

1.1. Learning environment setup

Normally, according to HCL specifications, a Domino Server is to be installed on a Windows Server (or one of the other possible server operating systems - e.g. Linux).

Since we are only implementing a learning environment, Windows 10/11 Pro is also very suitable. Equipped with a reasonably up-to-date CPU and with 3-4 GByte RAM, all shown functions will run smoothly.

If you also want to install a learning environment at your end, you will need the following:

- **Windows 10/11 Pro**
(these do not have to be physical PCs - a virtual machine is also suitable)

One Domino Server + Domino Administrator can be installed on one Windows instance at the same time - if there are to be multiple Domino Servers, the rule is:

- 1 x Windows 10/11 Pro for each Domino Server

- **Notes Client (inkl. Administrator) and Domino Server Version 9.0.1.x bis 12.0.1**

Before someone asks: Notes and Domino are commercial products of the company HCL and cannot be downloaded »just like that« somewhere.

However, since you are probably dealing with Domino Administration as an employee of a company (Notes/Domino is hardly used by private persons), the software should be available in your company.

Hint

To be able to try out functions such as those described in the chapters [2. Working with multiple Domains](#) on page 11 or [7. Domino Cluster](#) on page 179, at least two Domino Servers are required.

Language of the operating system and Notes/Domino software

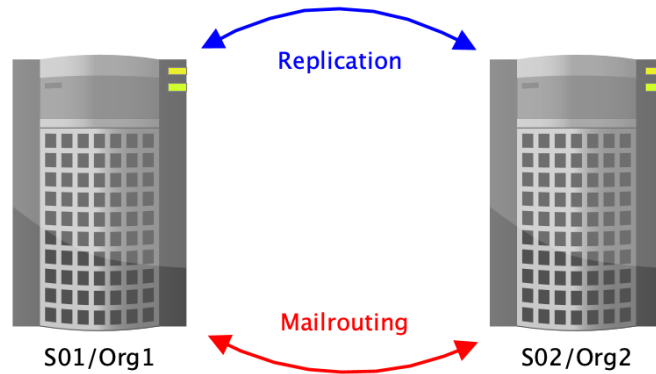
Also in the German edition of this book, both the Windows operating system and the Notes/Domino software are used in **English**. This is primarily for the following reasons:

- Many administrators now prefer the English language for software. A search for possible solutions to problems in English is much more successful.
- When creating the book, I don't have to take all the screenshots multiple times.

2. Working with multiple Domains

2.2. Communication between foreign Domains

This chapter shows how to connect Domino Servers from different domains/organizations. Since we are talking about Domino Servers, we are discussing replication and mail routing (NRPC mail routing, not SMTP).



Communication between Domino Servers from different domains/organizations is basically not different from the communication that takes place between Domino Servers from the same domain/organization.

Only the authentication, i.e. the »handshake« when the Domino Servers connect, will not work »just like that«, because the server IDs involved come from different organizations (i.e. are »descendants« of different cert.id's).

We remember:

When setting up the first Domino Server, a certificate (you could call it the root certificate of the Notes/Domino environment) is created, which is stored in the cert.id file and is included in the ID files of servers or users when they are registered.

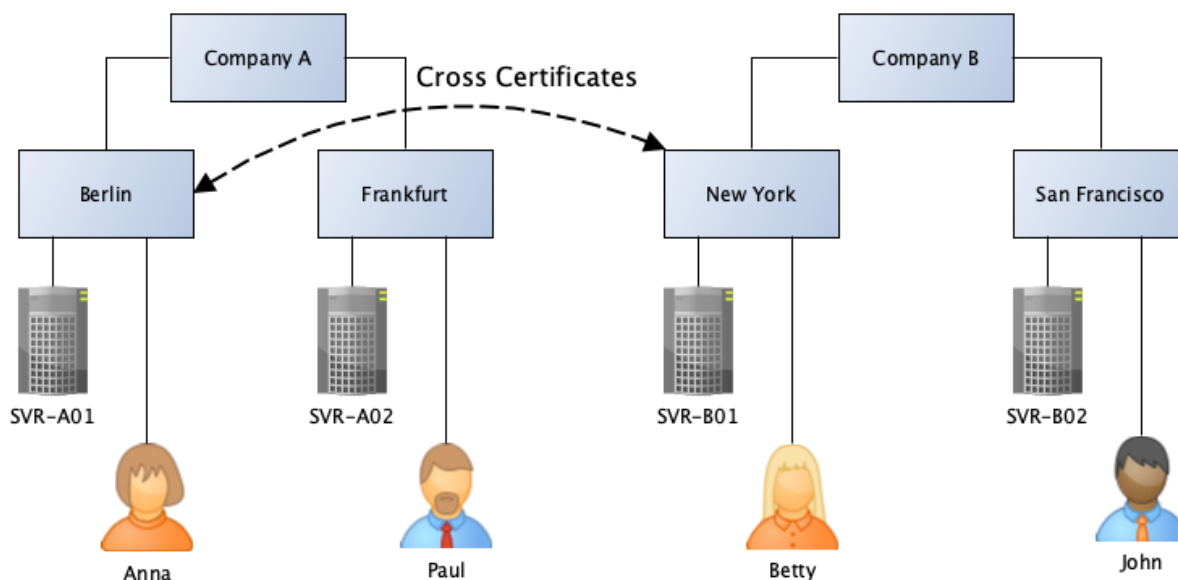
If a connection attempt is now made between two Domino Servers, each of the Domino Servers involved checks whether the other side also has this certificate. If this is the case, the subsequent communication will take place without any problems. Otherwise, error messages will appear on the Domino console (or in the »log.nsf«) and access will be denied.

Domino Server and Notes Clients only communicate with each other if the server or user IDs used carry the same root certificates, i.e. originate from the same cert.id file (or a unit ID created with it).

To enable communication between »foreign« Domino Servers and/or Notes Clients, so-called Cross Certificates have to be created on both systems involved.

This can be done at different levels (organization, unit, server or person ID). The details of this will be presented in the next chapter.

2.3.2. Cross certificates at the unit level (OU)



Here, cross certification takes place at the **organizational unit** level.

By creating the Cross Certificates at the unit level, significantly fewer Domino Server or Notes users are already able to access Domino Servers on the remote side.

At the Berlin location, only Anna and the server SVR-A01 are granted access to the Domino Server SVR-B01 at the New York location. Betty and the Domino Server SVR-B01 at the New York location are granted access to the Domino Server SVR-A01 in Berlin.

The number of communication partners is thus considerably reduced compared to cross certification at the organizational level. Nevertheless, the responsible administrator must at least reckon with accesses from strangers - their number cannot be readily estimated and thus not the resources used on the company's own Domino Servers.

Likewise, the ACLs of all applications must be carefully maintained so that the employees of the foreign company cannot access information not intended for them in an uncontrolled manner.

Conclusion

Although cross certification at the unit level, as opposed to the organization level, reduces the number of possible communication partners, the fundamental question is whether employees with their Notes Client have access to the other side at all?

The Domino Servers exchange all the necessary information via replication and mail routing, so individual access for individual employees is usually not required at all.

2.4. Setup of the cross certification

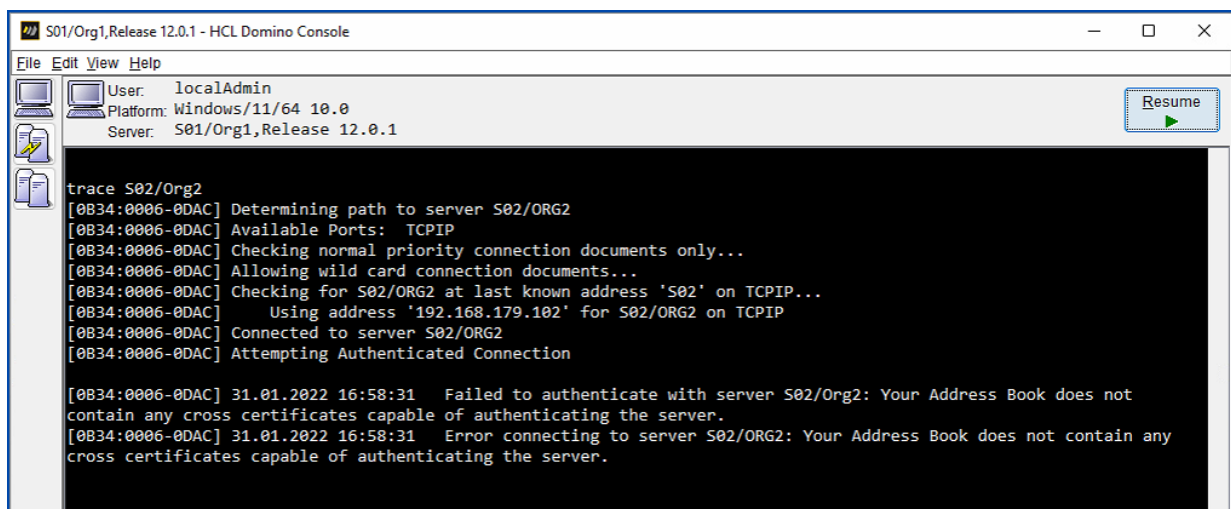
This chapter shows how to create a Cross Certificate quickly and conveniently.

Hint

In addition to the variant shown here for creating the Cross Certificates, this can also be done by exchanging ID files (possibly via mail routing). These variants are more complicated and time-consuming. For this reason, they are not presented in the book.

Subsequently, a Cross Certificate is created at the level of Server IDs.

2.4.1. Connection between Domino Servers without cross certificate



```
S01/Org1,Release 12.0.1 - HCL Domino Console
File Edit View Help
User: localAdmin
Platform: Windows/11/64 10.0
Server: S01/Org1,Release 12.0.1
Resume

trace S02/Org2
[0B34:0006-0DAC] Determining path to server S02/ORG2
[0B34:0006-0DAC] Available Ports: TCPIP
[0B34:0006-0DAC] Checking normal priority connection documents only...
[0B34:0006-0DAC] Allowing wild card connection documents...
[0B34:0006-0DAC] Checking for S02/ORG2 at last known address 'S02' on TCPIP...
[0B34:0006-0DAC] Using address '192.168.179.102' for S02/ORG2 on TCPIP
[0B34:0006-0DAC] Connected to server S02/ORG2
[0B34:0006-0DAC] Attempting Authenticated Connection

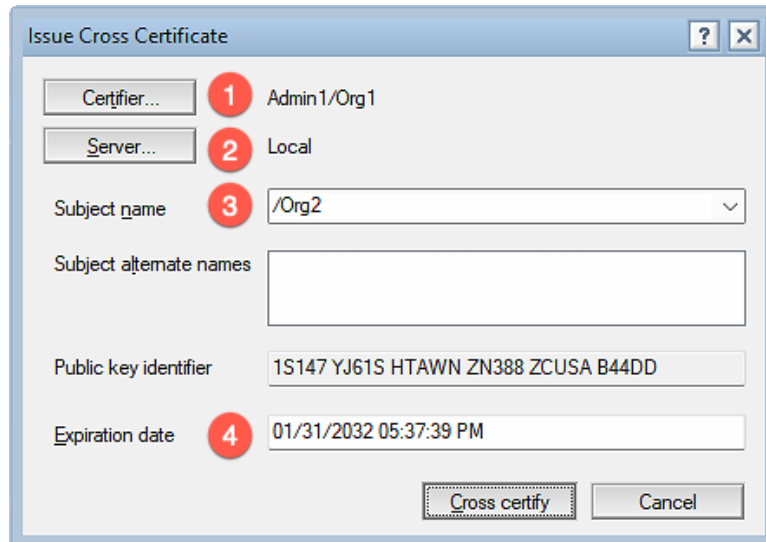
[0B34:0006-0DAC] 31.01.2022 16:58:31 Failed to authenticate with server S02/Org2: Your Address Book does not
contain any cross certificates capable of authenticating the server.
[0B34:0006-0DAC] 31.01.2022 16:58:31 Error connecting to server S02/ORG2: Your Address Book does not contain any
cross certificates capable of authenticating the server.
```

Communication between Domino Servers from different organizations is basically not possible. If you try to establish a connection with the console command »trace« (assuming accessibility via the network), the error messages shown in the screenshot appear.

Message at the Domino Console	Explanation
Attempting Authenticated Connection	An attempt is made to establish a connection, during which the two partners check each other (authentication).
Failed to authenticate with server S02/Org2: Your Address Book does not contain any cross certificates capable of authenticating the server.	Authentication fails because there is no Cross Certificate in the Directory (»names.nsf«) to confirm the foreign Domino Server.
Error connecting to server S02/Org2: Your Address Book does not contain any cross certificates capable of authenticating the server.	No connection can be established because there is no Cross Certificate in the directory (»names.nsf«) to confirm the foreign Domino Server.

This Cross Certificate would confirm that the currently used user ID trusts the »Org2« organization (the Notes Client accepts connections to the »Org2« organization).

Such a Cross Certificate stored locally on the Notes Client is useless for Domino Server communication. Therefore, click on the »Advanced« button.



These are the defaults in this dialog. Do **not** click the »Cross certify« button here immediately! These defaults are **not** suitable for creating the Cross Certificate for the Domino Servers.

1. Use the »Certifier...« button to select who from your Domino environment trusts the remote site. This should be the server ID of your own Domino Server.
2. Where should the Cross Certificate be stored? Locally in the »names.nsf« of the Notes Client (not useful) or in the »names.nsf« on your own server? Select one of your Domino Servers by the button »Server...«.
3. At which level do you trust the other side? Pre-selected is the organization level, but you can explicitly specify the Domino Server of the other side by clicking the selection arrow on the right.



4. How long should the Cross Certificate be valid? A validity period of 10 years is preset. Since you can later terminate the connection to the other side at any time by deleting the Cross Certificate, longer durations can be specified here without any problems.

Conclusion

As a result of the previously performed steps, a new cross certificate is stored in the Domino Directory ("names.nsf") on the specified own Domino Server.

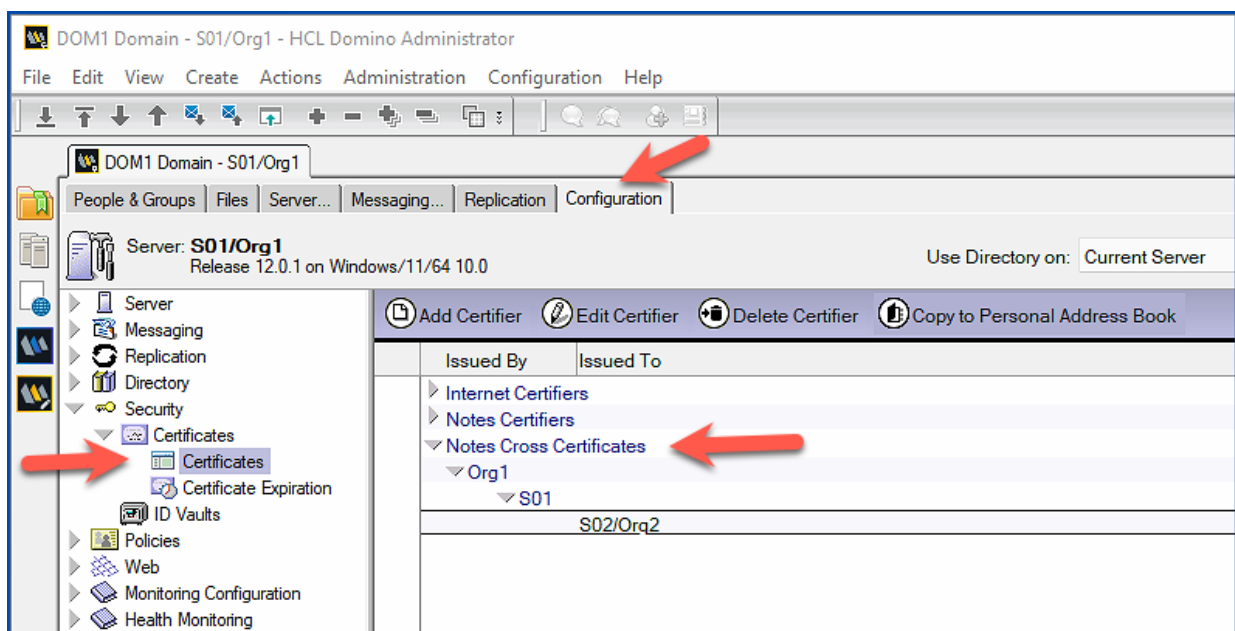
2.4.3. Cross certificate in the Domino Directory

In Domino Administrator, open the Configuration tab and select the »Security« → »Certificates« → »Certificates« view in the navigation on the left.

Hint

You can also find the »Certificates« view on the »People & Groups« tab.

Expand the »Notes Cross Certificates« category.



The Domino Server »S01/Org1« from the organization »Org1« trusts the Domino Server »S02/Org2« from the organization »Org2«. This is shown in the two columns »Issued By« and »Issued To«.

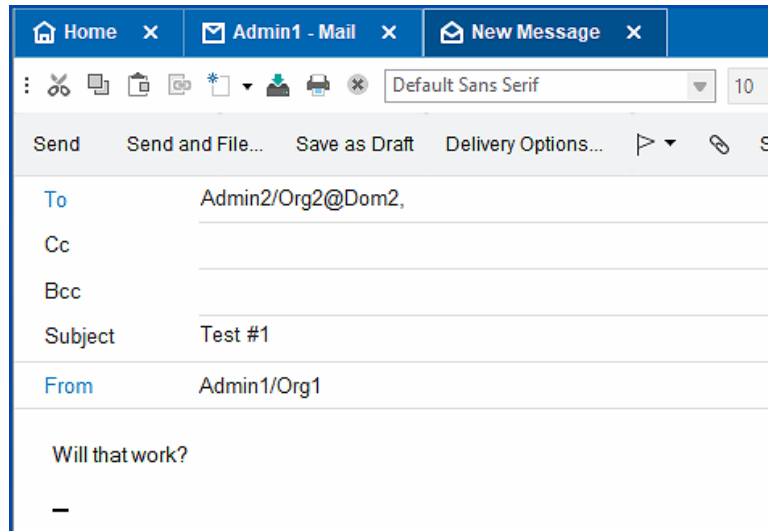
This completes all the required steps in the »Org1« organization.

