

- OR -

In the **Remove assignments** pane, remove the certificates.

6. Save the changes.

To specify an administrator for servers

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

5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
6. Save the changes.

To specify an administrator for server documents

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Server document** tab.
5. In the **Add assignments** pane, assign the server documents.
- OR -
In the **Remove assignments** pane, remove the server documents.
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 **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign administrators** task.
4. Select the **User** tab.
5. Assign user accounts in **Add assignments**.
- OR -
Remove user accounts from **Remove assignments**.
6. Save the changes.

To specify groups as administrators

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

5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove the groups.
6. Save the changes.

Maintaining excluded and additional 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 **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Additional** tab.
5. In the **Add assignments**, assign the groups in whose additional list the user account is to be a member.
 - OR -In the **Remove assignments** pane, remove groups.
6. Save the changes.

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

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Excluded** tab.
5. In the **Add assignments** pane, assign the groups in whose excluded list the user account is to be a member.
 - OR -In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Memberships in dynamic groups](#) on page 153

Assigning extended properties

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

To specify extended properties for a user account

1. Select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.
- OR -
In the **Remove assignments** pane, remove extended properties.
5. Save the changes.

For more detailed information about setting up extended properties, see the 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 are listed in a pipe () delimited list that is handled as a regular search pattern. |
| TargetSystem NDO PersonAutoDisabledAccounts | This configuration parameters specifies whether employees are automatically assigned to locked user accounts. User accounts do not obtain an account definition. |

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 on the basis of

existing user account master data. This mechanism can be triggered after a new user account is created either manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the "TargetSystem | NDO | PersonAutoFullsync" configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the "TargetSystem | NDO | PersonAutoDefault" configuration parameter and select the required mode.
- In the "TargetSystem | NDO | PersonExcludeList" configuration parameter, specify the user accounts that must not be assigned automatically to employees.

Example:

ADMINISTRATOR

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

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the domain is not yet known at the

time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

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

To select user accounts through account definitions

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

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

Related topics

- [Creating an account definition](#) on page 43
- [Assigning account definitions to a target system](#) on page 57
- [Editing search criteria for automatic employee assignment](#) on page 120

Editing search criteria for automatic employee assignment

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

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

NOTE: 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 assignments to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user accounts 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 **IBM Notes | Domains** category.
2. Select the domain in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 39: Default search criteria for user accounts

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

5. Save the changes.

Direct assignment of employees to user accounts based on a suggestion list

In the **Assignments** pane, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly. 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 using a suggestion list

1. Click **Suggested assignments**.

- a. Check the **Selection** box of all the user accounts to which you want to assign the suggested employees. Multi-select is possible.
- b. Click **Assign selected**.
- c. Confirm the security prompt with **Yes**.
The employees found using the search criteria are assigned to the selected user accounts.

– OR –

2. Click **No employee assignment**.

- a. Click the **Select employee** option of the user account to which you want to assign an employee. Select an employee from the menu.
- b. Check the **Selection** box of all the 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**.
The employees displayed in the **Employee** column are assigned to the selected user accounts.

To remove assignments

1. Click **Assigned user accounts**.

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

The assigned employees are removed from the selected user accounts.

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

Related topics

- [Automatic assignment of employees to user accounts](#) on page 118

Generating mailbox files

Table 41: Configuration parameters for creating a mailbox file

| Configuration parameter | Effect when set |
|--------------------------------------|--|
| TargetSystem NDO CreateMailDB | <p>This configuration parameter specifies whether the mailbox file is created after or during registration of the Notes user in 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.</p> <p>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 "TargetSystem NDO DefTemplatePath" configuration parameter.</p> |
| 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 "TargetSystem | NDO | CreateMailDB" configuration parameter 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 must exist on the gateway server.

"TargetSystem | NDO | CreateMailDB" is set.

If it is necessary to create the mailbox during the Notes user's registration, set the "TargetSystem | NDO | CreateMailDB" configuration parameter. 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 104
- [Additional master data of a Notes user account](#) on page 107

Saving user ID files

Table 42: Configuration parameters for creating a mailbox file

| Configuration parameter | Effect when set |
|---|---|
| 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 should 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 "TargetSystem | 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 One Identity Manager Target System Synchronization Reference Guide.

To specify the user ID file location on the gateway server

1. In the Designer, disable the configuration parameter "TargetSystem | NDO | StoreIDInAddressbook".
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 80
- [General master data for Notes servers](#) on page 163
- [Notes user account email system](#) on page 104

Restoring user ID files

If a user has forgotten the password to a user account and lost the user ID file, the user ID file can be restored. Since IBM Notes version 8.5, IBM Domino provides the ID vault function to do this.

One Identity Manager uses "ID Restore" to provide its own method for restoring the user ID files. This can be used if an older version of 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 an 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. One Identity Manager provides a process for resetting the passwords in the ID vault.

Prerequisites

- The Domino server that communicates with the gateway server, is also the ID vault server.
- There are executing permissions defined for agents for the synchronization user account. For more information, see [Running restricted LotusScript/Java agents](#) on page 182.
- ID vault database permissions for the synchronization user account are set to: "Manager" access function and "Auditor" role. 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 **IBM Notes | Domains** category.
2. Select the domain you want to use for the ID vault in the result list and run the **Change master data** task.
3. Set the **ID vault enabled** option.
This setting effects all user accounts in the domain.
4. Save the changes.

NOTE: If certain user accounts are excluded from the ID vault by the ID vault policy in 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 IBM Notes, One Identity Manager saves the initial password in the One Identity Manager database (NDOUser.PasswordInitial). This initial password is used when a user account password needs to be reset. Passwords are saved automatically for user accounts that are initially setup in One Identity Manager. The initial password for all other user accounts has to be transferred to the One Identity Manager database by a customized process.

To reset a user account password

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

This task starts the NDO_NDOUser_PWReset_from_Vault process. This process replaces the password from the user ID file saved in the ID Vault with the initial password from the One Identity Manager database. If the user is logged into the 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 **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **ID restore** task.

