Backup and disaster recovery

Installation manual

for system providers and tenants

7/25/2025

Product line Neo, version 7.x

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at https://www.asctechnologies.com.

Copyright © 2025 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

ASC Technologies AG - Seibelstr. 2-4 - 63768 Hösbach - Germany

Contents

1 Introduction 5

2 Preconditions 6

3 Quick guide - Backup 7

3.1 Create snapshots in VMWare 7

3.2 Create database backup 7

3.3 Backup data directory 7

3.4 Read out machine ID 7

3.5 Back up CallPool 7

3.6 Read out system configuration 7

3.7 Backup speech analysis server 7

4 Backup - step-by-step instructions 8

4.1 Create database backups 8

4.1.1 PostgreSQL database 8

4.1.1.1 Backup of the database 8

4.1.1.2 Backup of the configuration files 10

4.1.2 MSSQL database 11

4.1.2.1 Backup of the MSSQL database 11

4.2 Backup data directory 15

4.3 Read out machine ID 16

4.4 Back up CallPool 16

4.5 Read out system configuration 16

4.6 Backup EML speech analysis server 17

5 Failure scenarios 19

6 Quick guide - Recovery 20

6.1 Install recording server again 20

6.2 Restore of PostgreSQL database 20

6.3 Restore of MSSQL database 21

6.4 Import certificates 21

6.5 Rebuild conversations 21

7 Exchange drive 22

8 Restore of EML speech analysis server (optional) 23

9 Recovery - step-by-step instructions 24

9.1 Download and deployment 24

9.2 Recovery of the recording software 24

9.3 Restore of database 25

9.3.1 Restore PostgreSQL database 25

9.3.1.1 Apply configuration data 26

9.3.1.2 Restore of the PostgreSQL database 26

9.3.1.3 Updater 29
9.3.2 Restore MSSQL database 30
9.3.2.1 Restore of the MSSQL database 30
9.3.2.2 Updater 32
9.4 Conclusive steps 33
9.4.1 Import certificates 33
9.5 Rebuild of recordings 34
9.5.1 Configure import job 34
9.5.1.1 Tab Details 35
9.5.1.2 Tab Drives 36
9.5.2 Verifying functionality 37
9.6 Rebuild of recordings without database backup 38
9.6.1 Configure import job 38
9.6.1.1 Tab Details 39
9.6.1.2 Tab Drives 40
9.6.2 Verifying functionality 42
9.7 Rebuild Solr Database (optional) 42
Glossary 45
Index 46

1 Introduction

This manual describes the preconditions and the procedure to create backups and to recover data after a partial or total failure of the system.

ASC offers different possibilities to backup the data of a Neo system before a failure. It does not matter which recording architecture you use or whether you deploy a single- or a multi-core system. The following backup scenarios can be used with all architecture types and core variants.

In general, you have to distinguish between the following terms:

- *Backup of recordings*
  This is the communication data itself (audio, video, screen or chat). This data is stored on external media for long-term data storage.
- *Backup of metadata*
  This is the additional data corresponding to the calls. It is saved in the database and can be stored long-term by means of the database backup.
- *Backup of the system configuration*
  This is a backup of the entire configuration of the application *System Configuration* contained in a database backup.

Solution concept

For PostgreSQL databases, a backup job is set up during the installation of the Neo recording software which backs up the PostgreSQL database every 24 hours. As many as five complete backups are stored before the oldest backup is overwritten. This guarantees that the latest database backups of the last 5 days are available. These backups are stored in the directory `\ASCDATA\DatabaseBackup`. By configuring an automatic copy job to external drives, e. g. to a backup server in the customer environment, backups can be saved separately. This solution safeguards the database until the latest backup.

For external MSSQL databases, you must set up a backup job manually.

Possible gaps from the latest backup to the latest recording can be filled with the import functionality Neo Rebuild. See chapter "Rebuild of recordings", p. 34 orchapter "Rebuild of recordings without database backup", p. 38.

The restore should definitely be carried out by an authorized ASC service technician. Contact your local ASC support or call ASC support at +49 700 27278776.