Hint

Cross Certificates only work if they exist in both Notes/Domino environments. Consequently, the responsible administrator on the remote side must also perform these steps.

2.5. Mail routing between foreign domains

Once Domino Servers from different domains/organizations communicate based on the Cross Certificates , NRPC mail routing will still not work.

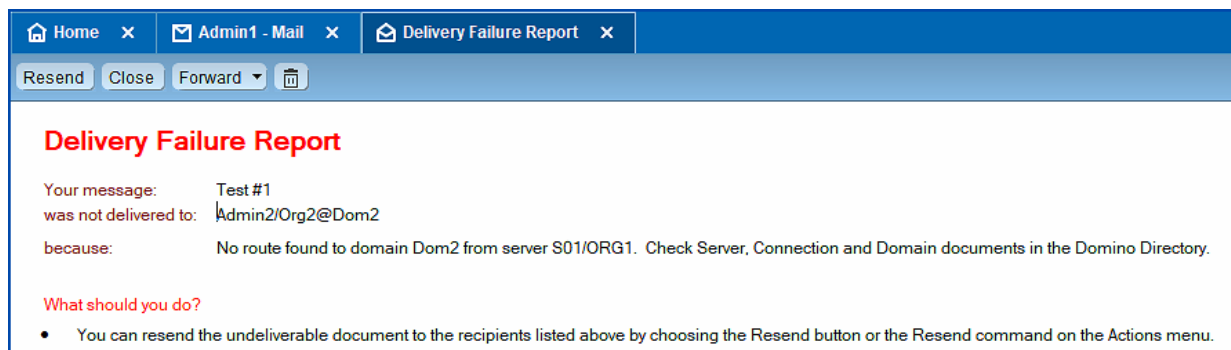


A mail is sent from »Admin1/Org1@Dom1« to the person »Admin2/Org2@Dom2«.

Hint

The recipient **cannot** be selected by the link »To« from the own Domino Directory - there is no person document for this person.

In the chapter [2.8. Activation of foreign Directories](#) on page 35 you will learn how to integrate foreign directories into your own Domino environment for convenient selection of recipients.



The sender receives this »Delivery Failure Report« - the mail cannot be delivered.

The note »Check Server, Connection and Domain documents in the Domino Directory« is correct - the required connection documents are missing at the moment.

Server Connection: S01/Org1 to S02/Org2

Basics | Replication/Routing | Schedule | Comments | Administration

Scheduled Connection

Schedule: Enabled

Connect at times: 12:00 AM - 11:59 PM each day

Repeat interval of: 5 minutes

Days of week: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Mail routing should be enabled around the clock.

Save the new connection document. After the server accepts the settings (see chapter 9.9. [Why are changes not applied immediately?](#) on page 220), mails are routed to the foreign domain.

At the Domino console, you can use the »show schedule« command to check whether the Domino Server is using the settings from the connection document.

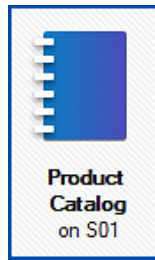
```
sh sch
[235C:0006-12B4] Scheduled   Type   Next schedule
[235C:0006-12B4] S02/Org2           Mail Routing           02.02.2022 14:05:00
```

2.5.2. Functional test through mails

Send another mail to a recipient in the foreign Notes/Domino domain.

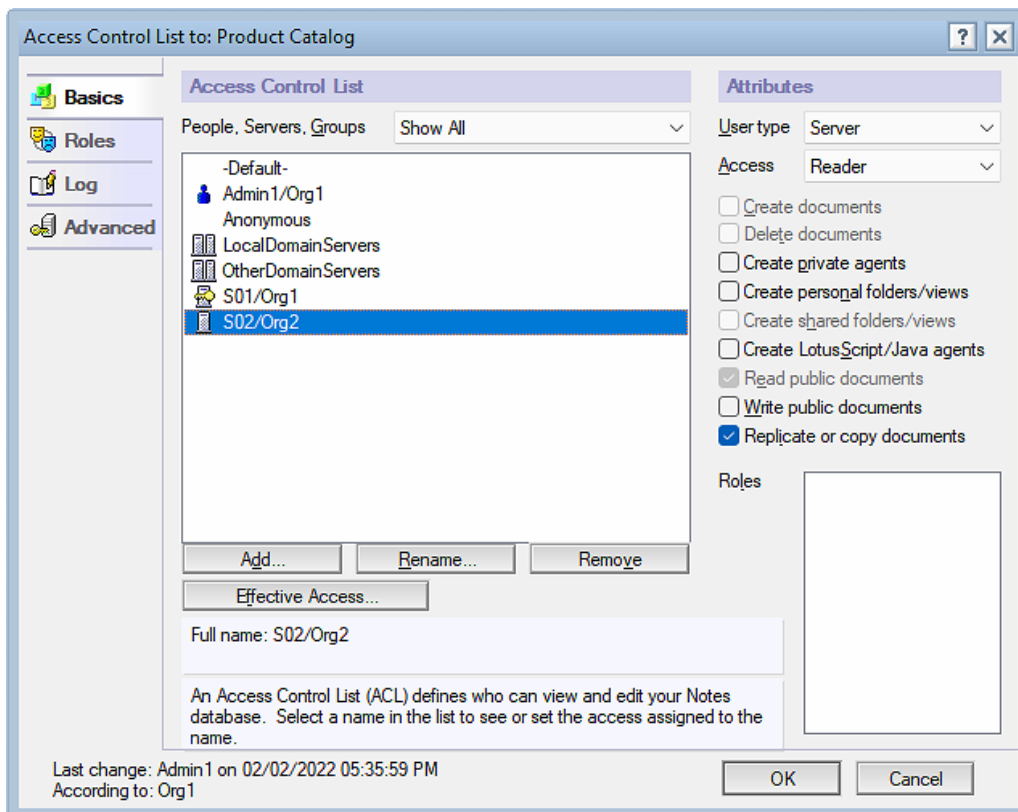
If all settings in the connection document are correct and the Domino Server has accepted them, the mail will be delivered without any problems.

```
[2110:000C-0E6C] 02.02.2022 14:19:19 Router: Transferring mail to S02/ORG2 via Notes
[2110:000C-0E6C] 02.02.2022 14:19:19 Router: Transferred 1 messages to S02/ORG2 via Notes
[2110:0006-1F2C] 02.02.2022 14:19:20 Router: Message 00287519 transferred to S02/ORG2 for Admin2/Org2@Dom2 via Notes
```



We have a (fictitious) product catalog, which we would like to replicate with a partner company.

Example 1: Sharing information



The foreign Domino Server »S02/Org2« receives the ACL level »Reader«. This allows the remote Domino Server to replicate all information from our application to itself, but not to pass any new documents, changes or deletions to our application.

Hint

Alternatively to the server name »S02/Org2« you could use the predefined group »OtherDomainServers« (»S02/Org2« must then be a member of this group).

I personally prefer entries with the server name. This way you can see at a glance which foreign Domino Servers access with which level - but this is surely a matter of taste.

On the »Basics« tab, the source and target servers and the source and target domains are named.

Tab Replication/Routing

Mail routing is disabled on the »Replication/Routing« tab.

Important

Be sure to specify the relevant applications in the »Files/Directory paths to replicate« field! If you leave the field empty, all applications and templates will be replicated. HCL delivers the templates worldwide with the same replica IDs. If modified templates exist on the foreign Domino Server, these changes could be reflected in your templates. Do not rely on the fact that the ACLs of the templates are set so that this does not happen!

Tab Schedule

```
[0A90:0002-0FE0] 02.02.2022 19:26:38 Starting replication with server S02/Org2
[0A90:0002-0FE0] 02.02.2022 19:26:38 Access control is set in S02/Org2 ProductCatalog.nsf to not replicate forms or
views from ProductCatalog.nsf
[0A90:0002-0FE0] 02.02.2022 19:26:38 Replicator added 1 document(s) to ProductCatalog.nsf from S02/Org2
ProductCatalog.nsf
[0A90:0002-0FE0] 02.02.2022 19:26:38 Finished replication with server S02/Org2
```

Replication can be performed successfully.

2.7.2. Domain document for adjacent domains

Tab **Basics**

Domain Dom2

Basics | Restrictions | Calendar Information | Comments | Administration

Basics

Domain type: 1

Adjacent domain name: 2

Domain description: 3

The following settings are defined on the »Basics« tab.

1. In the »Domain type« field, select the Adjacent Domain option.
2. In the »Adjacent domain name« field, enter the name of the adjacent domain.
3. The specification in the »Domain description« field is optional and describes the neighboring domain in general.

Tab **Restrictions**

Domain Dom2

Basics | Restrictions | Calendar Information | Comments | Administration

Restrictions

Allow mail only from domains: 1

Deny mail from domains: 2

The fields on the Restrictions tab control who is allowed to send mails to the neighboring domain (in our example »Dom2«).

Hint

We will discuss the details in more detail in the following chapter, but basically mail can be routed through a neighboring domain to another, non-neighboring domain. In order for the domain »in the middle« to allow or disallow this, there are these two fields.

1. In the »Allow mail only from domains« field, you specify which other domains are allowed to route messages through their own domain to the domain named on the »Basics« tab. The domains entered here are granted permission to do so. If the field remains empty, there is no restriction.
2. The »Deny mail from domains« field controls which other domains are not allowed to send messages to the domain specified on the »Basics« tab. If the field is left empty, there is no restriction.

The mail address of a mail sent from a sender in domain »Dom1« to a recipient in domain »Dom3« must be structured in the following form:

Admin3/Org3@Dom3@**Dom2**

Such a Notes mail address looks unusual. But it works anyway, because the router of a Domino Server evaluates the mail address starting from the right.

The router on the Domino Server of domain »Dom1« sees that the mail should be sent to »Dom2« first. Since connection documents exist between domain »Dom1« and »Dom2«, the mail is successfully routed to domain »Dom2«.

The Domino Server in domain »Dom2« receives the mail and looks at the mail address minus the last domain (@Dom2) and tries to route the mail to the recipient »Admin3/Org3@Dom3«. Since suitable connection documents also exist between domain »Dom2« and »Dom3«, the message is forwarded to the destination domain.

Addressing mails with the specification of multiple Domino domains is not reasonable for users, therefore non-adjacent domain documents are used, which allow addressing mails with only one domain.

Hint

In the following example, we assume that we are creating a domain document in the domain »Dom1«.

2.7.4. Domain document for non adjacent domains

Tab **Basics**

Domain Dom3	
Basics	Restrictions Calendar Information Comments Administration
Basics	
Domain type:	<input type="text" value="Non-adjacent Domain"/> 1
Mail sent to domain:	<input type="text" value="Dom3"/> 2
Route through domain:	<input type="text" value="Dom2"/> 3
Domain description:	<input type="text" value="Another Customer"/> 4

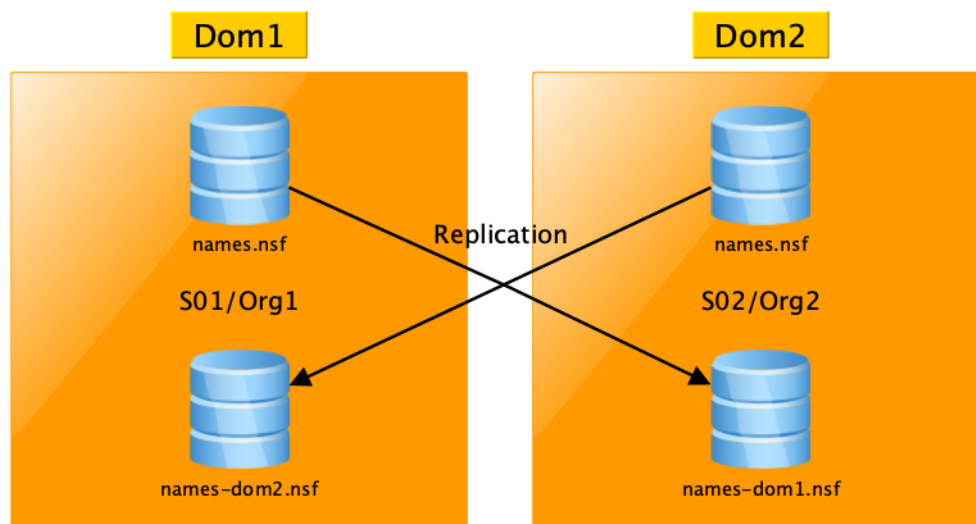
On the »Basics« tab, you set the following options:

1. In the »Domain type« field, select the »Non-adjacent domain« option.
2. Mails are sent to this domain. This is the domain (not adjacent) to which there is no direct connection.
3. The mails are routed via this domain.
4. The entry in the »Domain description« field is optional.

2.8. Activation of foreign Directories

For users it is inconvenient when creating mails if they cannot select recipients from a Domino Directory («names.nsf») with a click or use the quick addressing. Therefore it is a good idea to integrate foreign directories into your own Notes/Domino environment.

2.8.1. Replication



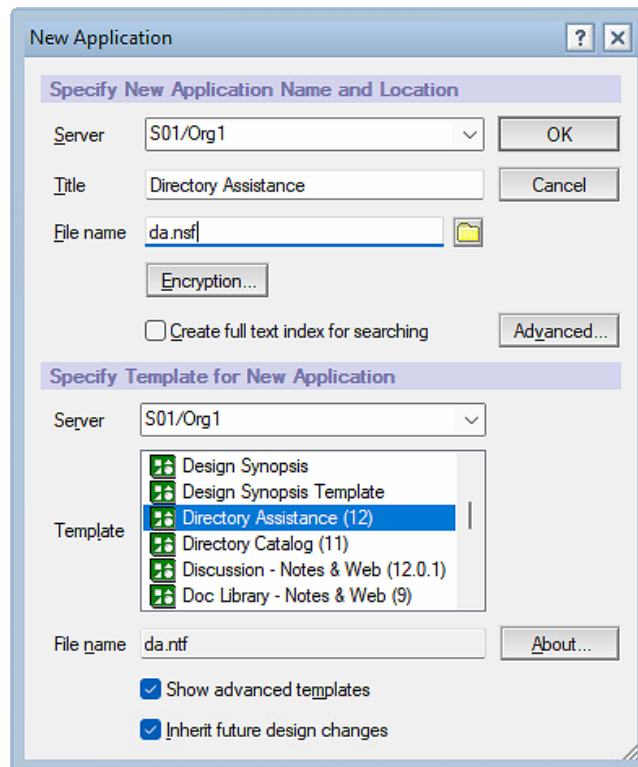
In the example, »Dom1« gives its directory as a replica to »Dom2« and in return receives the directory of »Dom2« as a replica.

It is a good idea to name the foreign directory accordingly. Thus »Dom1« could store the foreign directory as »names-dom2.nsf« on its own Domino Servers. There is no confusion and the assignment is clear.

Important

- **Replication**
The contents of the replicas must be kept up to date.
Therefore, do not forget to include the foreign directory (for »Dom1«, for example, »names-dom2.nsf«) in the connection document created for replication with the other side.
- **ACL settings**
The other side should be given the »Reader« level for our directory - this prevents unwanted changes in our own directory.
The foreign Domino Server should have »Editor« access to the directory received from the other side. This will replicate all document changes. Replication of design changes and ACL changes are thus excluded.

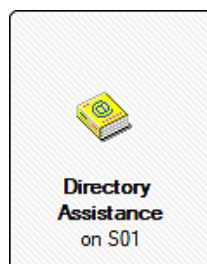
Only by storing foreign directories on the own Domino Servers, a directory is not considered by the Domino Servers for the addressing of mails. Foreign directories must be activated, for this the following possibilities exist.



First create the new Directory Assistance application with the parameters given in the screenshot and select the correct template.

Hints

- The title and file name are freely selectable. The application is entered in the server document with the assigned file name.
- In order for the template to be displayed to you, you must activate the »Show advanced templates« option at the bottom of the dialog.



Since the title and file name of the application can be freely chosen, the »Directory Assistance« application must be made known to the Domino Server in the server document.

Tab **Basics**

DIRECTORY ASSISTANCE

Basics | Naming Contexts (Rules) | Domino

Basics

Domain type: 1 Notes

Domain name: 2 Dom2

Company name: 3 Dom2 Inc.

Search order: 4 1

Make this domain available to: 5 Notes Clients & Internet Authentication/Authorization
6 LDAP Clients

Group authorization: 6 No

Enabled: 7 Yes

The following fields exist on the »Basics« tab:

1. Domain type

Select whether the foreign directory is a Notes/Domino or an LDAP directory.

2. Domain name

The name of the foreign domain (in the example: »Dom2«).

3. Company name

The name of the company to which the foreign directory belongs (in the example »Dom2 Inc.«).

4. Search order

The search sequence is defined here in the event that other third-party directories are used. The start value is »1«.

5. Make this domain available to

The option »LDAP Clients« is only required if the own Domino Server is used as LDAP Server and information from the foreign Directory should be available for LDAP queries.

6. Group authorization

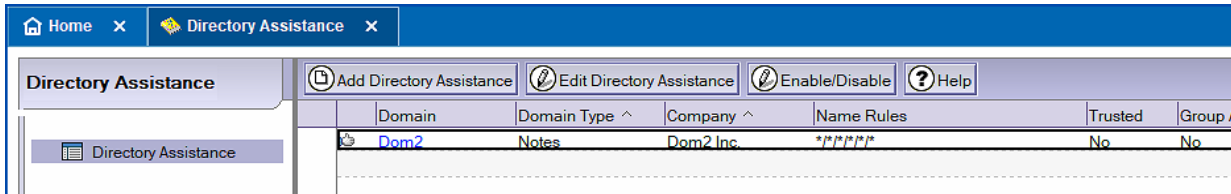
If desired, groups in the foreign directory can be used for access control of Notes Clients in ACLs or for access control when using the HTTP service.