The ID restore process carries out the following steps:

- Deletes all current employee documents from the Domino directory.
 - Copies initial employee documents from archive database to the Domino directory.
 - Exports the initially saved ID files to the gateway server.
 - Starts the AdminP request to track the changes made to the original ID up until now. This includes changes to the components of the user's name, changes to the ID expiry date and exchanging certifiers.
 - Update the restored employee document using the known values.
4. If the ID file is restored, provide the user with the ID file and the initial password.

Related topics

- [Creating an archive database for backing up employee documents](#) on page 22

Locking and unlocking Notes user accounts

Table 43: Configuration parameters for locking/unlocking user accounts

| Configuration parameter | Effect when set |
|---------------------------------------|---|
| 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 "Not access server" permissions type for the corresponding server document. This is very complicated in environments with several servers because a user account, which is going to be locked, must be given this permissions type for every server document.

For this reason, denied access groups are used. Each denied access group initially gets the "Not access server" permissions type for each server document. A user that is going to be

locked becomes a member of the denied access group and therefore is automatically prevented from accessing the domain servers.

The way you lock user accounts depends on how they are managed.

Scenario:

- The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `NDOUser.AccountDisabled` column.

Scenario:

- The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the employee's user accounts are locked when the employee is permanently or temporarily disabled.
- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To lock the user account when the configuration parameter is disabled

1. In the Manager, select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To lock a user account that is no longer linked to an employee

1. In the Manager, select the **IBM Notes | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

The user account becomes anonymous when it is locked and is not shown in address books. Access to Notes servers is removed. The "TargetSystem | NDO | MailBoxAnonymPre" configuration parameter is checked if the user is made anonymous.

To unlock a user account

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

Anonymity is rescinded and the user account removed from denied access groups.

Detailed information about this topic

- [Locking groups](#) on page 151

Related topics


- [Setting up account definitions](#) on page 42
- [Creating manage levels](#) on page 45

Deleting and restoring 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 assignment of an account definition is removed, the user account that was created from this account definition is deleted.

To delete a user account

1. Select the **IBM Notes | User accounts** category.
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 a user account

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

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 accounts are deleted from the database and cannot be restored anymore. In the Designer, you can set an alternative delay on the NDOUser table.


Related topics

- [Locking and unlocking Notes user accounts](#) on page 127

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 group's type specifies its intended purpose and whether it is visible in the Domino Directory.

To edit group master data

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the group's master data.
4. Save the changes.

Detailed information about this topic

- [General master data for Notes groups](#) on page 131


General master data for Notes groups

Table 44: Configuration parameters for risk assessment of user accounts

| Configuration parameter | Effect when set |
|--------------------------|---|
| 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 enabled, values for the risk index can be entered and calculated. |

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. |
| Notes domain | Domain in which the group is managed. |
| Group type | <p>Purpose of the group. The group type defines the visibility of the group in the Domino directory.</p> <p>Applicable group types are:</p> <ul style="list-style-type: none"> • 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 | <p>Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is activated.</p> <p>For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.</p> |
| Category | <p>Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.</p> <p>For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.</p> |
| 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 | Text field for additional explanation. |
| Allow foreign | Specifies whether the information about this group can be forwarded to |

| Property | Description |
|---------------------------|---|
| directory synchronization | a foreign directory. |
| Locked group | Specifies whether the group is set as a denied access group. |
| IT Shop | <p>Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.</p> <p>The option cannot be set if the group is a dynamic group.</p> <p>For more detailed information, see the One Identity Manager IT Shop Administration Guide.</p> |
| Only for use in IT Shop | Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted. |
| Dynamic group | Specifies whether this is a dynamic group. This option is set depending on the setting of "Import dynamic members". |

Detailed information about this topic

- [Extension groups](#) on page 153
- [Specifying categories for inheriting Notes groups](#) on page 82
- [Dynamic groups](#) on page 152
- [Locking groups](#) on page 151

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 (departments, cost centers, locations, or business roles).
- User accounts are marked with the **Groups can be inherited** option.
- User accounts and groups belong to the same domain.

Groups can also be assigned to employees through IT Shop requests. So that groups can be assigned using IT Shop requests, employees are added to a shop as customers. All groups 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 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 134
- [Assigning Notes groups to business roles](#) on page 135
- [Assigning Notes user accounts directly to a Notes group](#) on page 136
- [Adding Notes groups to system roles](#) on page 137
- [Adding Notes groups to the IT Shop](#) on page 138

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. This task is not available for dynamic groups.

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

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

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

To remove an assignment

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

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

1. In the Manager, select the **Organizations | Departments** category.
- OR -

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


- OR -

In the Manager, select the **Organizations | Locations** category.

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

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

To remove an assignment

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

Related topics

- [Assigning Notes groups to business roles](#) on page 135
- [Assigning Notes user accounts directly to a Notes group](#) on page 136
- [Adding Notes groups to system roles](#) on page 137
- [Adding Notes groups to the IT Shop](#) on page 138
- [One Identity Manager users for managing IBM Notes](#) on page 11

Assigning Notes groups to business roles

Installed modules: Business Roles Module


You assign groups to business roles in order to assign them to user accounts over business roles. This task is not available for dynamic groups.

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

1. In the Manager, select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

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

To remove an assignment


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

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

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

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

To remove an assignment

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

Related topics

- [Assigning Notes groups to departments, cost centers and locations](#) on page 134
- [Assigning Notes user accounts directly to a Notes group](#) on page 136
- [Adding Notes groups to system roles](#) on page 137
- [Adding Notes groups to the IT Shop](#) on page 138
- [One Identity Manager users for managing IBM Notes](#) on page 11

Assigning Notes user accounts directly to a Notes group

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

To assign a group directly to user accounts

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts. To filter the user accounts in the list, select a domain in the **Notes domains** field.
 - OR -
 - In the **Remove assignments** pane, remove the user accounts.
6. Save the changes.

Related topics

- [Assigning Notes groups directly to a Notes user account on page 111](#)
- [Assigning Notes groups to departments, cost centers and locations on page 134](#)
- [Assigning Notes groups to business roles on page 135](#)
- [Adding Notes groups to system roles on page 137](#)
- [Adding Notes groups to the IT Shop on page 138](#)
- [Assigning owners to Notes groups on page 149](#)
- [Assigning administrators to Notes groups on page 150](#)

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 user accounts belonging to these employees inherit the group. This task is not available for dynamic groups.


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

To assign a group to system roles

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

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

To remove an assignment

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

Related topics

- [Assigning Notes groups to departments, cost centers and locations on page 134](#)
- [Assigning Notes groups to business roles on page 135](#)
- [Assigning Notes user accounts directly to a Notes group on page 136](#)
- [Adding Notes groups to the IT Shop on page 138](#)

Adding Notes groups to the IT Shop

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

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

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

- If you only want the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

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

To add a group to the IT Shop.

1. In the Manager select the **IBM Notes | Group** category (non role-based login) category.
- OR -
In the Manager, select the **Entitlements | Notes groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the group to the IT Shop shelves.
5. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager select the **IBM Notes | Group** category (non role-based login) category.
- OR -
In the Manager, select the **Entitlements | Notes groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
5. Save the changes.

To remove a group from all shelves of the IT Shop

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

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

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

Related topics

- [General master data for Notes groups on page 131](#)
- [Assigning Notes groups to departments, cost centers and locations on page 134](#)
- [Assigning Notes groups to business roles on page 135](#)
- [Assigning Notes user accounts directly to a Notes group on page 136](#)
- [Adding Notes groups to system roles on page 137](#)

Additional tasks for managing Notes groups

After you have entered the master data, you can run the following tasks.

Displaying an overview of Notes groups

To obtain an overview of a group

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

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 **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases. To filter the mail-in databases in the list, select a domain in the **Notes domains** field.
- OR -
In the **Remove assignments** pane, remove the mail-in DBs.
6. Save the changes.

Related topics

- [Assigning Notes user accounts directly to a Notes group](#) on page 136
- [Assigning Notes servers to a Notes group](#) on page 140
- [Adding Notes groups to Notes groups](#) on page 141

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 **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign the servers. To filter the servers shown, select a domain in the **Notes domains** field.
- OR -
In the **Remove assignments** pane, remove the servers.
6. Save the changes.

Related topics

- [Assigning Notes user accounts directly to a Notes group](#) on page 136
- [Assigning Notes mail-in databases to Notes groups](#) on page 140
- [Adding Notes groups to Notes groups](#) on page 141

Adding Notes groups to Notes groups

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

To assign child groups

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign members** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign child groups. To filter the groups, select a domain in the **Notes Domains** input field.
 - OR -
 - In the **Remove assignments** pane, remove the child groups.
6. Save the changes.

To assign parent groups

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign parent groups** task.
4. In the **Add assignments** pane, assign parent groups. To filter the groups, select a domain in the **Notes Domains** input field.
 - OR -
 - In the **Remove assignments** pane, remove the parent groups.
5. Save the changes.

Related topics

- [Assigning Notes user accounts directly to a Notes group](#) on page 136
- [Assigning Notes servers to a Notes group](#) on page 140
- [Assigning Notes mail-in databases to Notes groups](#) on page 140

Effectiveness of group memberships

Table 46: Configuration parameters for conditional inheritance

| Configuration parameter | Effect when set |
|---|---|
| QER Structures Inherit 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 this parameter require the database to be recompiled. |

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

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

NOTE:

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

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

Example of the effect of group memberships

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

Clara Harris has a user account in this domain. She primarily belongs to the "Marketing" department. The "Control group" business role and the "Finance" department 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 (NDOGroupExclusion table)

| 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 "control group" business role 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 **QER | Structures | Inherit | GroupExclusion** configuration parameter is set.
- Mutually exclusive groups belong to the same domain

To exclude a group

1. In the Manager, select the **IBM Notes | Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.
- OR -
In the **Remove assignments** pane, remove the groups that are not longer mutually exclusive.
5. Save the changes.

Notes group inheritance based on categories

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table enter your categories for the target system-dependent groups. Each table contains the **Position 1** to **Position 31** category positions.