7. Enabled

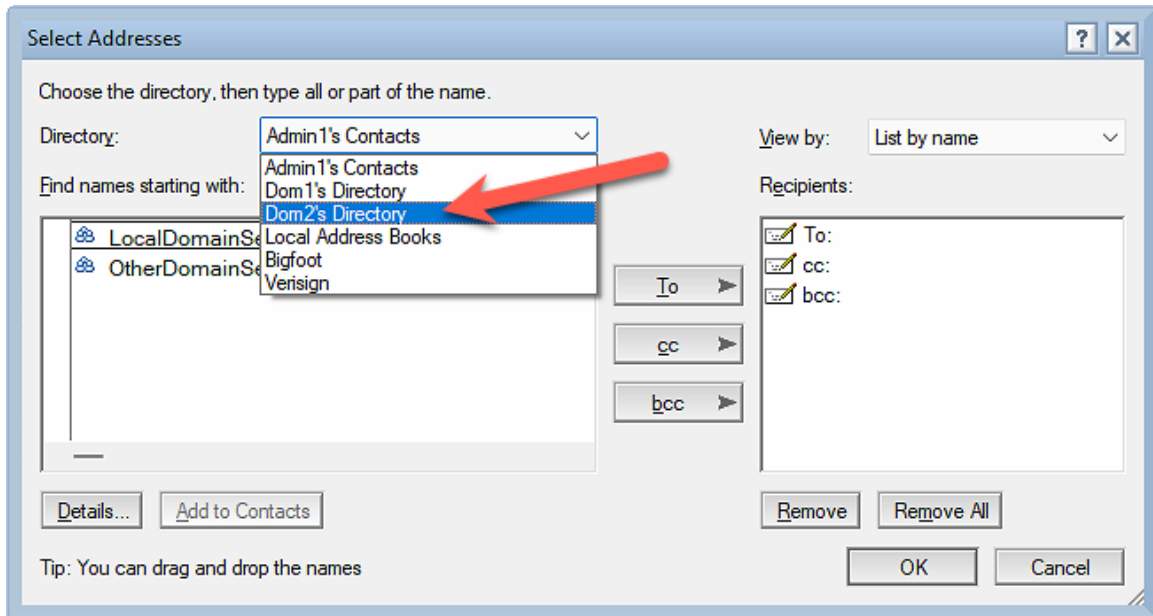
If you want the foreign directory to be temporarily unavailable, change this option to »No«.

By using multiple links or specifying up to 5 replicas, the Domino Server can switch to a different replica in case of problems with a foreign directory.

Save and close the document.



The Directory Assistance for the domain »Dom2« is now active. Check in the Notes Client whether this directory is offered for selection when addressing recipients for new mails.



Hint
 In all likelihood, the Domino Server and Notes Client (including Domino Administrator and Domino Designer) will require a restart.

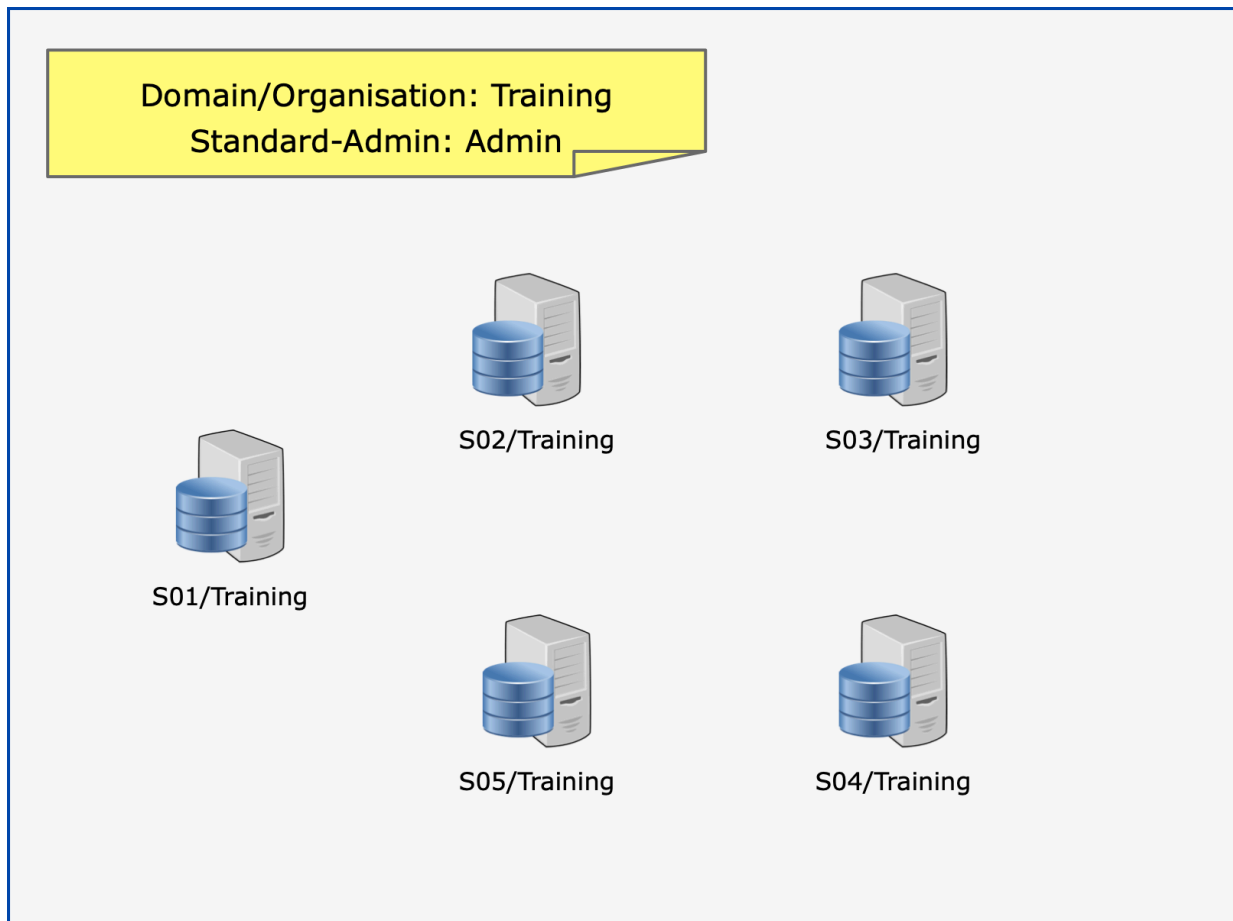
2.10. Learning environment for all further chapters in this book

In order to try the »Domino Cluster« or »ID Vault« (these do not work across domains/organizations) in subsequent chapters, we need to replace the current learning environment.

Provided that you have followed the recommendation in the [2.1. Learning environment for chapters on this topic](#) on page 12 and made a backup of the installation files, you must perform the following steps:

- Stop the Domino Server (additionally the service in Windows) and all Notes Clients.
- Delete (or rename the folders) the installation folders for the Domino Server and Notes Client (in my case this is the folder »D:\HCL«).
- Copy the folders from the backup back to the same position in the file system.
- Modify the »hosts« file according to the new names.
- Run the setup for the Domino Servers and get the Notes Clients up and running.

The following names are suitable:



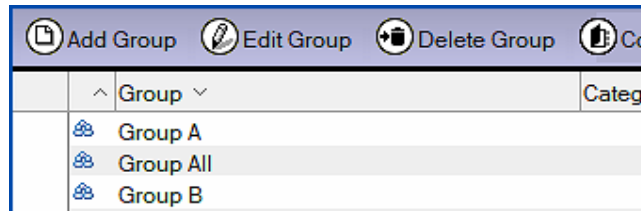
The number of Domino Servers is freely selectable - at least **2** are required for the learning environment.

3.1. Resolve nested groups

Groups may be nested within each other. If this is used with many groups over several levels, it is easy to lose the overview.

The question in which groups a user is contained (direct or nested) can hardly be answered anymore.

Let's assume the following constellation.

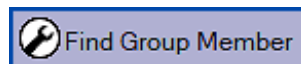


Group structure:

Name	Member(s)	Note
Group A	Admin/Training	
Group B	Betty Jones/Training	
Group All	Group A Group B	Nested

In which groups is »Betty Jones/Training« directly or indirectly a member?

A search in the directory (menu »View« → »Search This View«) finds only groups in which the person is directly entered.



Also a search via action »Find Group Member« (at the top of the action bar) returns only direct memberships (please note that the first **and** last name must be used - otherwise there will be no hits at all).

Solution: Select the tool »Groups« → »Manage...« on the right.

This tool is basically for managing groups, but it can also resolve memberships across all levels of nesting.

3.2. Service generates out-of-office messages

In older Notes/Domino versions, out-of-office messages were generated by an agent stored in the users' mailbox.

Since the schedule for the execution of this agent was set to an interval of several hours (default), it was not possible to speak of timely notification for the sender of a mail. In addition, the minimum adjustable time span for an absence was set to one day.

Since Notes/Domino version 8.x the generation of out of office messages by a service (Malrouter) is possible. The following advantages can be achieved:

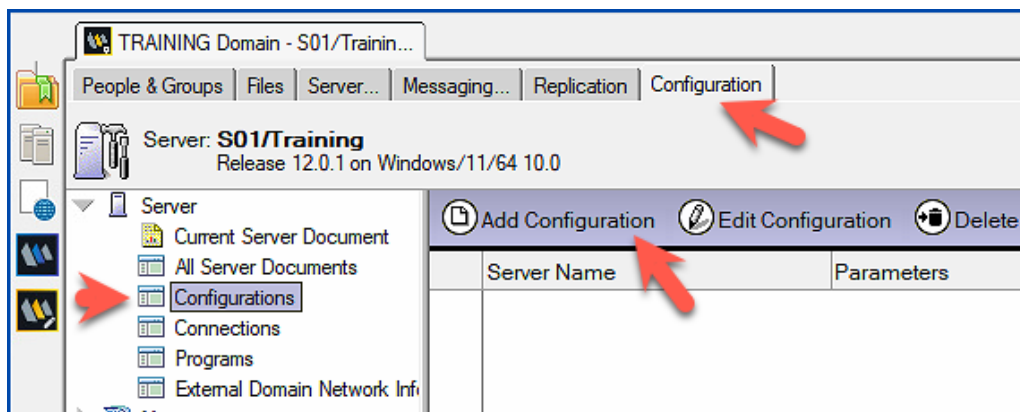
- Out-of-office messages are sent in real time, i.e. immediately after a new mail is received.
- The minimum time period that can be set for the absence is 1 hour.

Hint

The use of the Out-of-Office Service is optional and not automatically activated after the installation of a new Notes/Domino environment.

3.2.1. Activation in the configuration document

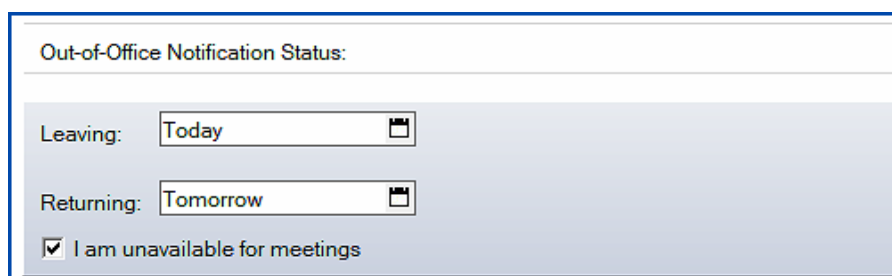
In Domino Administrator, open the »Configuration« tab and select the »Configurations« view on the left.



Click the »Add Configuration« action (or open an existing configuration, if available).

3.2.2. Changed setting options for the user

When a user sets the out-of-office settings in his mailbox, he basically sees the following setting options:



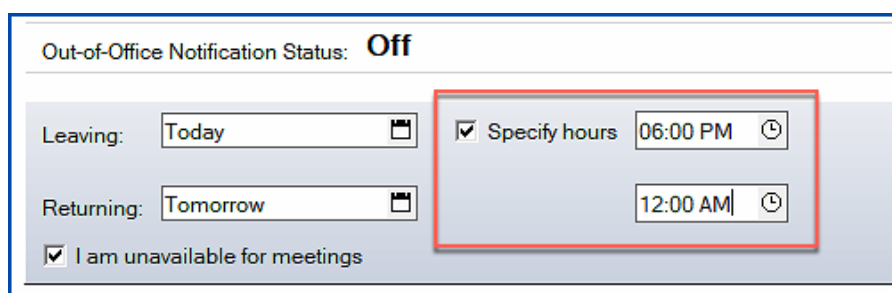
Out-of-Office Notification Status:

Leaving: Today

Returning: Tomorrow

I am unavailable for meetings

The fields »Leaving« and »Returning« exist. A setting for a desired time span in hours is missing.



Out-of-Office Notification Status: **Off**

Leaving: Today

Returning: Tomorrow

Specify hours 06:00 PM

I am unavailable for meetings

12:00 AM

As soon as the Out-of-Office service is active on the Domino Server, an additional time period (minimum: 1 hour) can be set.

3.3.1. What is the ID Vault?

- ID Vault is a Domino application that keeps protected copies of user IDs.
- Administrators and users are given a tool to manage user ID files with the ID Vault.
- Ability to restore user IDs and reset passwords by authorized users (besides administrators, additionally people from the helpdesk, power users, etc.).
- Support for 3rd party programs (C, Java, JavaScript or LotusScript).
- Automatic synchronization of multiple user ID files (e.g. when using notebook and desktop PC).
- Little to no user activity required.
- User ID files can be extracted to access the IDs stored encrypted in the ID Vault (»Auditor« role in the Vault application).
- The login dialog in the Notes Client displays self-defined hints on how to proceed in case of a forgotten password (green »+« symbol directly in the login dialog).
- The assignment of users to an ID Vault is implemented by policies in conjunction with settings documents of the »Security« type.

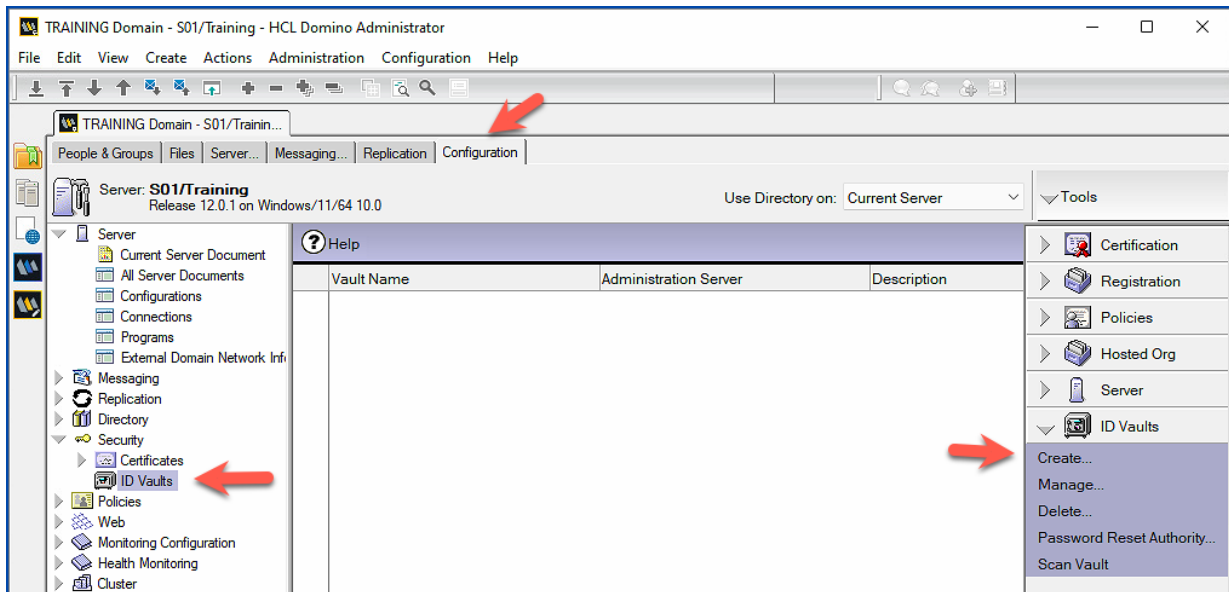
3.3.2. Requirements for the ID Vault

- Notes Client and Domino Server version 8.5 or higher.
- Vault Trust Certificates (are created automatically).
- Policies in conjunction with »Security« type settings documents (both documents are automatically created during ID Vault setup, if desired).
- It is mandatory for the Notes Client to have a valid entry for the home/mail server in the location settings.

3.3.3. How does the ID Vault work?

- **Active Notes users**
After the policies are effective, the user ID file is copied to the Vault the first time the user logs in (randomized timing, can take up to 8 hours).
- **Registration of new users**
The user ID file is already copied to the ID Vault during user registration.

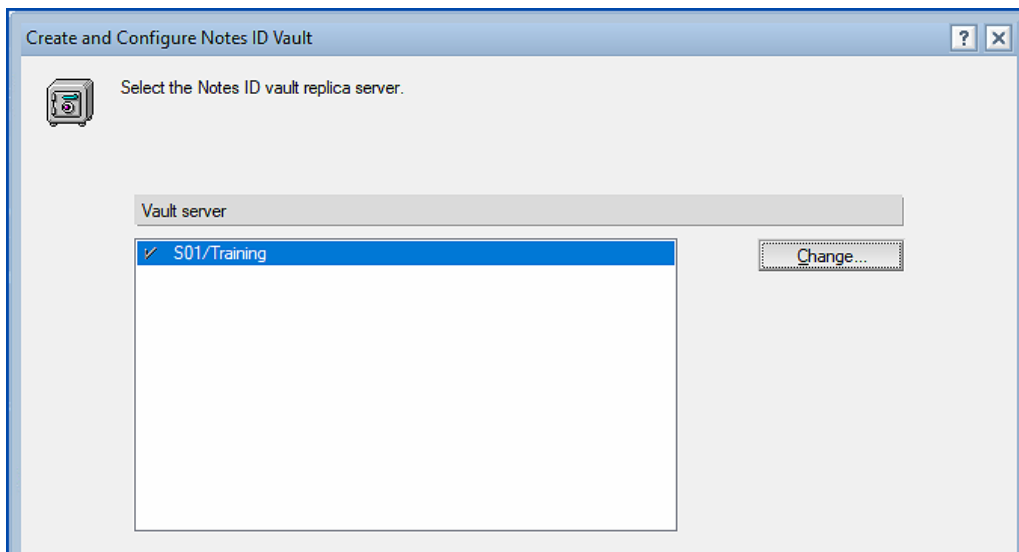
3.3.7. Setting up the ID Vault



Open the »Configuration« tab in the Domino Administrator and select the view »Security« → »ID Vaults« on the left. Click on the tool »ID Vaults« → »Create...« on the right.