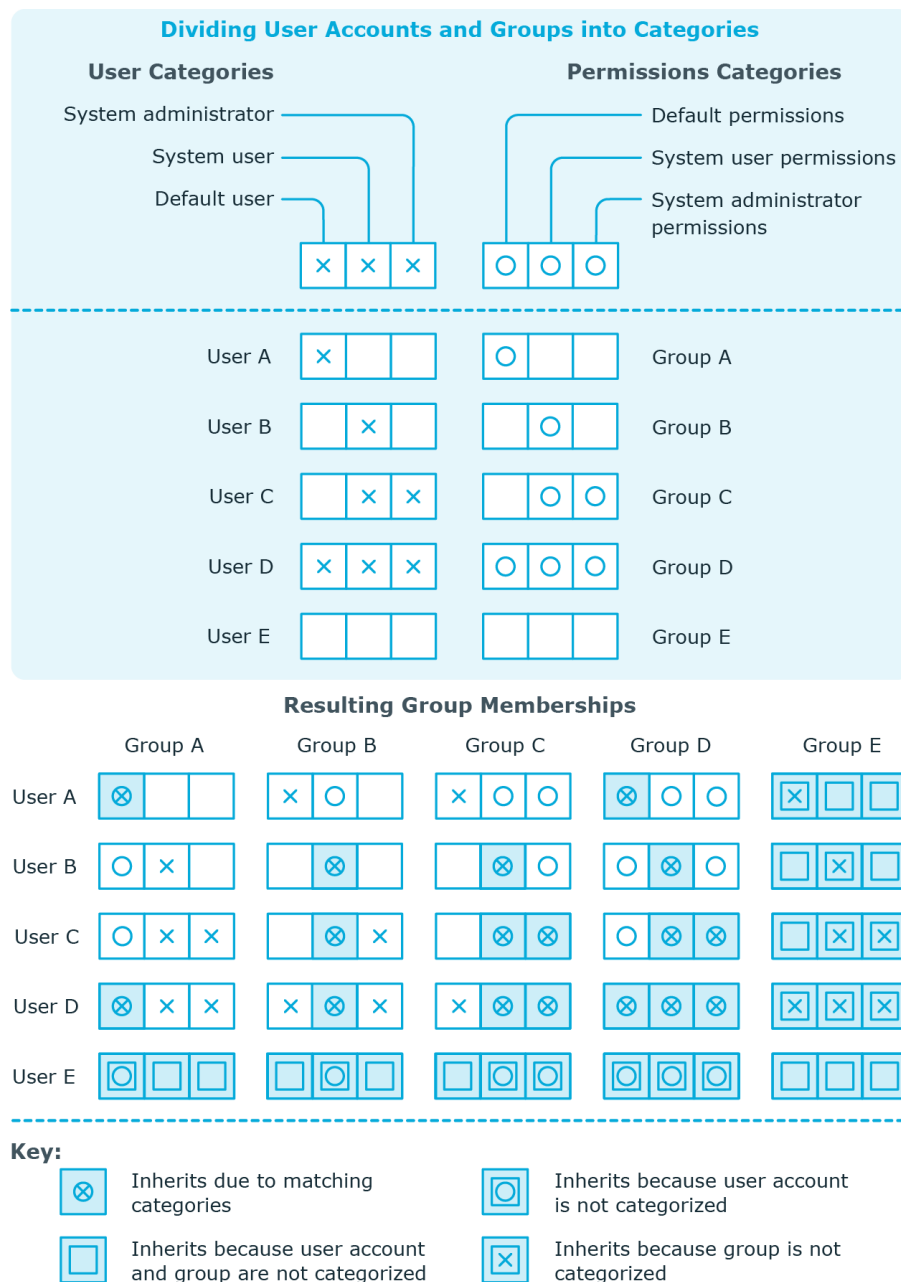
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or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

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

Table 50: Category examples

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

Figure 2: Example of inheriting through categories.



To use inheritance through categories

- 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 82
- [General master data of a Notes user account](#) on page 101
- [General master data for Notes groups](#) on page 131

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 **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify a group as group owner

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

To specify a group as mail-in database owner

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select **Mail-in DB**.

5. In the **Add assignments** pane, assign mail-in databases.
- OR -
In the **Remove assignments** pane, remove mail-in databases.
6. Save the changes.

To specify a group as certificate owner

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.
- OR -
In the **Remove assignments** pane, remove the certificates.
6. Save the changes.

To specify a group as server owner

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign document owner** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
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 **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **User** tab.

5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify a group as administrator for groups

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

To specify a group as administrator for mail-in databases

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.
- OR -
In the **Remove assignments** pane, remove mail-in databases.
6. Save the changes.

To specify a group as administrator for certificates

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Certificate** tab.
5. In the **Add assignments** pane, assign certificates.
- OR -
In the **Remove assignments** pane, remove the certificates.
6. Save the changes.

To specify a group as administrator for server documents

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.

3. Select the **Assign administrable documents** task.
4. Select the **Server document** tab.
5. In the **Add assignments** pane, assign the server documents.
 - OR -
 - In the **Remove assignments** pane, remove the server documents.
6. Save the changes.

To specify a group as administrator for servers

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrable documents** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign servers.
 - OR -
 - In the **Remove assignments** pane, remove servers.
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 **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign owner** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as owner of a group

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign owner** task.
4. Select the **Groups** tab.

5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove the groups.
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 **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrators** task.
4. Select the **User** tab.
5. In the **Add assignments** pane, assign user accounts.
 - OR -In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators for groups

1. Select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign administrators** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove the groups.
6. Save the changes.

Assigning extended properties to Notes groups


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

To specify extended properties for a group

1. In the Manager, select the **IBM Notes | Groups** category.
2. Select the group in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

- Select the extended property and double-click .
5. Save the changes.

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

Locking groups

Table 51: Configuration parameter for setting up denied access groups

| Configuration parameter | Effect when set |
|---|--|
| 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 "Not access server" permissions type for the corresponding server document. This is very complicated in environments with several servers because a user account, which is going to be locked, must be given this permissions type for every server document.

For this reason, denied access groups are used. Each denied access group initially gets the "Not access server" permissions type for each server document. A user that is going to be locked becomes a member of the denied access group and therefore is automatically prevented from accessing the domain servers.

Immediately after a user account has been locked in One Identity Manager, a denied access group is found for the user. If a denied access group of the right type is not found, the One Identity Manager Service creates a new group, "Deny list only", and automatically stores it on each server with "Not access server". The group name is made up of a prefix and a sequential index (for example "viDenyAccess0001"). Furthermore, this group is labeled with **Denied access group**.

To change the prefix of a denied access group.

1. In the Designer, edit "TargetSystem | NDO | DenyAccessGroups | Prefix".
2. Enter the prefix when a denied access group is initially created.
3. Save the changes.

It is also possible to specify the maximum number of user accounts in a denied access group. This is necessary in an environment with a large number of user accounts to prevent the maximum number of user names in one group being exceeded. If this limit is reached, a new denied access group is created with an index value incremented by "1" and added with the permissions type "Not access server" on all domain servers.

To change the number of user accounts permitted in a denied access group

- In the Designer, edit the value of "TargetSystem | NDO | DenyAccessGroups | Memberlimit".

TIP: The denied access groups are found using the VI_Notes_GetOrCreateRestrictGroup script and 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 **Denied access group** for this group.
2. Modify the prefix in "TargetSystem | NDO | DenyAccessGroups | Prefix" if necessary.
3. Modify the VI_Notes_GetOrCreateRestrictGroup script 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 "Home server" is selected in "Load dynamic member" (column AutoPopulateInput = '1'). Members cannot be assigned directly to these groups.

Dynamic groups are excluded from inheritance through hierarchical roles. This means that system roles, business roles, and organizations cannot be assigned to dynamic groups.

Inheritance exclusion cannot be defined and dynamic groups cannot be requested in the IT Shop.

Extension groups

If the maximum number of members in a group has been reached, IBM Notes adds so called extension groups. These extension groups are imported into the One Identity Manager database by synchronization and cannot be edited. The connection to the dynamic group is created using the **Parent Notes group** property (UID_NotesGroupParent column). Excluded and additional lists are maintained exclusively for parent dynamic groups. Extension groups are only shown on the overview form.

Memberships in dynamic groups

You cannot assign members directly to dynamic groups. Members are determined over the home servers assigned to the group. All user accounts that are assigned as mail server to this server are automatically members of the dynamic group. In addition, memberships can be edited through an excluded and additional list. At the same time, user accounts that are assigned to both the excluded and additional lists cannot be members of the dynamic group. User accounts and groups can both be added to the excluded and additional lists.

When 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 a member of a Notes group
- Are assigned to an excluded list
- Are assigned to an excluded list as a member of a Notes group.

Effective memberships in dynamic groups (table NDOUserInGroup) are not maintained in One Identity Manager, but only loaded in the One Identity Manager by synchronization. Excluded and additional lists can be edited in the Manager. Changes are immediately provisioned in the target system. Membership lists are recalculated there. After resynchronizing, the changes to the effective memberships are visible in One Identity Manager and can be taken into account by, for example, compliance checking.

If you use One Identity Manager's identity audit functionality and also check memberships in dynamic Notes groups in compliance rules, note the following:

NOTE: Changes to the excluded and additional lists in the Manager, cannot be immediately acted upon as effective memberships in dynamic groups are not updated until after resynchronization. Customize the synchronization schedule for your 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 One Identity Manager Target System Synchronization Reference Guide.

Additional tasks for dynamic groups

To maintain memberships in dynamic groups, apply the following tasks to dynamic groups. **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 **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Assign home server** task.
4. In the **Add assignments** pane, assign the servers. To filter the servers shown, select a domain in the **Notes domains** field.
 - OR -
 - In the **Remove assignments** pane, remove the servers.
5. Save the changes.

Editing the excluded list

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

To exclude user accounts from a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Users** tab.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To exclude groups from a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

To exclude servers from a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
6. Save the changes.

To exclude mail-in databases from a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.
- OR -
In the **Remove assignments** pane, remove mail-in databases.
6. Save the changes.

Editing the inclusion list

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

To add additional user accounts to a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Users** tab.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To add additional groups to a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

To add additional servers to a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Server** tab.
5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
6. Save the changes.


To add additional mail-in databases to a dynamic group

1. Select the **IBM Notes | Groups** category.
2. Select the dynamic group in the result list.
3. Select the **Edit additional list** task.
4. Select the **Mail-in DB** tab.
5. In the **Add assignments** pane, assign mail-in databases.
- OR -

- In the **Remove assignments** pane, remove mail-in databases.
6. Save the changes.

Deleting Notes groups


To delete a group

1. Select the **IBM Notes | Groups** category.
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.

Mail-in databases

To edit mail-in database master data

1. Select the **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the mail-in database's master data.
4. Save the changes.

Mail-in DB 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. |

| Property | Description |
|-----------------------|--|
| Encrypt incoming post | Specifies whether incoming emails are encrypted. |
| Notes template | Name of the template to use for creating the mail-in database. |
| Description | Text field for additional explanation. |

Additional tasks for mail-in databases

After you have entered the master data, you can run the following tasks.

Overview of the mail-in DB

To obtain an overview of a mail-in database

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

Assigning Notes groups to a mail-in DB

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 **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign groups. To filter the groups, select a domain in the **Notes Domains** input field.
- OR -
In the **Remove assignments** pane, remove the groups.
5. Save the changes.

Assigning owners to a mail-in DB

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 **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select "Notes user accounts".
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as owner

1. Select the **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Assign owner** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

Assigning administrators to a mail-in DB

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 **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select "Notes user accounts".

5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators

1. Select the **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

Maintaining excluded and additional lists

Mail-in databases can be members of dynamic groups. Use the excluded list to specify which mail-in databases you want to exclude from membership in a dynamic group. Use the additional list to specify which mail-in databases you want to additionally include in membership in a dynamic group.

To add a mail-in database to a dynamic group's additional list

1. Select the **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Additional** tab.
5. In the **Add assignments** pane, assign dynamic groups whose membership list you want to add to the mail-in database.
- OR -
In the **Remove assignments** pane, remove the dynamic groups.
6. Save the changes.

To add a mail-in database to a dynamic group's excluded list

1. Select the **IBM Notes | Mail-In DB** category.
2. Select a mail-in database in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Excluded** tab.

5. In the **Add assignments** pane, assign the dynamic groups from whose membership list you want to exclude the mail-in database.
 - OR -In the **Remove assignments** pane, remove the dynamic groups.
6. Save the changes.

Related topics

- [Memberships in dynamic groups](#) on page 153

Notes server

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

To edit the master data of a Notes server

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list. Select the **Change master data** task.
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 | Effect when set |
|---|---|
| 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 | Notes domain to which the server belongs. |

| Property | Description |
|-----------------------------------|---|
| domain | |
| 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 "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 data is only required if the Has Notes mailbox files option is enabled. |
| Server document | Specifies whether the Notes server only corresponds to a server document in the Domino directory and does not exist physically. |
| Cluster name | Name of the cluster if the server belongs to a cluster. |
| DNS server name | Full name of the server. |
| Load internet configuration | Specifies whether the internet protocol configuration is loaded from the internet site documents in the Domino directory. If this option is not set, the information is taken from the server document. |
| Starts SMTP service automatically | Specifies whether the SMTP service is started automatically when the server is started. |
| Operating system | Name of the operating system installed. |
| Formula 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 | Telephone number in case the server can take calls over a modem. |

| Property | Description |
|---------------------------------|---|
| 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 | Text field for additional explanation. |
| Detailed description | Text field for additional explanation. |

Notes server security settings

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 run the following tasks.