The configuration is implemented in the following dialogs (first a dialog with further information is displayed) in a total of 10 steps.

Step 3

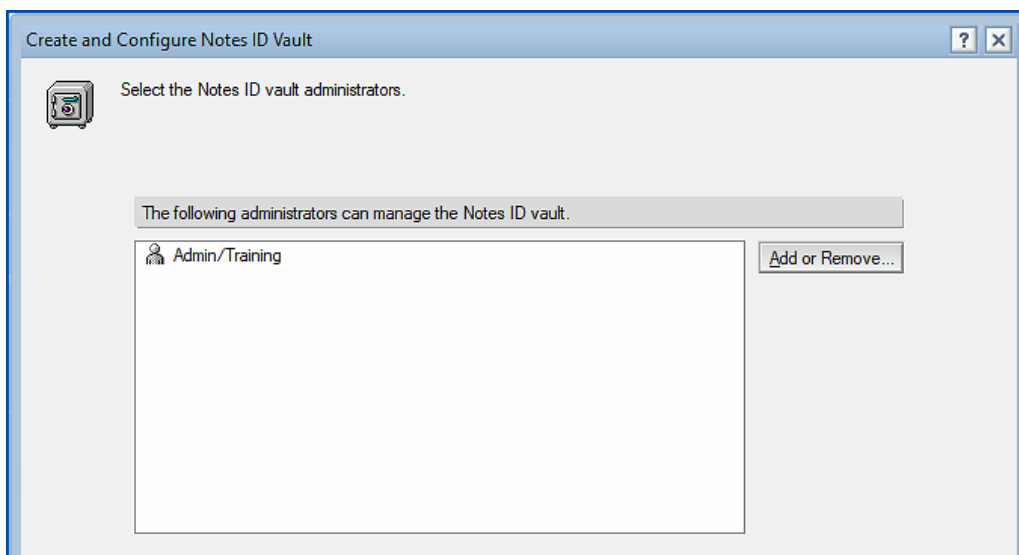


The ID Vault application is stored on this Domino Server. The »Change...« button can be used to select another Domino Server.

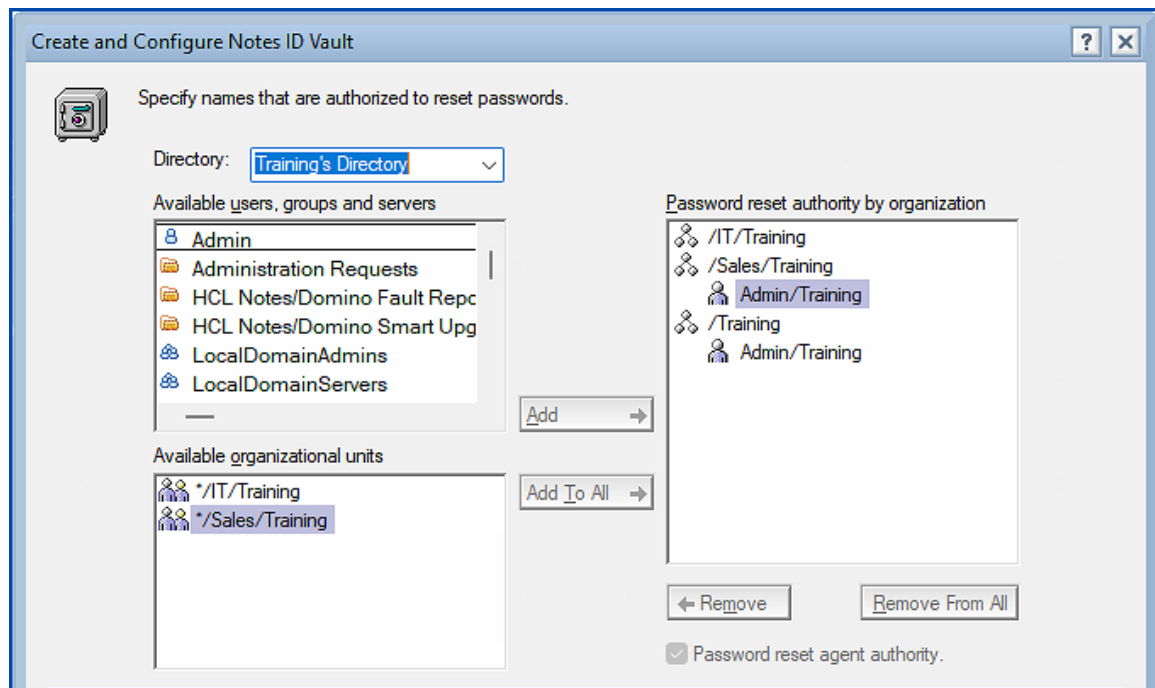
Hint

Only **one** Domino Server can be selected at a time. You can later create replicas on additional Domino Servers using the ID Vault Management tool.

Step 4



The person shown here is allowed to manage the ID Vault. The »Add or Remove...« button can be used to select other persons (not groups). Only persons are available for selection who are entered in the server document on the »Security« tab in the »Administrators« field directly or as a member of a group.

Step 6

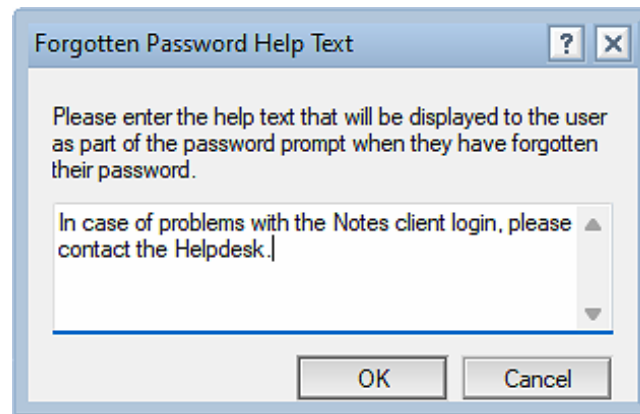
Select here for each Organization or Organizational Unit listed in the right window which person is allowed to perform a password reset. If you select a group, a separate password reset certificate will be created for each member of the group.

Hint

There will be no connection to the members of the group later. If the members change, this does not affect currently created password reset certificates.

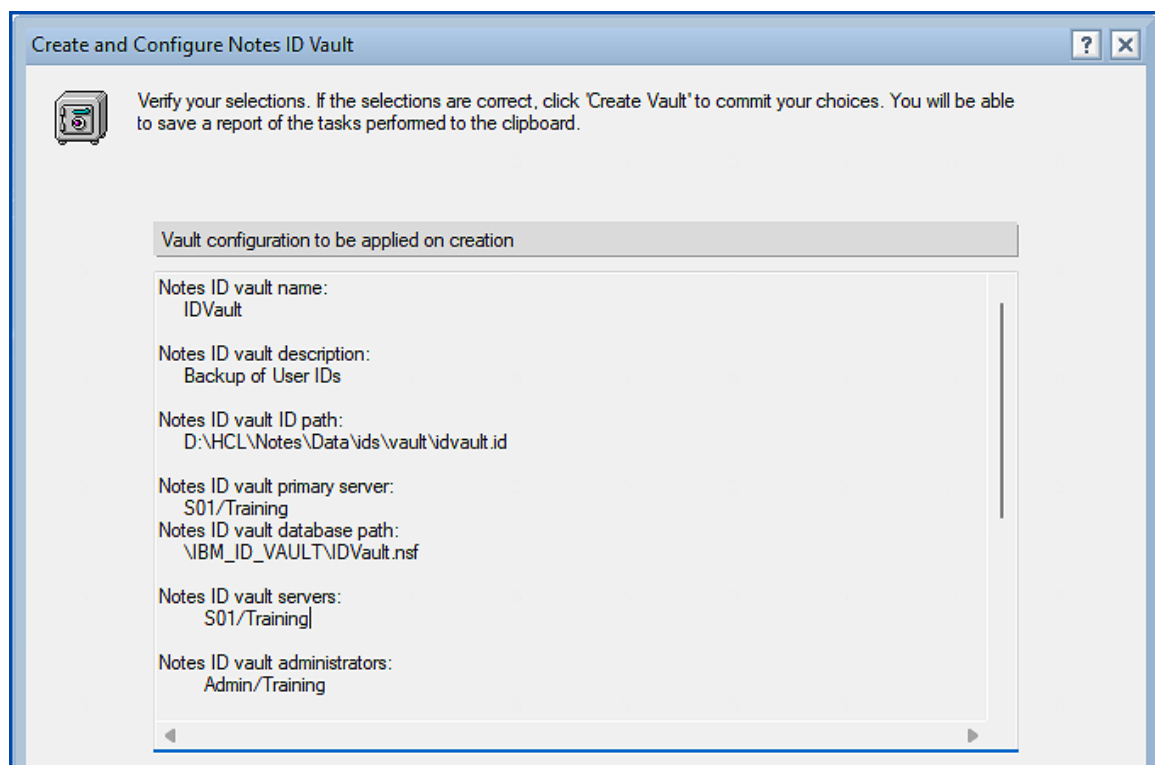
Important

Care should be taken when using the »Available organizational Units« option. If »*/Sales/Training« is used as an example, any user from this organizational unit may reset passwords.



The entered text will be displayed in the Notes Client login dialog when you click on the green »+« icon.

Step 9



All previously defined parameters are displayed here for review. Confirm the dialog by clicking the »Create Vault« button.

3.3.8. Checking the ID Vault setup

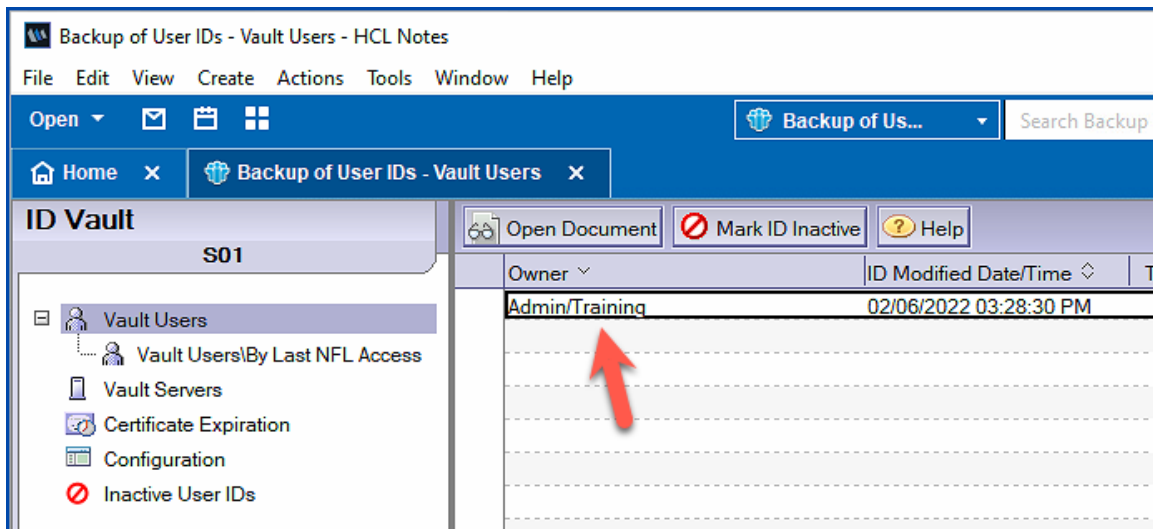
After setting up the ID Vault, you will find the following newly created items.

- **ID Vault Application**
The application was saved in the »IBM_ID_FAULT« directory below the »Data« directory.
- **ID Vault Document** (saved in the directory)
In the Domino Administrator, select the »Configuration« tab and then the item »Security« → »ID Vaults« in the navigation on the left.
- **Password Reset Certificates** (saved in the directory)
In Domino Administrator, select the »Configuration« tab and then the item »Security« → »Certificates« → »Certificates« in the navigation on the left.
- **Vault Trust Certificates** (saved in the directory)
In Domino Administrator, select the »Configuration« tab and then the item »Security« → »Certificates« → »Certificates« in the navigation on the left.
- **Policy-/Settingsdocuments** (saved in the directory)
In Domino Administrator, select the »People & Groups« tab and then the item »Policies« or »Settings« in the navigation on the left.

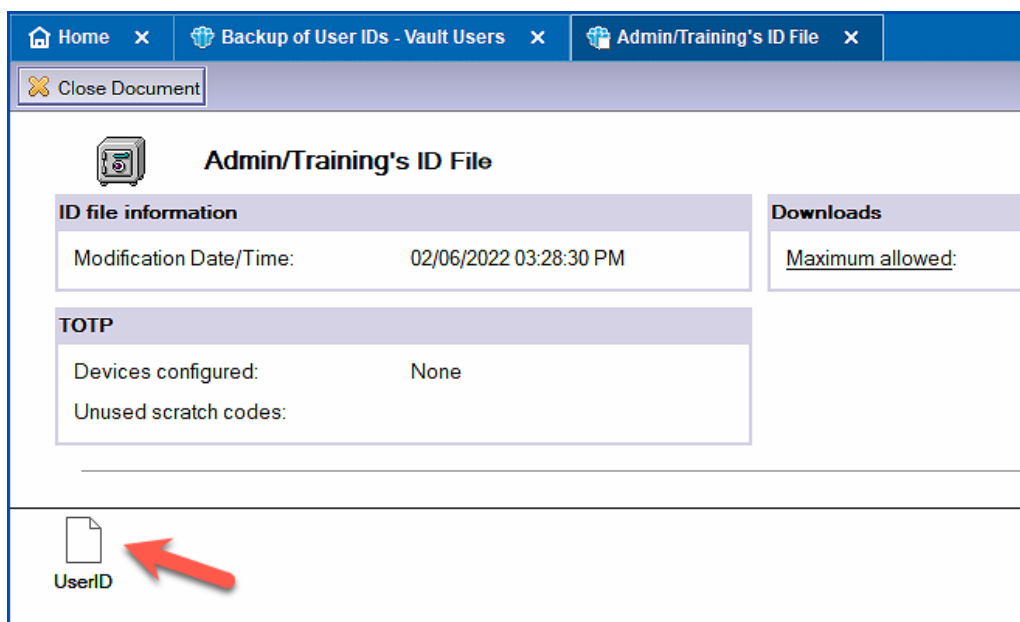
3.3.9. Upload of user IDs to the ID Vault

In order for the user ID files to be uploaded to the ID Vault application, the new policy created or changed during the ID Vault setup must be effective. This can be checked (see the following screenshot) in the login dialog when starting the Notes Client.

If you click on the green plus (+) at the »Forgot your password?« message and then your self-defined message is displayed, then the policy is effective for the user named in the login dialog.



The document should be available immediately.



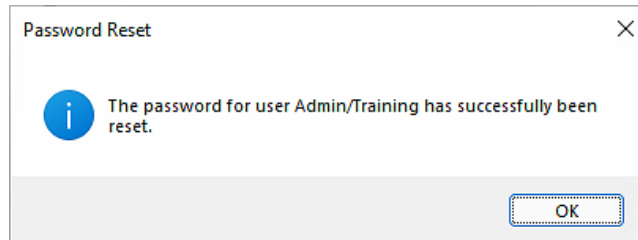
In the opened document you will see the attached user ID file.

(e.g. the manager) to whom a randomly generated password is sent by e-mail.

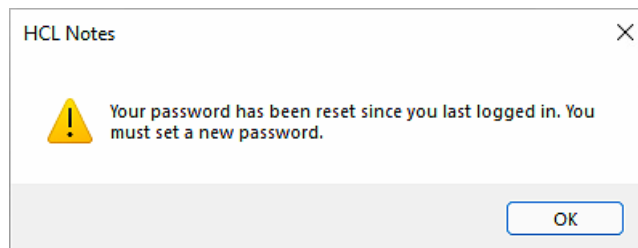
4. New password und Confirm new password

Enter and confirm the password you set yourself.

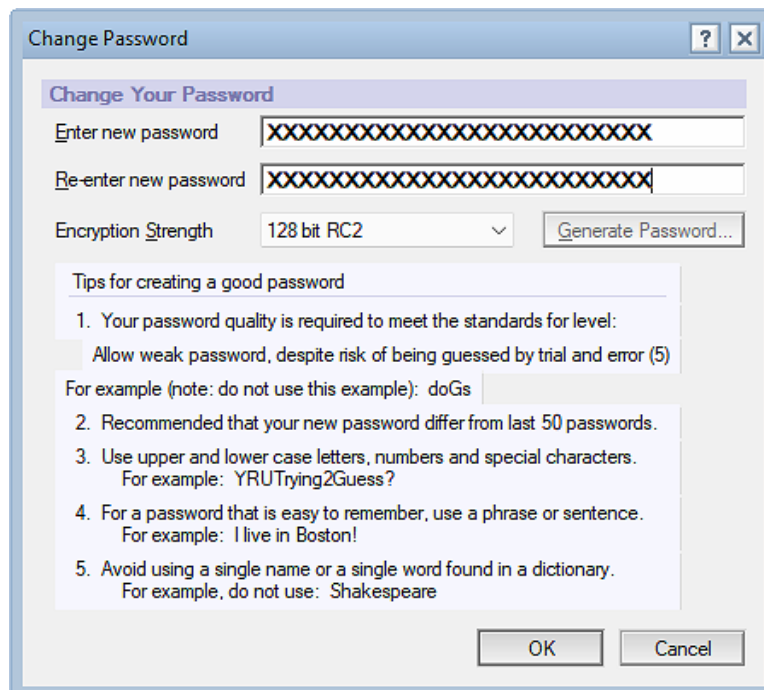
Confirm the password reset by clicking the »Reset Password« button.