The Notes server overview

To obtain an overview of a Notes server

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

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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.
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). The task is only available if the **Has Notes mailbox files** option is enabled.

To assign Notes servers directly to user accounts

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

3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
5. Save the changes.

Assigning owners to the server document

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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign document owner** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as owners of a server document

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign document owner** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove the groups.
6. Save the changes.

Assigning administrators to the server document

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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign document administrators** task.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators for a server document

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign document administrators** task.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.
6. Save the changes.

Specifying administrator access

In IBM Notes, you can limit administrator's access permissions, whereby you issue permissions 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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign full access administrators** task.
4. In the **Table** input field, select the "Notes user accounts" table.

5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as full access administrators

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign full access administrators** task.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign administrators** task.
4. In the **Table** input field, select the "Notes groups" table.

5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Assign database administrators](#) on page 170
- [Assigning administrators with full remote console access](#) on page 171

Assign database administrators

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

To specify user accounts as database administrators

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select **Assign database administrators**.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as database administrators

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select **Assign database administrators**.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select **Assign full remote console administrators**.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as remote console administrators

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select **Assign full remote console administrators**.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Assign view-only administrators](#) on page 171

Assign view-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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.

3. Select the **Assign view only administrators** task.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators with read access

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign view only administrators** task.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.
6. Save the changes.

Assign 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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select **Assign system administrators**.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as system administrators

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select **Assign system administrators**.
4. In the **Table** input field, select the "Notes groups" table.

5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Assign restricted system administrators](#) on page 173

Assign restricted system administrators

Assign 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 **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign restricted system administrators** task.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To specify groups as administrators with restrictions

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Assign restricted system administrators** task.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Assign system administrators](#) on page 172

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.

Access servers

By default, all user accounts, groups, and servers can access the server. To limit server access, you can explicitly assign user accounts, groups, and servers that may access the server. After you have assigned the objects, server access is denied for all other user accounts, groups, and servers.

To only deny server access for individual user accounts, groups, and servers, use the **Not access server** task. For more information, see [No access servers](#) on page 175.

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 the **Access server** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
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 the **Access server** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
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 the **Access server** task.

4. In the **Table** field, select the "Notes server" table.
5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
6. Save the changes.

No access servers

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 [Access servers](#) on page 174.

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**.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
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 the **Deny server access** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
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 the **Deny server access** task.
4. In the **Table** field, select the "Notes server" table.

5. In the **Add assignments** pane, assign servers.
 - OR -In the **Remove assignments** pane, remove servers.
6. Save the changes.

Creating databases & 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 the **Create databases & templates** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -In the **Remove assignments** pane, remove user accounts.
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 the **Create databases & templates** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
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 the **Create databases & templates** task.
4. In the **Table** field, select the "Notes server" table.

5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
6. Save the changes.

Creating new replicas

The given user accounts, groups, and servers can create new replicas on the server. If no user accounts, groups, and servers are assigned, everyone is allowed to create new replicas.

To allow user accounts to create replicas

1. Select the category **IBM Notes | Notes server**.
2. Select the server in the result list.
3. Select the **Create new replicas** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
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 the **Create new replicas** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
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 the **Create new replicas** task.
4. In the **Table** field, select the "Notes server" table.

5. In the **Add assignments** pane, assign servers.
 - OR -
- In the **Remove assignments** pane, remove servers.
6. Save the changes.

Pass-through route

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 [Pass-through destinations for routing](#) on page 179.

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 the **Route through Server** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
- In the **Remove assignments** pane, remove user accounts.
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 the **Route through Server** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
- In the **Remove assignments** pane, remove groups.
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 the **Route through Server** task.
4. In the **Table** field, select the "Notes server" table.

5. In the **Add assignments** pane, assign servers.
 - OR -In the **Remove assignments** pane, remove servers.
6. Save the changes.

Pass-through 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 the **Access this server** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -In the **Remove assignments** pane, remove user accounts.
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 the **Access this server** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -In the **Remove assignments** pane, remove groups.
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 the **Access this server** task.
4. In the **Table** field, select the "Notes server" table.

5. In the **Add assignments** pane, assign servers.
- OR -
In the **Remove assignments** pane, remove servers.
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 [Pass-through destinations for routing](#) on page 179. Furthermore, the user accounts, groups, or servers these servers can use must be defined. For more information, see [Pass-through route](#) on page 178.

To allow user accounts to use the pass-through server for placing calls

1. Select the category **IBM Notes | Notes server**.
2. Select the server in the result list.
3. Select the **Cause calling** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
- OR -
In the **Remove assignments** pane, remove user accounts.
6. Save the changes.

To allow groups to use the pass-through server for placing calls

1. Select the category **IBM Notes | Notes server**.
2. Select the server in the result list.
3. Select the **Cause calling** task.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
- OR -
In the **Remove assignments** pane, remove groups.
6. Save the changes.

To allow servers to use the pass-through server for placing calls

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

3. Select the **Cause calling** task.
4. In the **Table** field, select the "Notes server" table.
5. In the **Add assignments** pane, assign servers.
 - OR -
 - In the **Remove assignments** pane, remove servers.
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 [Pass-through destinations for routing](#) on page 179. Furthermore, the user accounts, groups, or servers these servers can use must be defined. For more information, see [Pass-through route](#) on page 178.