After entering the reseted password in the Notes Client login dialog, the user will be prompted to enter a new and permanently valid password.



Confirm the dialog with »OK«.

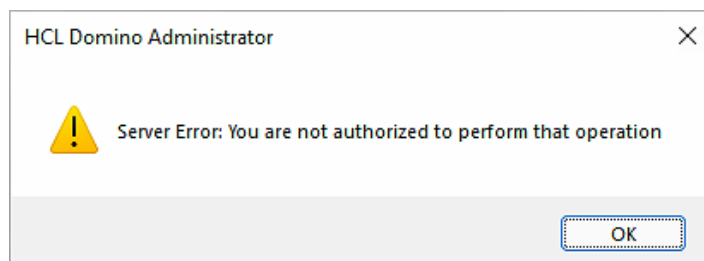


Enter a new password. In the basic configuration of the Domino Server, this may be the previously used password.

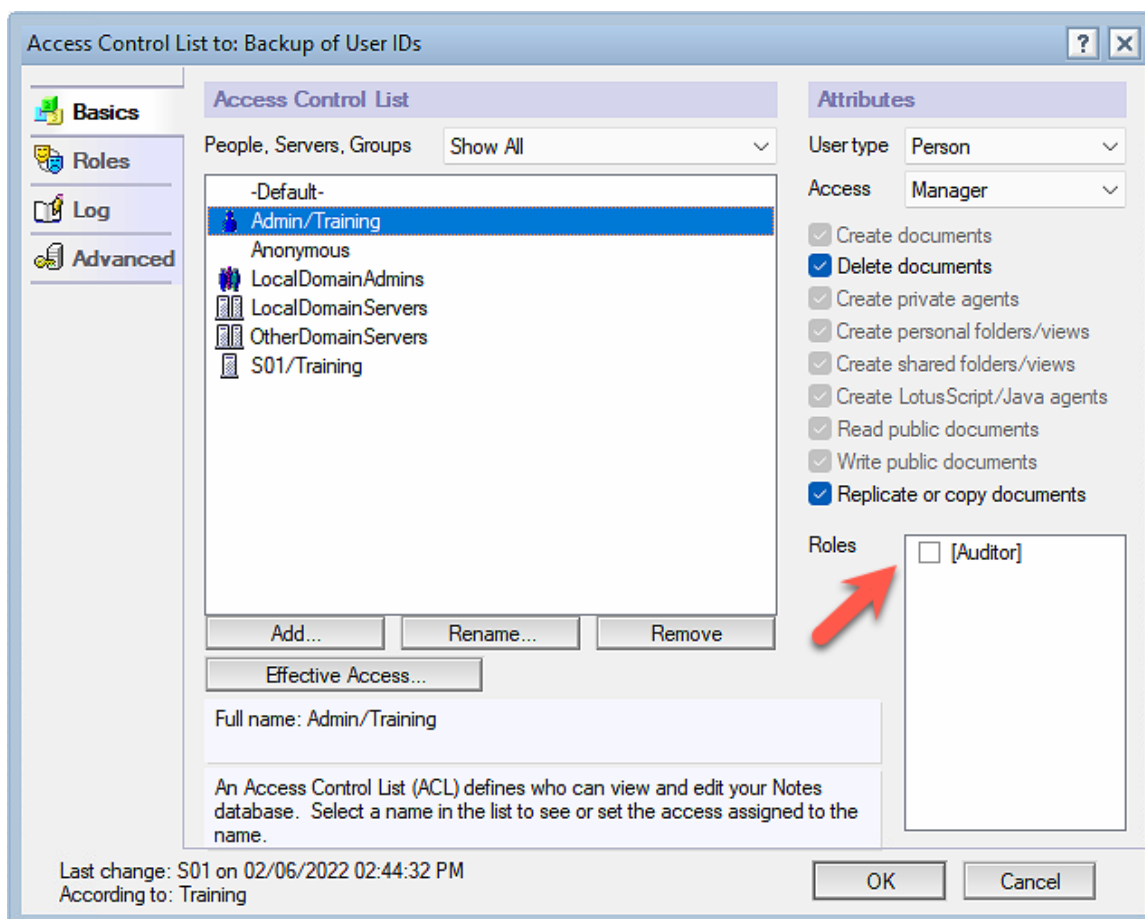
3.3.12. Using the ID Vault - extract user ID file

A user ID can be manually downloaded from the ID Vault and made available to a user.

For this purpose, the »Auditor« role is required in the ACL of the »ID Vault« application.



Without this role, you will get the error message shown in the screenshot. Open the dialog for managing the ACL for your ID Vault.



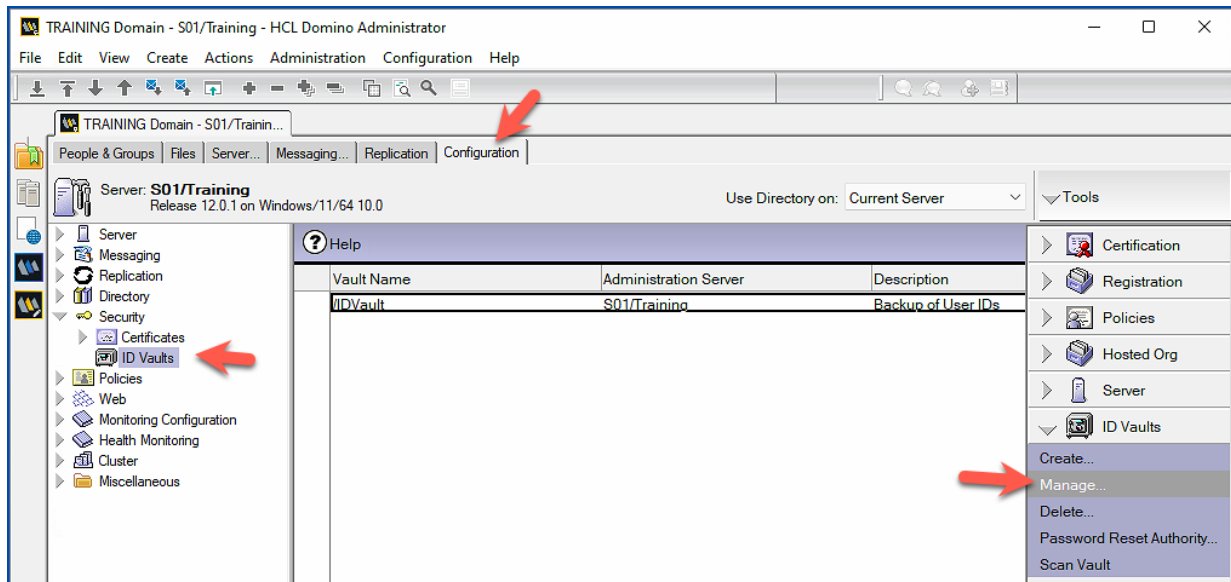
Activate the role »Auditor« for your user and confirm the dialog with »OK«.

In Domino Administrator, open the »People & Groups« tab and select the »People« view on the left. After you have selected the desired user, click on the tool »ID Vaults« → »Extract ID From Vault...«.

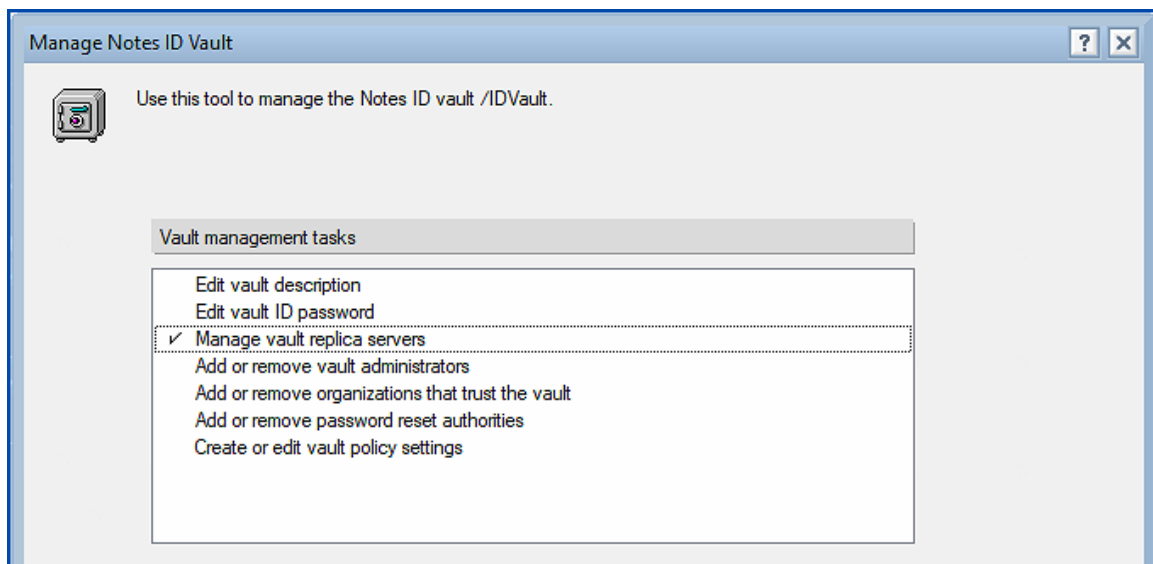
3.3.13. Make changes to the ID Vault configuration

The configuration of the ID Vault can be changed after the initial setup.

Open the »Configuration« tab in the Domino Administrator. Select the view »Security« → »ID Vaults« in the navigation on the left and select the desired ID Vault in the overview. Click on the tool »ID Vaults« → »Manage« on the right.



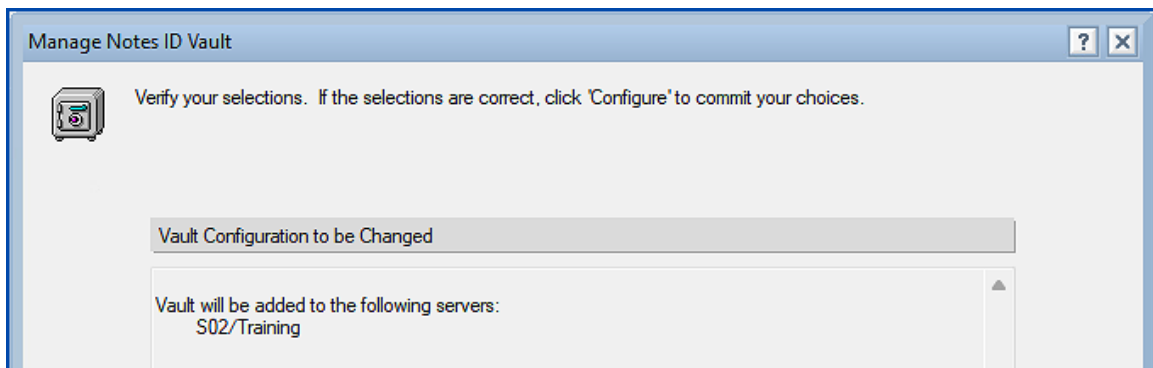
An information dialog appears first (if you did not deactivate this when creating the ID Vault). In the following dialog you select what you want to change in the configuration (multiple selection is possible).



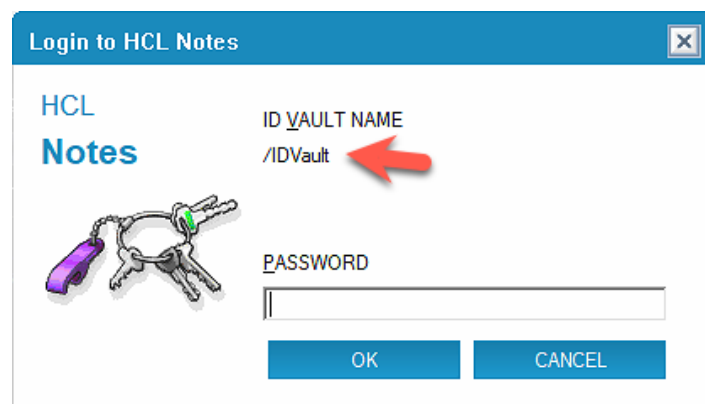
As an example, we will also make the ID Vault available as a replica on another Domino Server. Basically, the ID Vault should be available on all Domino Servers that are used as home servers for users.

Confirm the dialog with the »Next« button.

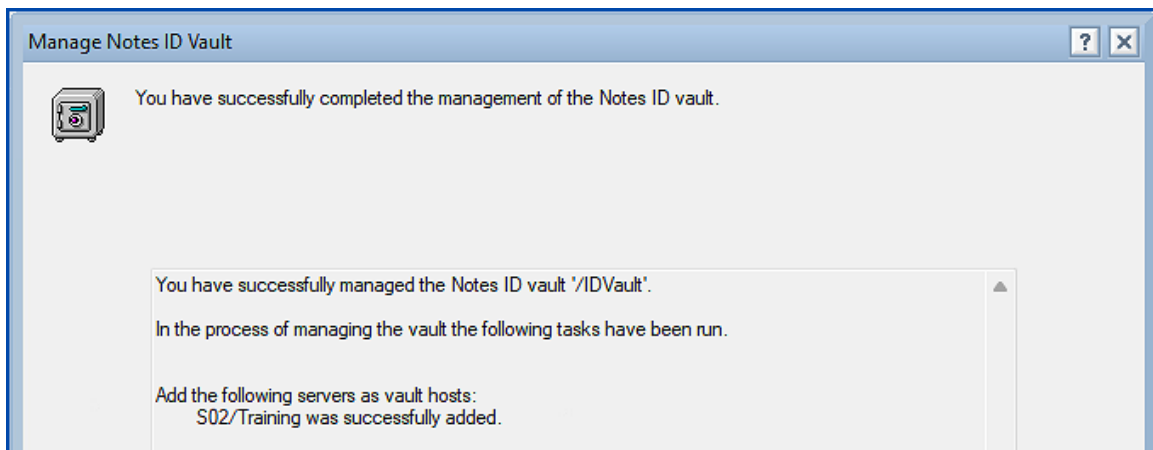
Confirm the dialog by clicking the »Next« button.



The selected configuration is displayed for control. Confirm this dialog using the »Configure« button.



Before the new replica is created, you must enter the password to the ID file of the ID Vault.



The replica of the ID Vault was created on the Domino Server »S02/Training«.

Hint

Further changes to the ID Vault configuration are similarly convenient. Feel free to try out additional options in your learning environment!

Restarting the synchronization: Management

By the console command »qvault« (query vault) as well as by a new option in the Domino Administrator different options can be used when managing the ID vault.

First, the following entry must be added to the »notes.ini« file:

```
IDV_Enable_Vault_Scan=1
```

Now the console command »qvault« can be used (it may be necessary to restart the Domino Server to use it). By adding the »/?« option to the command, the allowed parameters are listed.

```
load qvault /?
[1C1C:0002-1250] Query Vault Tool.
[1C1C:0002-1250] Usage: load qvault [-x <vaultname> [-u <username> [-r | -a | -d | -i | -v | -p]] | [-d | -p]]
[1C1C:0002-1250] Usage: Usage: Add quotes around <vaultname> or <username> if the name contains a space
[1C1C:0002-1250] -x <vaultname> Scan O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> Scan O=VaultName for UserName
[1C1C:0002-1250] -x <vaultname> -u <username> -r Revert Archived UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -a Archive UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -i Inactivate UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -v Reactivate UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -d Delete Archived UserName in O=VaultName
[1C1C:0002-1250] -x <vaultname> -u <username> -p Update User Data in O=VaultName
[1C1C:0002-1250] -x <vaultname> -d Delete All Archived Users in O=VaultName
[1C1C:0002-1250] -x <vaultname> -p Update All User Data in O=Vaultname
[1C1C:0002-1250] e.g. load qvault -x <vaultname> -p Update All User Data in O=Vaultname
```

Example (Be sure to use canonical Notes names):

```
load qvault -x O=IDVault -u "CN=Admin/O=Training"
```

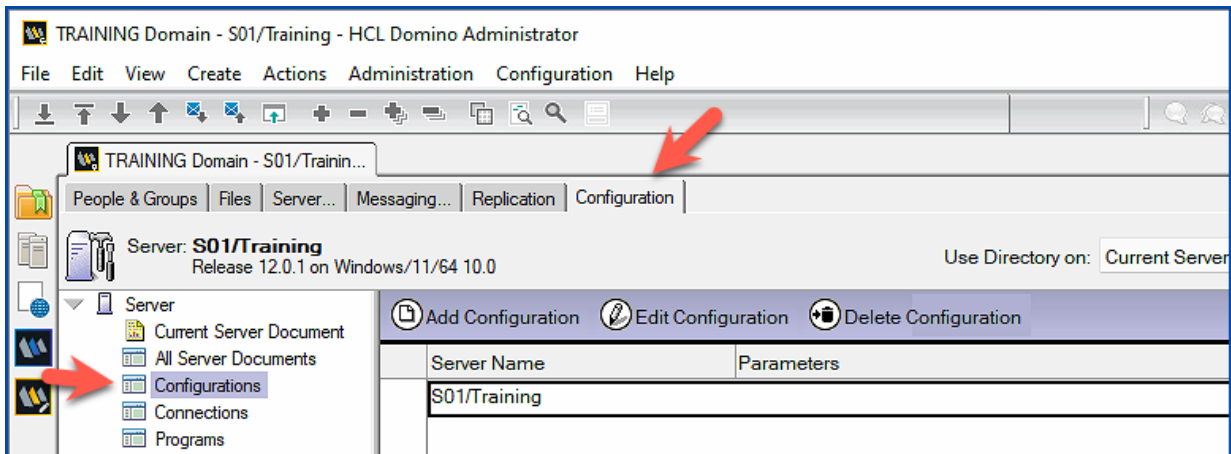
```
load qvault -x O=IDVault -u "CN=Admin/O=Training"
[2344:0002-0348] QVR: Vault O=IDVault
[2344:0002-0348] QVR: User CN=Admin/O=Training
[2344:0002-0348] Scan Vault : O=IDVault, Total 1, Updated 0, No Update Needed 1, Update failures 0
[0448:005B-0FD4] 06.02.2022 18:59:04 Opened session for S01/Training (Release 12.0.1)
[0448:005B-0FD4] 06.02.2022 18:59:04 Closed session for S01/Training Databases accessed: 1
```

3.4. License tracking

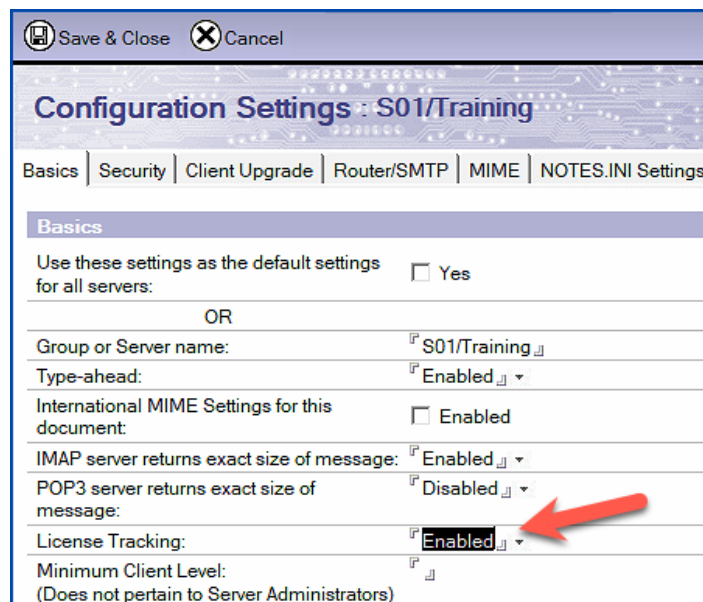
License tracking enables monitoring of licenses actively used by users. After activation, accesses to the Domino Server are recorded and stored in the **Domino User License Tracking** application (»userlicenses.nsf«).

3.4.1. Activation of license tracking

In Domino Administrator, open the Configuration tab and select the view »Server« → »Configurations« on the left.



Create a new or open an existing configuration document.

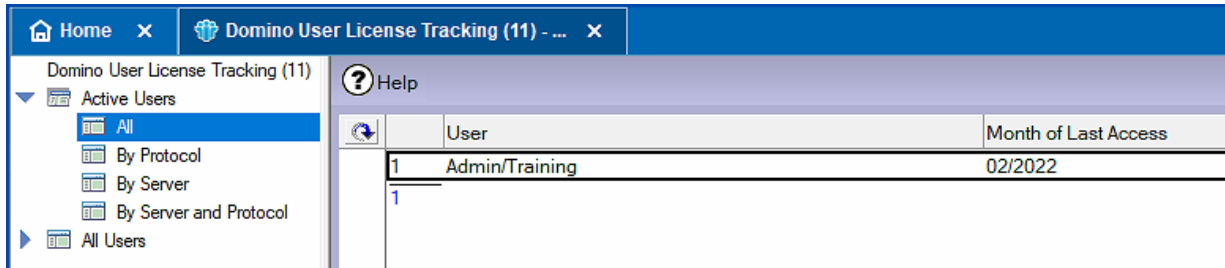


Enable license tracking in the »License Tracking« field on the »Basics« tab. Save and close the document.

As soon as license tracking is activated, each authenticated connection (Notes NRPC, HTTP, IMAP, POP3, SMTP and LDAP) of a user is registered and first temporarily stored in the »license.ncf« file. Here, the complete user name, the used protocol as well as date and time are recorded.

3.4.2. Documents in the userlicenses.nsf application

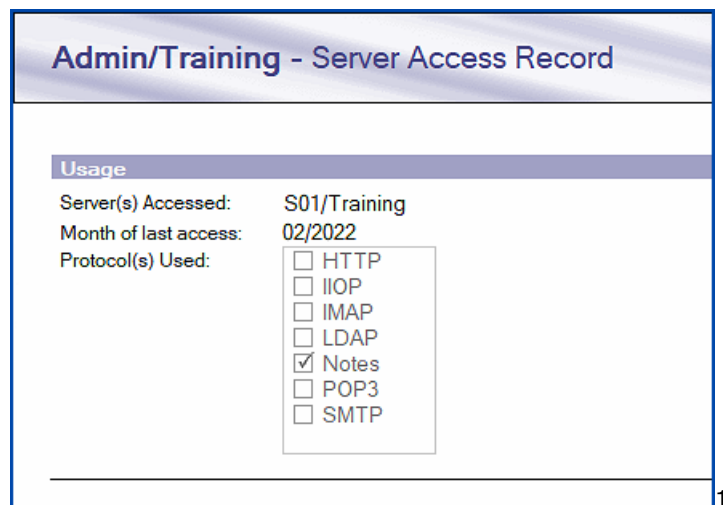
Once the Domino User License Tracking application (>userlicenses.nsf<) has been created, it can be opened and the documents for the individual users can be viewed. Different views are available for evaluation.



Hint

If you want to open this application in the Notes Client, you have to type the file name »userlicenses.nsf« yourself in the Open Application dialog - the application will not be displayed automatically because of a specific flag.

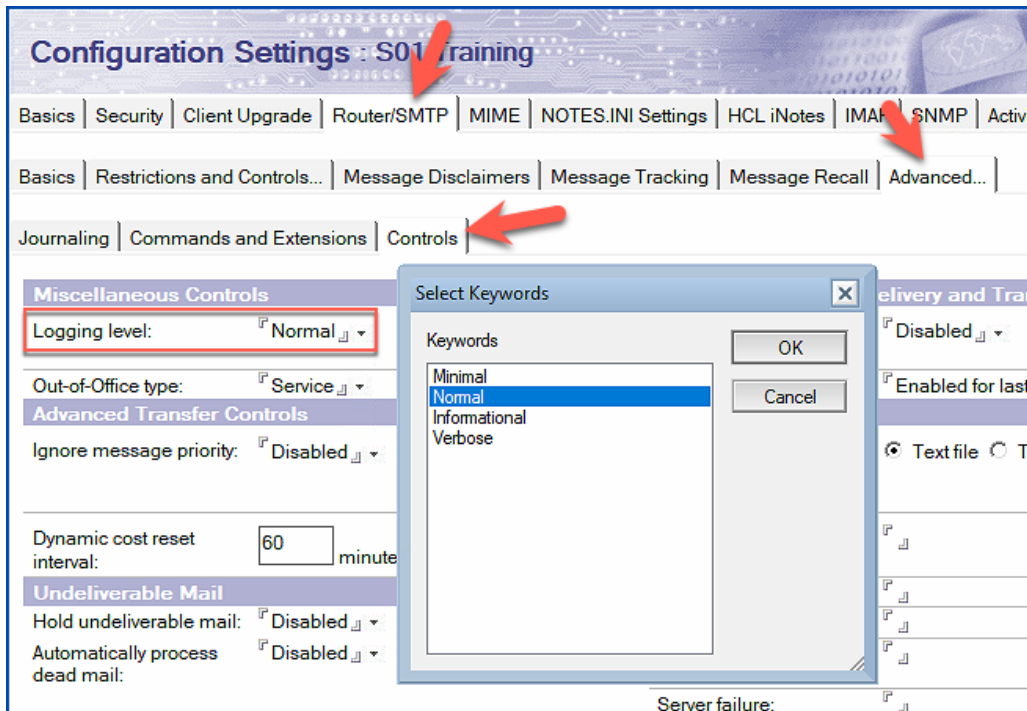
Open one of the documents.



The opened document displays the Domino Servers used by the user, the month of the last access and the protocols used.

4. Mailrouting

Create a new configuration document or open an existing one. Select the tab »Router/SMTP« → »Advanced...« → »Controls«.



In the field »Logging level« there are several options to choose from - the default is »Normal«. The option »Minimal« shows even less information at the Domino console and is therefore not applicable.

For practical use the option »Informational« seems to be useful - it provides the following information about a sent mail at the Domino console:

- [064C:0006-0E28] 07.02.2022 16:55:11 Router: Message 0050BD9B transferred to S02/TRAINING for Betty Jones/Training@Training **from Admin/Training Size: 1K** via Notes

Additionally, the sender and the size of the mail are displayed. When using the »Verbose« option, further messages from the router service are added - sometimes without much added value for the administrator.

Try it out!

3. Do not allow recall of messages older than

For the time span selected here in minutes, hours, days or weeks, the recall of a mail is possible. Default: 14 days.

Hint

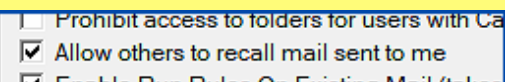
Unless a policy with message recall settings is in effect (see next chapter), the setting made here applies to all users whose mailboxes are stored on this Domino Server.

Save and close the configuration document.

Important

Unless specified by a policy, users may decide for themselves in the preferences of the mailbox whether a mail sent to the user may be recalled.

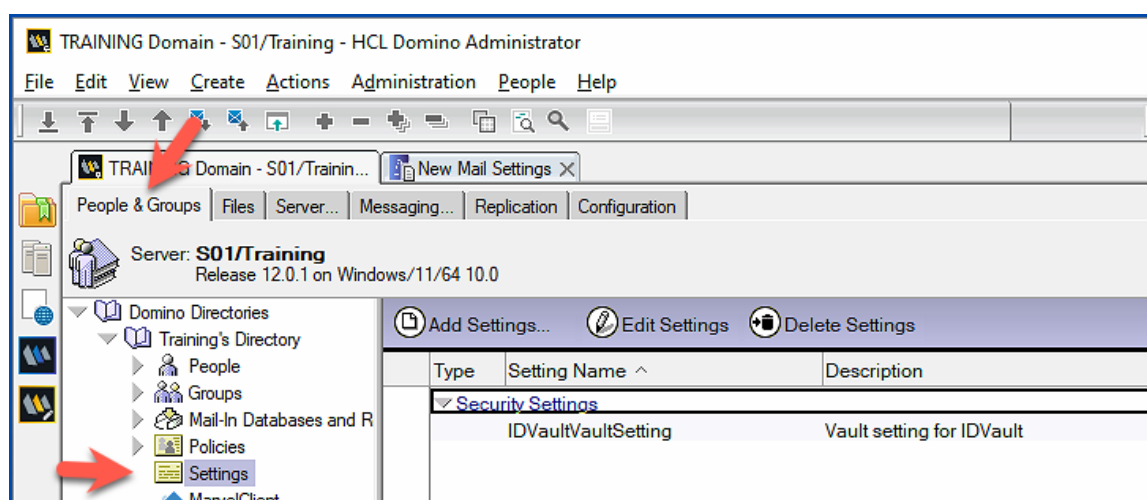
You can find this setting in the »Preferences« dialog (click the action »More« → »Preferences« in the open mailbox) on the »Mail« → »Basics« tab in the »View and Folder Management« section.



4.2.2. Configuration through policies

A policy in combination with a settings document for the »Mail« section can **override** the settings in the configuration document.

In Domino Administrator, open the »People & Groups« tab and select the »Settings« view on the left.

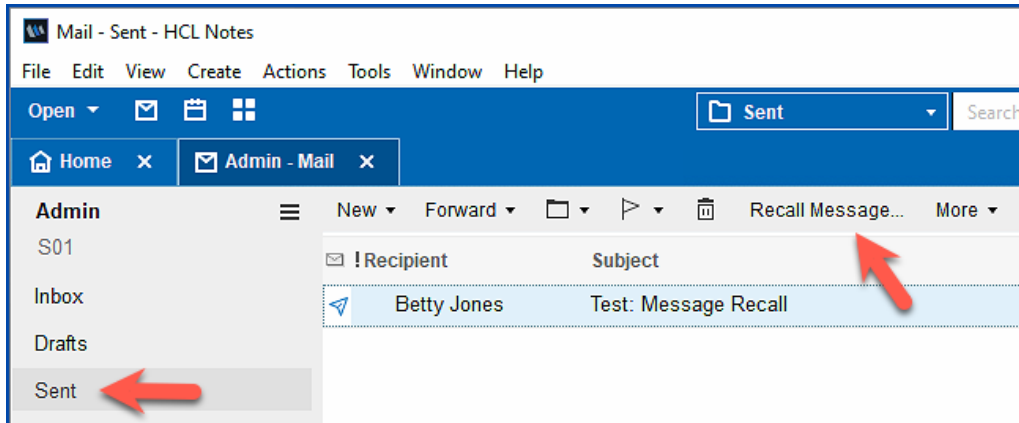


Create a new or open an existing settings document from the »Mail« area. Select the tab »Mail« → »Message Recall«.

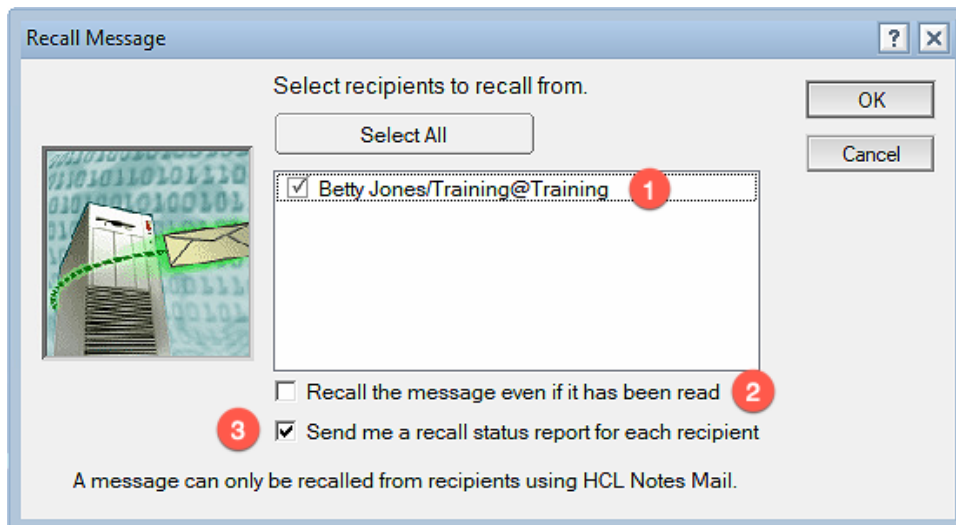
4.2.3. Recall of mails by the user

Provided that the administrative settings allow mail recall, the user can start message recall directly from his mailbox.

Open your mailbox and select the Sent view.



Click on the action »Recall Message...«.



The following options are available:

- 1. Select recipients to recall from**
If the mail was addressed to more than one recipient, the »Select All« button can be used to select all recipients.
- 2. Recall the message even if it has been read**
This option works **only** if the recall of read messages is allowed in the configuration document or policy.
- 3. Send me a recall status report for each recipient**
If you wish, the Domino Server will send you a status report in the form of a mail for each selected person.

4.3. Mail tracking

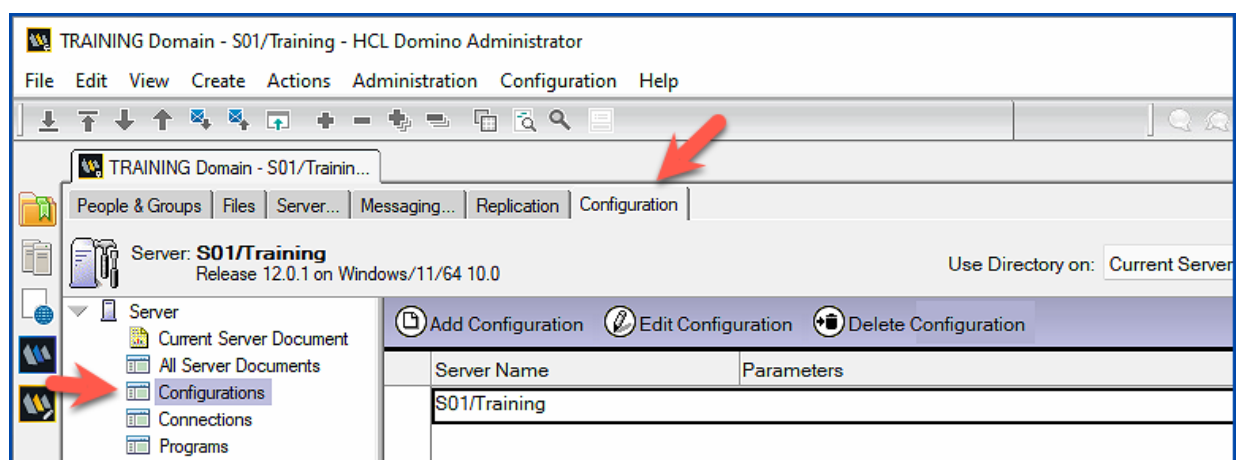
Mail tracking allows to trace the transfer of mails from the sender to the recipient. Additionally one receives the information whether the receiver has read or deleted the mail.

If you have ever tried to track a mail across multiple Domino Servers using the information in the LOG applications (»log.nsf«), you will love mail tracking.

Tracking mails basically only works within your own Notes/Domino environment.

4.3.1. Settings in the configuration document

In Domino Administrator, open the Configuration tab and select the view »Server« → »Configurations« on the left.



Create a new configuration document or open an existing one. Select the tab »Router/SMTP« → »Message Tracking«.

Important

Mail tracking must be enabled on **all** Domino Servers involved in the transfer of mail. Otherwise, tracking across multiple Domino Servers is not possible.