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 the **Destinations allowed** task.
4. In the **Table** input field, select the "Notes server" table.
5. In the **Add assignments** pane, assign target servers.
 - OR -
 - In the **Remove assignments** pane, remove the servers.
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 the **Run or sign unrestricted methods and operations** task.
4. In the **Table** field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
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**.
4. In the **Table** field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Running restricted LotusScript/Java agents on page 182](#)
- [Running simple agents and formula agents on page 183](#)

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**.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
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**.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.
6. Save the changes.

Related topics

- [Signing or running unrestricted methods and operations](#) on page 181

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 the **Run simple and formula agents** task.
4. In the **Table** input field, select the "Notes user accounts" table.
5. In the **Add assignments** pane, assign user accounts.
 - OR -
 - In the **Remove assignments** pane, remove user accounts.
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 the **Run simple and formula agents** task.
4. In the **Table** input field, select the "Notes groups" table.
5. In the **Add assignments** pane, assign groups.
 - OR -
 - In the **Remove assignments** pane, remove groups.

6. Save the changes.

Related topics

- [Signing or running unrestricted methods and operations](#) on page 181

Maintaining excluded and additional lists

Notes servers can be members of dynamic groups. Use the excluded list to specify which servers you want to exclude from membership in a dynamic group. Use the additional list to specify which servers you want to additionally include in membership in a dynamic group.

To add a Notes server to a dynamic group's additional list

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Additional** tab.
5. In the **Add assignments** pane, assign the dynamic groups to whose membership list you want to add the server.
 - OR -
 - In the **Remove assignments** pane, remove dynamic groups.
6. Save the changes.

To add a Notes server to a dynamic group's exclusion list

1. Select the **IBM Notes | Notes Server** category.
2. Select the server in the result list.
3. Select the **Maintain excluded and additional** task.
4. Select the **Excluded** tab.
5. In the **Add assignments** pane, assign the dynamic groups from whose membership list you want to exclude the server.
 - OR -
 - In the **Remove assignments** pane, remove dynamic groups.
6. Save the changes.

Related topics

- [Memberships in dynamic groups](#) on page 153

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

To confirm pending AdminP requests regularly

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

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

Confirmation of the following requests has currently been implemented:

- Approve MailfileDeletion
- Approve MovedReplicaDeletion
- Approve ReplicaDeletion

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

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

To display the master data of an response document

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

| Property | Description |
|------------------|---|
| request document | Unique ID for the associated request document |
| Object | Name of the object that was processed. |
| Author | Name of the AdminP request author. |
| Executing server | Server that 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. |

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 that 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 that 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 provisioned by 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 My One Identity Manager Target system overviews |

| Report | Description |
|--|---|
| | category. |
| 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 My One Identity Manager Data quality analysis category. |


Overview of all assignments


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


Examples

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

To display detailed information about assignments

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

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

- Double-click a control to show all child roles belonging to the selected role.
- By clicking the  button in a role's control, you display all employees in the role with the base object.






- Use the small arrow next to  to start a wizard that allows you to bookmark this list of employees for tracking. This creates a new business role to which the employees are assigned.

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



Table 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. |
|  | Displays all roles or only the affected roles. |

Configuration parameters for synchronizing 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 this parameter require the database to be recompiled. |
| TargetSystem NDO Accounts | Parameter for configuring Notes user account data. |
| TargetSystem NDO Accounts InitialRandomPassword | This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy. |
| TargetSystem NDO Accounts InitialRandomPassword SendTo | 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 provide users with the login data for their user accounts. The Employee - new user account created mail template is used. |
| TargetSystem NDO Accounts InitialRan- | This configuration parameter contains the name of the mail template sent to provide users with information about |

| Configuration parameter | Meaning if Set |
|---|--|
| domPassword SendTo MailTemplatePassword | their initial password. The Employee - initial password for new user account mail template is used. |
| 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. The Employee - new user account with default properties created mail template is used. |
| 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. |
| TargetSystem NDO CreateMailDB | <p>This configuration parameter specifies whether the mailbox file is created after or during registration of the Notes user in 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.</p> <p>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 "TargetSystem NDO DefTemplatePath".</p> |
| 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. |

| Configuration parameter | Meaning if Set |
|---|---|
| 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. |
| 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 PersonAutoDisabledAccounts | This configuration parameters specifies whether employees are automatically assigned to locked user accounts. User accounts do not obtain an account definition. |
| TargetSystem NDO PersonAutoFullsync | 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 are listed in a pipe () delimited list that is handled as a regular search pattern. |
| 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 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 that 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. |

Default project template for IBM Notes

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows, and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

The 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 |

| Schema type in IBM Notes | Table in the One Identity Manager Schema |
|--------------------------|--|
| PolicySecurity | NDOPolicySetting |
| PolicySetup | NDOPolicySetting |
| Server | NDOServer |
| Template | NDOTemplate |

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

A

- Access Server 174
- account definition
 - add to IT Shop 55
 - assign to system roles 55
- achive database
 - add 22
- additional list 153
 - edit 155, 161, 184
- administrator
 - certificate 87
 - for documents 147
 - group 147, 150
 - mail-in database 160
 - policies 92
 - user account 116
- adminP task 185
 - confirm automatically 185
 - grant approval 186
- application role 11
 - target system managers 77
- architecture 9

C

- CA process 84
- calculation schedule
 - disable 40
- certificate 84
 - add 18
 - administrator 87
 - CA database 84

- expiry date 84
- ID file 84, 88
- overview form 86
- owner 86
- specify administrator 147
- specify owner 146
- certificate type 84
- certifier
 - contact data 85
- compliance check 153
- create INI file 19

D

- direction of synchronization
 - direction target system 23, 31
 - in direction of 23
- domain 80
 - account definition 80
 - category 144
 - employee assignment 120
 - mail-in database, assign 80
 - report 188
 - specify category 82
 - target system manager 11
 - target system managers 80
 - use ID vault 80, 125
 - user account, assign 80
- Domino directory
 - filter 16
 - full text index 16