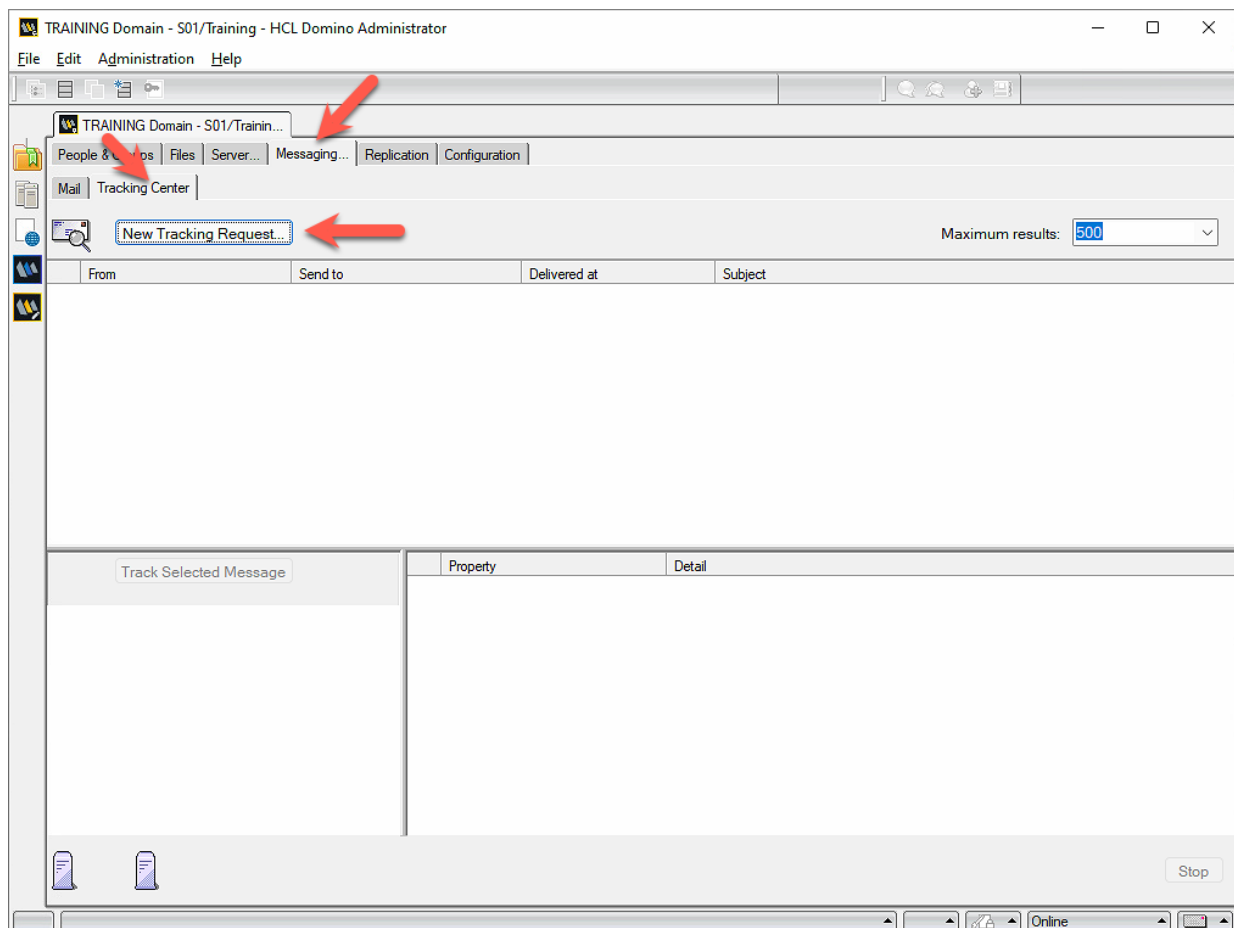
Save and close the configuration document.

Hint

After activating mail tracking, you need to restart the Domino Server. The folder »mtdata« is then created below the Data directory and the Domino MailTracker Store application (»mtstore.nsf«) is created in it.

4.3.2. Using mail tracking

In Domino Administrator, open the tab »Messaging...« → »Tacking Center«.

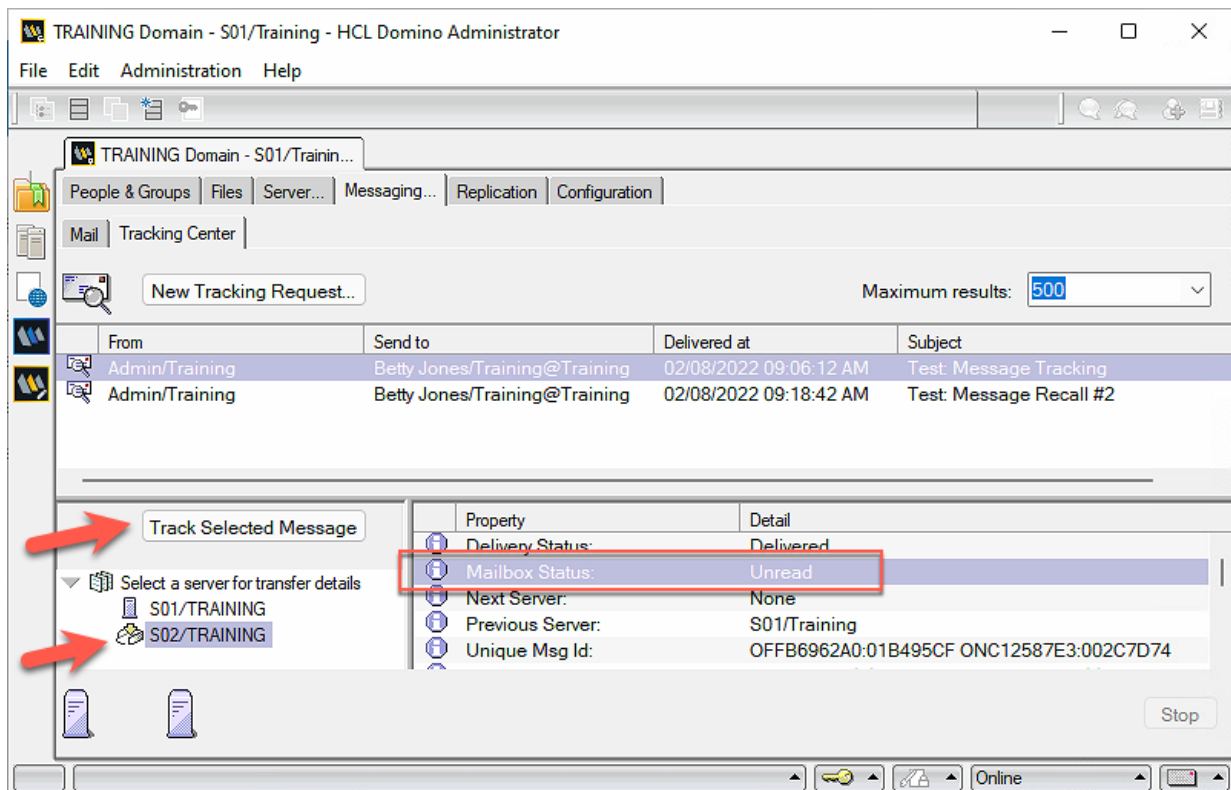


Click on the »New Tracking Request« button.

6. Message ID

Every mail that is routed via Domino Server receives a unique »Message ID«. However, this is only displayed on the Domino console (or in the LOG application) and is usually not available to an administrator.

Confirm the dialog with »OK«.



Select the desired mail and click the »Track Selected Message« button (or alternatively double-click directly on the mail).

In the lower left area you can click on the individual Domino Servers and many details about the mail are displayed on the right. The Domino Server »S02/Training« marked in the screenshot is displayed with a different icon than the previously listed servers, because it has finally delivered the mail in the user mailbox.

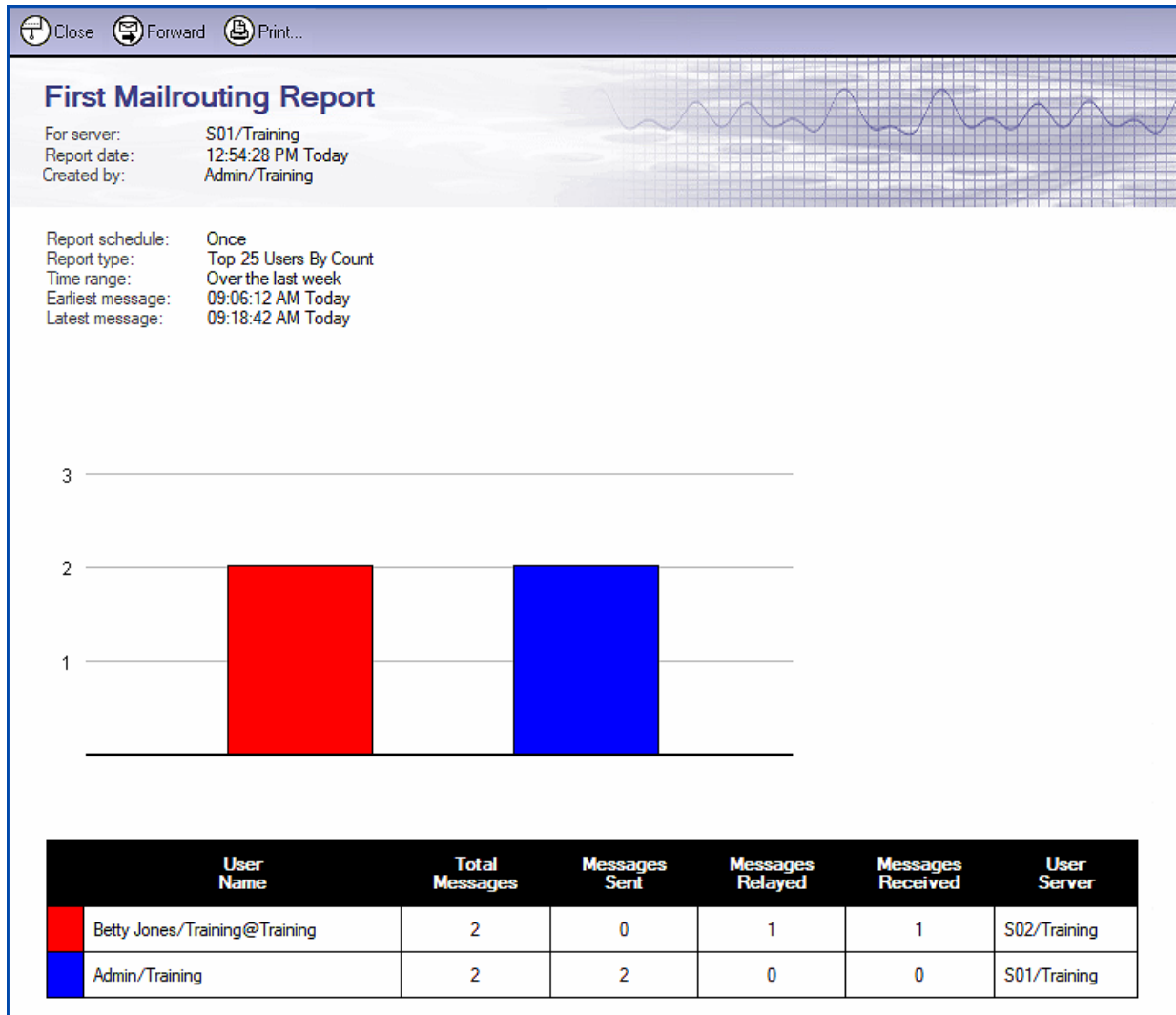
Hint

Especially for the final delivering Domino Server the »Mailbox Status« is interesting. Here, even the status »Deleted« is displayed if the user has deleted the mail.

In practice, this makes it easy to prove that the mail was delivered - if the user claims that he never received the mail.

On the »Basics« tab, in addition to a name, the parameters »Report Type«, »Time Range«, »Run this report« (one-time or recurring) and »Report should be« (the report is saved in the application or sent by mail) can be selected.

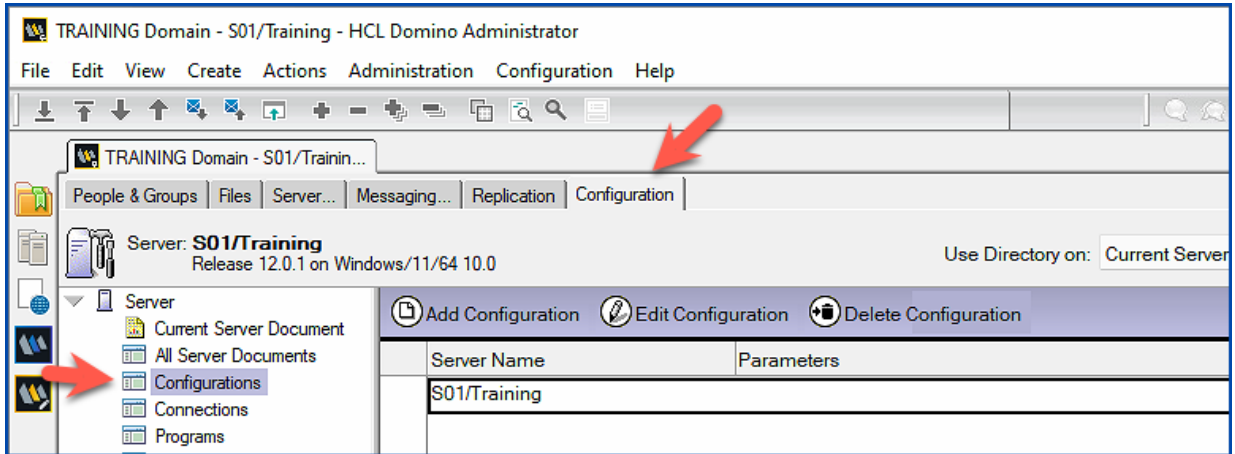
On the »Conditions« tab, filters can be activated according to the criteria »Sender's Name«, »Recipient's Name«, »Delivery Status« and »Message Size«.



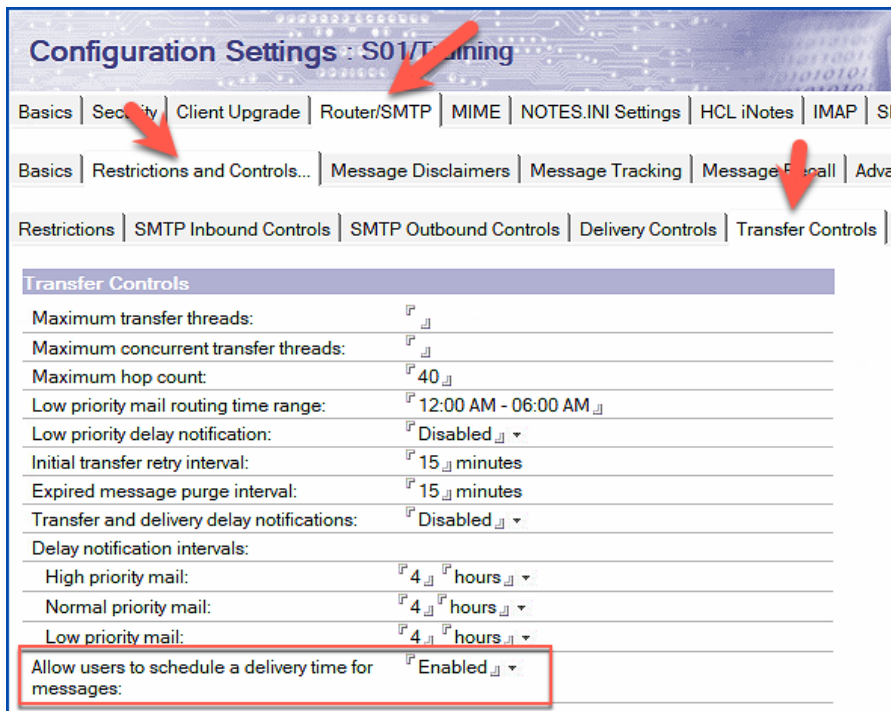
This is an example with the standard defaults. Feel free to try out other reports!

4.4.2. Setting in the configuration document

In Domino Administrator, open the tab »Configuration« and select the view »Server« → »Configurations« on the left.



Create a new configuration document or open an existing one. Select the tab »Router/SMTP« → »Restrictions and Controls...« → »Transfer Controls«.



You can enable or disable scheduled delivery in the »Allow users to schedule a delivery time for messages« field.