Domino server

settings 16

dynamic group 152

E

email notification 71

employee

disable 127

employee assignment

manual 121

remove 121

search criteria 120

excluded list 153

edit 154, 161, 184

exclusion definition 142

explicit policy 90

extended group 153

extended property

group 150

user account 118

G

gateway server 16, 72

configure 16

create archive database 22

install 16

install One Identity Manager
Service 19

server function 75

group 131

about IT Shop requests 131

add to IT Shop 138

administrable document 147

administrators 150

assign business roles 135

assign category 131

assign cost center 134

assign department 134

assign extended properties 150

assign hierarchical role 133

assign location 134

assign mail-in database 140

assign server 140, 154

assign system role 137

assign user account 133, 136

category 144

delete 157

dynamic group 131, 153

calculate members 153

edit additional list 153

edit exclusion list 153

number of members 153

edit additional list 155

edit exclusion list 154

effective 142

exclusion 142

extended group 153

group membership 136, 141

inheriting through categories 82

inheriting through system roles 137

locked group 127, 131, 151

number of members 151

overview form 139

own document 146

owner 149

risk index 131

specify administrator 147

specify owner 146

I

- ID file
 - expiry date 108
 - extend 108
 - restore 125
 - save 124
- ID restore 126
- ID vault 125
- ID vault server 125, 163
- inheritance
 - category 144
- IT operating data 48
 - change 51
 - default value 48
 - log 49
- IT Shop shelf
 - assign account definition 55
 - assign group 138

J

- Java Agent 182
- Job server
 - load balancing 38
 - properties 73

L

- load balancing 38
- locked group 151
- login data 71
- LotusScript Agent 182

M

- mail-in database 158
 - additional list 161
 - administrator 160
 - assign group 159
 - domain 158
 - dynamic group 161
 - excluded list 161
 - owner 160
 - server 158
 - specify administrator 147
 - specify owner 146
 - template 158
- mailbox file 104
 - create 123
 - limit size 107
 - logical size 107
 - physical size 107
- membership
 - modify provisioning 37

N

- Notes.INI 19
- notification 71

O

- object
 - delete immediately 35
 - outstanding 35
 - publish 35
- outstanding object 35
- owner
 - certificate 86

- for documents 146
- group 146, 149
- mail-in database 160
- policies 92
- user account 112, 114

P

- password
 - initial 70-71
- password policy 59
 - assign 61
 - character sets 65
 - check password 69
 - conversion script 66-67
 - default policy 61, 63
 - display name 63
 - edit 63
 - error message 63
 - excluded list 69
 - failed logins 64
 - generate password 69
 - initial password 64
 - name components 64
 - password age 64
 - password cycle 64
 - password length 64
 - password strength 64
 - predefined 60
 - test script 66
- policies setting 93
- policy 90
 - administrators 92
 - assign group 91
 - assign user accounts 91
 - owner 92

- project template 194
- provisioning
 - members list 37

R

- report
 - overview of all assignments 189
- request document 186
- response document 186
- revision filter 34

S

- schema
 - changes 33
 - shrink 33
 - update 33
- server 163
 - access guarantee 174
 - access restriction 174-175
 - additional list 184
 - administration read permissions 171
 - administrator 168, 170-173
 - administrator access 168
 - administrators 167, 169
 - assign group 166
 - assign user account 166
 - contact 164
 - create database 176
 - create template 176
 - database administrator 170
 - deny access 175
 - destination server 181
 - dial-up 180
 - dynamic group 184

- excluded list 184
- full access administrator 168
- ID vault server 163
- location 164
- mail server 164, 166
- not access server 127, 151
- overview form 166
- owner 167
- pass-through destination 179, 181
- pass-through server 164, 178, 180-181
- remote console administrator 171
- replication 177
- routing 178
- run agents 181-183
- security 165
- set up 163
- specify administrator 147
- specify owner 146
- system administrator 172-173
- server document
 - administrator 167
 - owner 167
 - specify administrator 147
- server function 75
- server permissions 174
- single object synchronization
 - accelerate 38
- synchronization
 - accelerate 34
 - authorizations 15
 - base object
 - create 32
 - configuration parameter 191
 - configure 23, 30
 - connection parameter 23, 30, 32
 - different domains 32
 - only changes 34
 - prevent 40
 - scope 30
 - sequence 9
 - set up 14
 - start 23
 - synchronization project
 - create 23
 - user 15
 - variable 30
 - variable set 32
 - workflow 23, 31
 - synchronization analysis report 39
 - synchronization configuration
 - customize 30-32
 - synchronization log 29
 - synchronization project
 - create 23
 - disable 40
 - edit 82
 - project template 194
 - synchronization server 16
 - server function 75
 - synchronization workflow
 - create 23, 31

T

- target system manager 77
- target system synchronization 35
- template 89
 - IT operating data, modify 51

U

user account 95

- address data 107
- administrable document 114
- administrative user account 96
- administrators 116
- apply template 51
- assign category 101
- assign employee 95, 118
- assign extended properties 118
- assign group 111
- assigned groups 188
- category 144
- certificate 101
- configuration profile 108
- default user accounts 96
- deferred deletion 129
- delete 129
- disable employee 127
- edit additional list 117
- edit exclusion list 117
- email system 104
- full name 101
- ID file
 - restore 126
- ID vault 125
 - permissions 125
 - viAgentsDB.nsf 125
- identity 96, 101
- license type 108
- lock 101, 127, 129
- mailbox file 104
 - limit size 107
 - logical size 107

- physical size 107
- make anonymous 127
- manage level 111
- overview 111
- own document 112
- owner 114
- password 70, 108
 - notification 71
- password policies 108
- privileged user account 96, 101
- provision 88
- recertification 17, 88
- reset password 125
- restore 129
- risk index 101
- same time server 107
- set up 100
- short name 101
- specify administrator 147
- specify owner 146
- type 96
- unlock 127
- unused 188
- user ID file
 - expiry date 108
 - extend 108
 - restore 125
 - save 124