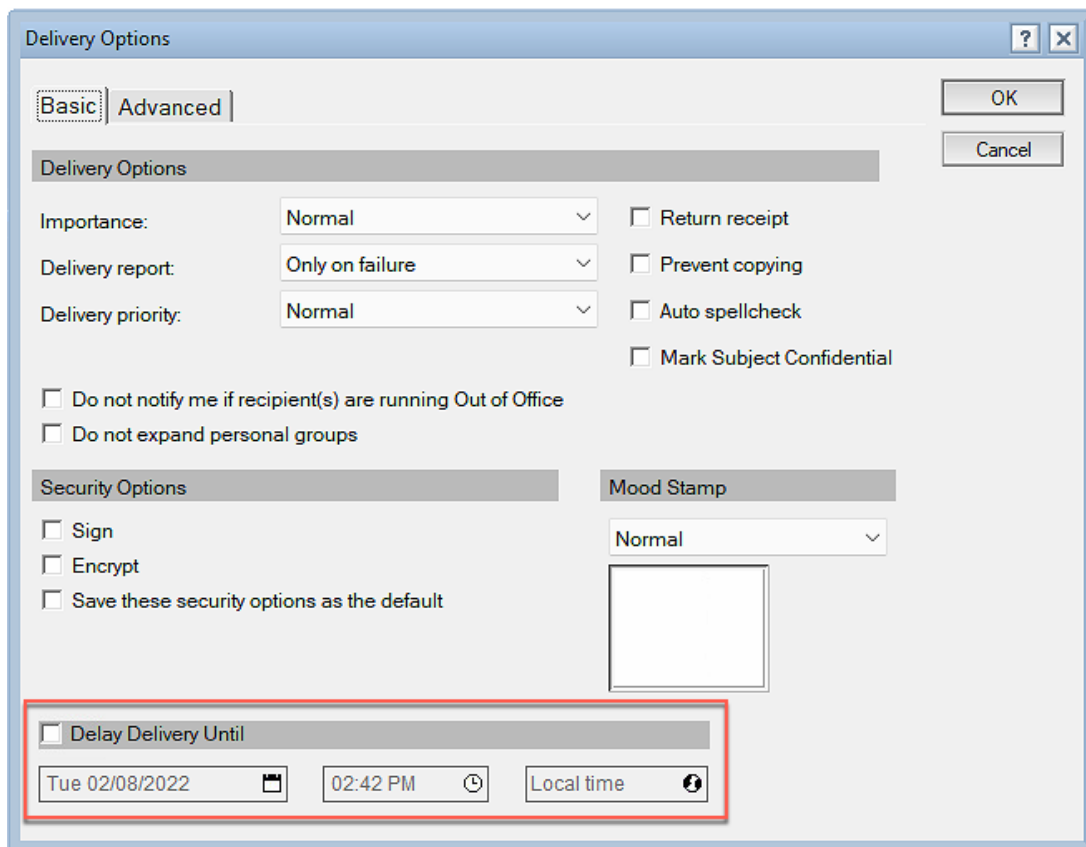
Hint

It can take up to 12 hours for a Notes Client to adopt this setting. For the change to take effect immediately, use the following command at the Domino Console:

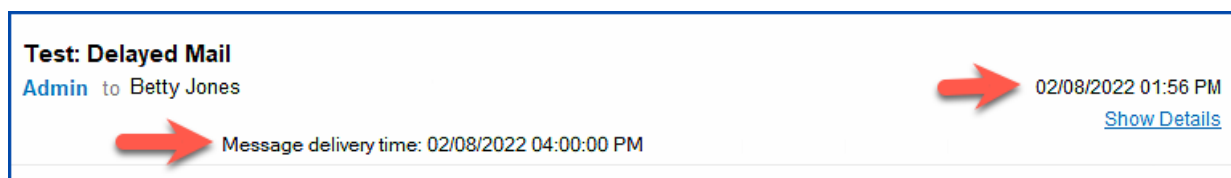
»tell admin process mailpolicy«

4.4.4. Using scheduled sending in the Notes Client

Provided that scheduled sending is active on a Domino Server, users can set a send time in the delivery options when creating a mail, a reply or forwarding mails.



Open a sent mail which has a sending time.



Sent mails show when the mail was created and when the sending time was scheduled.

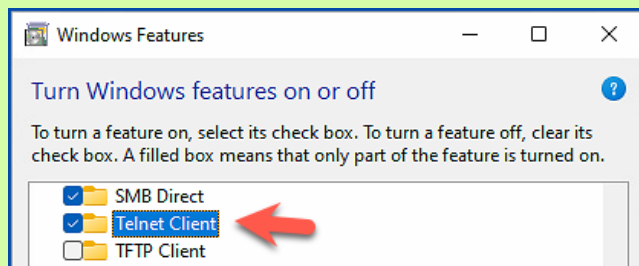
4.5.1.2. Functional test

You can perform a functional test by using the operating system's »telnet« command.

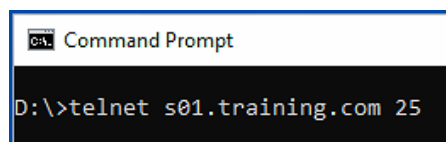
Hint

If your Windows operating system does not provide the »telnet« command, you must enable it as a »Windows Feature«.

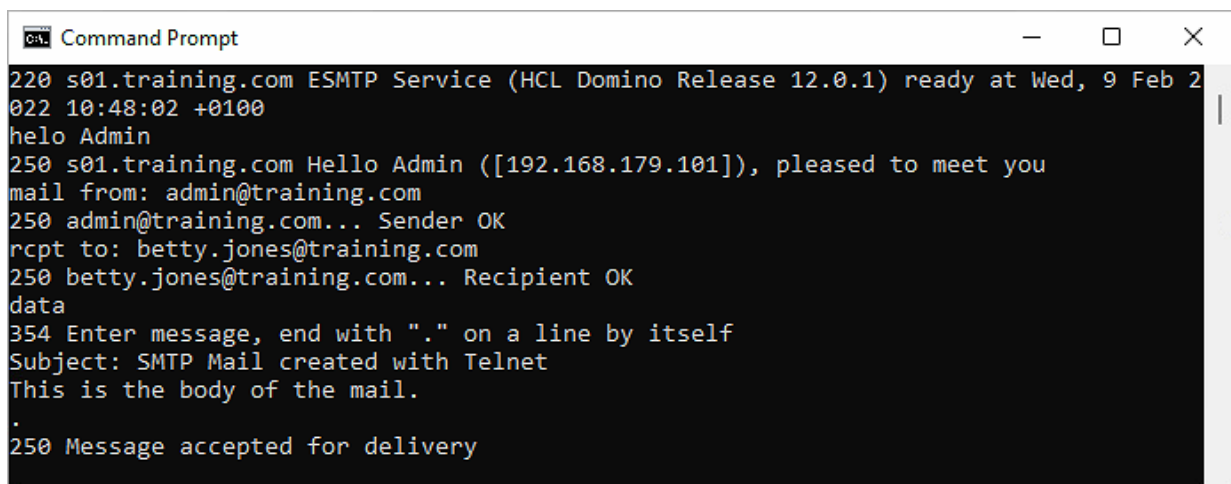
Enter »Feature« in the Windows search and then activate the »Telnet Client«.



Open a Windows command prompt.



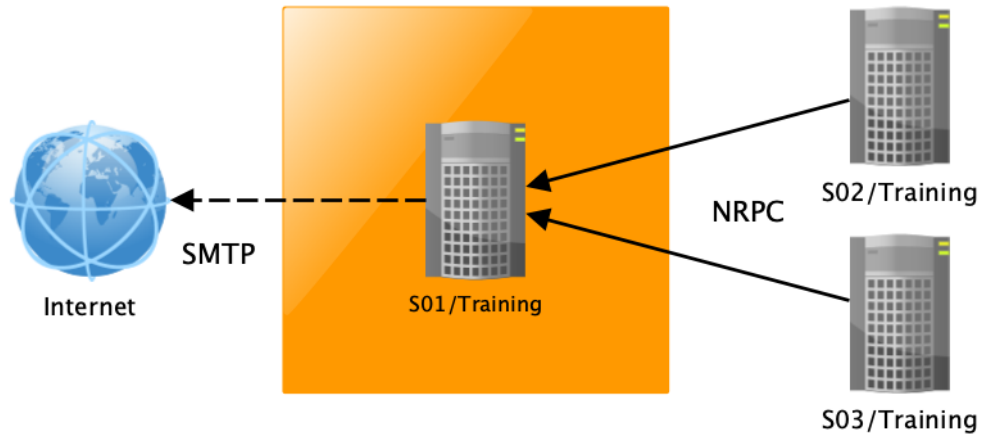
Enter the command »telnet s01.training.com 25«. A Domino Server always acts on port 25 for the SMTP protocol (this can be set in the server document).



Hint

The commands shown are documented for the SMTP protocol and can be easily found using an Internet search engine.

4.5.3. Outgoing SMTP mails when using multiple Domino Servers

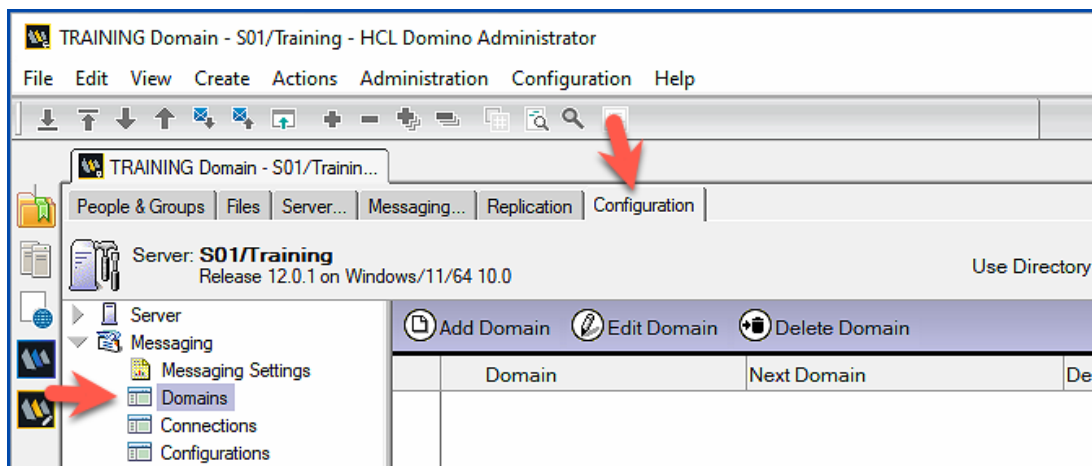


If a company operates several Domino Servers, outgoing SMTP mail routing is often only activated on one Domino Server (see previous chapter).

Other Domino Servers transfer SMTP mails for further delivery to this Domino Server (via Notes NRPC routing). For configuration 2 steps are required.

4.5.3.1. Domain document

In Domino Administrator, open the Configuration tab and select the view »Messaging« → »Domains« on the left.



Create a new or open an existing domain document. Select the »Basics« tab.

2. Domain name

Enter the freely selectable name of a fictitious domain here (the domain must not exist as a Domino domain).

If a Domino Server has recognized an SMTP mail, it tries to send this mail to the domain named here. This only works if a corresponding »SMTP connection document« (see next chapter) exists.

3. Internet host

As an alternative to the entry in the »Domain name« field, a host name or IP address can be entered in the »Internet host« field.

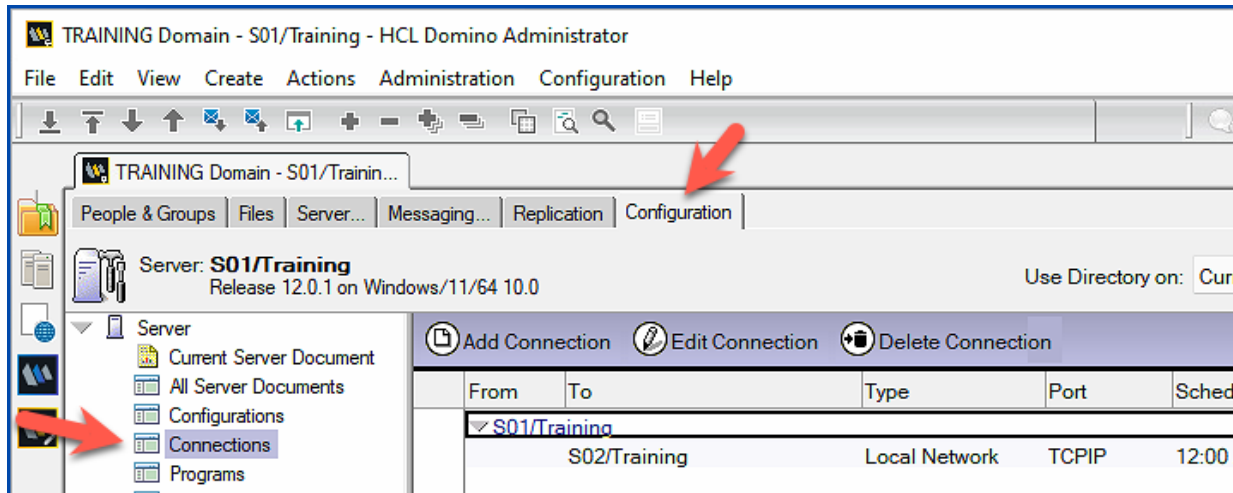
However, this means that each Domino Server will try to transfer its SMTP mails there. If all Domino Servers deliver their SMTP mails to a firewall, this is an additional option.

Save and close the document.

4.5.3.2. SMTP connection document

In order for the Domino Servers to know where to forward a mail addressed to the fictitious domain (see chapter Domain document), a connection document of type »SMTP« is required.

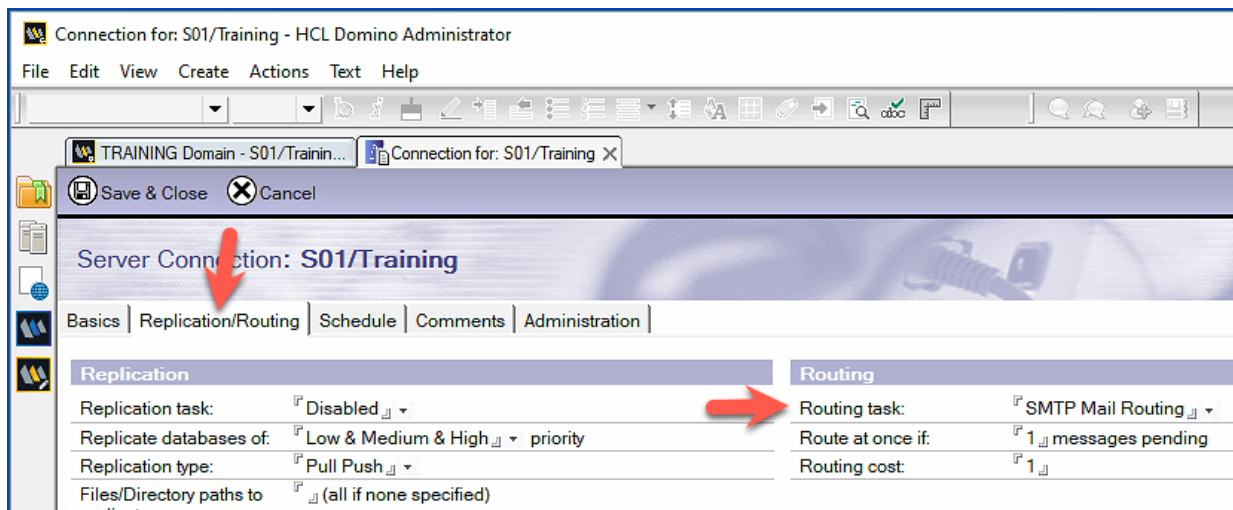
Open the »Configuration« tab in the Domino Administrator and select the view »Server« → »Connections« on the left.



Create a new connection document.

Hint
 I will discuss below only the tabs in the connection document relevant for SMTP routing. The other setting options (replication) are not relevant or already known to you.

Tab **Replication/Routing**



Only the »Routing Task« field is relevant here. Select the option »SMTP Mail Routing« there.

Save and close the connection document.

Hint

The SMTP routing in interaction of all Domino Servers will only work if all involved Domino Servers have received the documents via replication and have adopted the settings.

5.1. ODS (On Disk Structure)

5.1.1. What is the ODS?

The ODS (On Disk Structure) describes the inner structure of a Notes/Domino application. Over the various Domino versions, the ODS has been further developed, making it more powerful and robust.

The following aspects apply with regard to the ODS:

- **The ODS has no relation to the design of an application**
Changing the ODS does not affect the design elements located in the application. Similarly, changes to the design do not affect the ODS of an application. Current designs can also be saved in older ODS versions.
- **The ODS is not replicated**
If different ODS versions are used on different Domino Servers, this does not affect the replication of an application - during replication, the contents (documents, design and ACL) are matched, but the structure of the application is not changed.

What is the benefit of using a particular ODS version?

As an example I would like to mention the extensions of the ODS 51 (Domino version 8.5):

- **Compression of documents**
Documents (not file attachments) can be compressed - thus an application occupies less space in the file system.
- **Compression of design elements**
The size of an empty mailbox was about 30 MByte with Domino version 8.5. By compressing the design, the size can be reduced by almost 50%.
- **Use of DAOS** (Domino Attachment and Object Services)
Redundant file attachments in applications are consolidated - thus stored only once in the file system. This can save storage space in practice. For more detailed information, see the chapter [5.3. DAOS \(Domino Attachment and Object Services\)](#) on page [120](#).

Hint

The activation of a higher ODS version alone does not automatically activate most extensions.

The additional steps required are described in the following chapters.

5.1.3.2. Activation of ODS for existing applications

As soon as the parameter »Created_R12_Databases« is activated in the »notes.ini« file of the Domino Server, all new applications are created with the ODS 55.

Hint


For a newly installed Domino Server version 12, ODS 52 (Domino 9) is enabled by default. If you check this in the Domino Administrator on the »Files« tab, you will discover more applications and templates with older ODS versions.

Existing applications, on the other hand, must be converted using the »compact« command. The conversion to the new ODS only takes place if a »copy style« compression is performed and the parameter »-c« is used.

For example, to compact all user mailboxes available on the Domino Server (stored in the mail path below the data directory), use the following command at the Domino console.

```
load compact mail\ -c
```

Admin mailbox before the conversion:


	Title	Filename	Physical Path	File Format	Logical Size	Physical Size	Ma
	Admin	admin.nsf	D:\HCL\Domino\Data	R9 (52:0)	18,350,080	18,350,080	

Performing the conversion with a console command:

```
load compact mail\ -c

[230C:0004-11C0] 13.02.2022 08:25:24 Informational, database design compression is enabled in database mail
[230C:0004-11C0] 13.02.2022 08:25:24 Informational, LZ1 is enabled in database mail\admin.nsf.
[230C:0004-11C0] 13.02.2022 08:25:24 Compacting mail\admin.nsf (Admin), mail\ -c
[230C:0004-11C0] 13.02.2022 08:25:25 Compacted mail\admin.nsf, 256K bytes recovered (1%), mail\ -c
[230C:0002-0EE4] 13.02.2022 08:25:26 Database compactor process shutdown
```

Admin mailbox with the new ODS:

	Title	Filename	Physical Path	File Format	Logical Size	Physical Size	Ma
	Admin	admin.nsf	D:\HCL\Domino\Data	R12 (55:0)	18,350,080	18,350,080	