2 Preconditions

For the recovery of the recording system, the following information must be available:

- *System ID and order number*
  This additional information can be found in the application System Configuration by clicking on the icon at the top left. Select the menu item *Info* in the context menu. By clicking on the button *Additional Information* at the bottom right, a window opens which contains the *License Information*.
- *Machine ID of the affected servers*
  either by means of the registry key
  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ASC\Common\machineId`
  or by means of the file name of the backup log file: `\ASCDATA\DatabaseBackup`, see chapter "Read out machine ID", p. 16.
- *Backup of the data directory*
  `C:\Program Files (x86)\ASC\ASC Product Suite\data`, see chapter "Backup data directory", p. 15.
- *Backup of the database*, see chapter "Create database backups", p. 8.
- *Backup of the call data partition with the recordings*
  `\ASCDATA`, see chapter "Back up CallPool", p. 16
- *Backup of the system configuration for script adaptions by ASC*, see chapter "Read out system configuration", p. 16.

3 Quick guide - Backup

3.1 Create snapshots in VMWare

Snapshots of virtual systems serve to back up the status quo before maintenance or software updates. Using a snapshot only makes sense if it is up to date and created after business hours as all services must be stopped.

Do not try to create a snapshot while operating the system. You have to shut down all applications before creating a snapshot. After a successful check of the system functions after the update, delete the snapshots! Otherwise the snapshots affect the performance of the IO activities in this VM which may cause an unpredictable system behavior or even system failures.

3.2 Create database backup

1. Create database backup, see chapter "Create database backups", p. 8.

3.3 Backup data directory

1. Backup data directory,
   `C:\Program Files (x86)\ASC\ASC Product Suite\data`
   see chapter "Backup data directory", p. 15,

3.4 Read out machine ID

1. Read out machine ID
   by means of the registry key
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ASC\Common\machineId`
   or by means of the file name of the backup log file of the PostgreSQL database
   `\ASCDATA\DatabaseBackup`
   see chapter "Read out machine ID", p. 16.

3.5 Back up CallPool

1. Back up CallPool
   `\ASCDATA\CallPool`
   see chapter "Back up CallPool", p. 16.

3.6 Read out system configuration

1. Read out system configuration, see chapter "Read out system configuration", p. 16.

3.7 Backup speech analysis server

1. For systems working with EML speech analysis, you must backup the relevant files and directories for the decoder and for the server.
   see chapter "Backup EML speech analysis server", p. 17

4 Backup - step-by-step instructions

After an installation and after changes in the configuration, create the following backups to be able to fall back on them in case of a failure.

Take a written note of the entire number of the version which has been installed. A restore can only be carried out successfully with the same or a higher version.

4.1 Create database backups

Create a database backup to fall back on in case the database is defective or corrupted.

To create a backup, select the chapter corresponding to the database you are using and follow the instructions.

- See chapter "PostgreSQL database", p. 8.
- See chapter "MSSQL database", p. 11.

4.1.1 PostgreSQL database

During the installation of the provided PostgreSQL database der Neo-recording software, a backup job is created for the PostgreSQL database which covers the database backups of the last 5 days (default value).

By default, you find the files in the following directory:

- `%ASCDATA%\DatabaseBackup\`

The retention time for the backups of the PostgreSQL database (default value: 5 days) can be changed by means of the administration tool for the database, if required.

Move the backup to a separate drive so that you can access it in case of an error.

For information about customer-specific non-standard settings of the backup job for PostgreSQL databases (e. g. the path of the database backup or the number of local or remote database backups) refer to the description of entries in the main view of the administration manual for system providers *System Configuration - Expert Settings*.

4.1.1.1 Backup of the database

To create a backup of the PostgreSQL database, the PostgreSQL server must be running.

The following configuration has to be carried out as *postgres* windows user.

A script is available for creating a backup for the content of the PostgreSQL database.

1. Open the command prompt as administrator.
2. Change to the directory `C:\Program Files (x86)\ASC\ASC Product Suite\scripts`.
3. Enter *database backup* to execute the script *database.bat*.
4. Once the backup has run through properly, you find the backup file with the current date in the following path:
   `\ASCDATA\DatabaseBackup`
5. Check the size of the backup file. It must be approximately 20-30 % of the database.

4.1.1.1.1 Save backup directly on a network drive

To save the backup of the database directly on a network drive, you must create a system variable in the settings of the system where you save the path.

1. Open *System Control*.
2. Select the entry *System and Security* > *System*.

3. Click on the button *Advanced System Settings*.
   ⇨ The window System Properties opens.

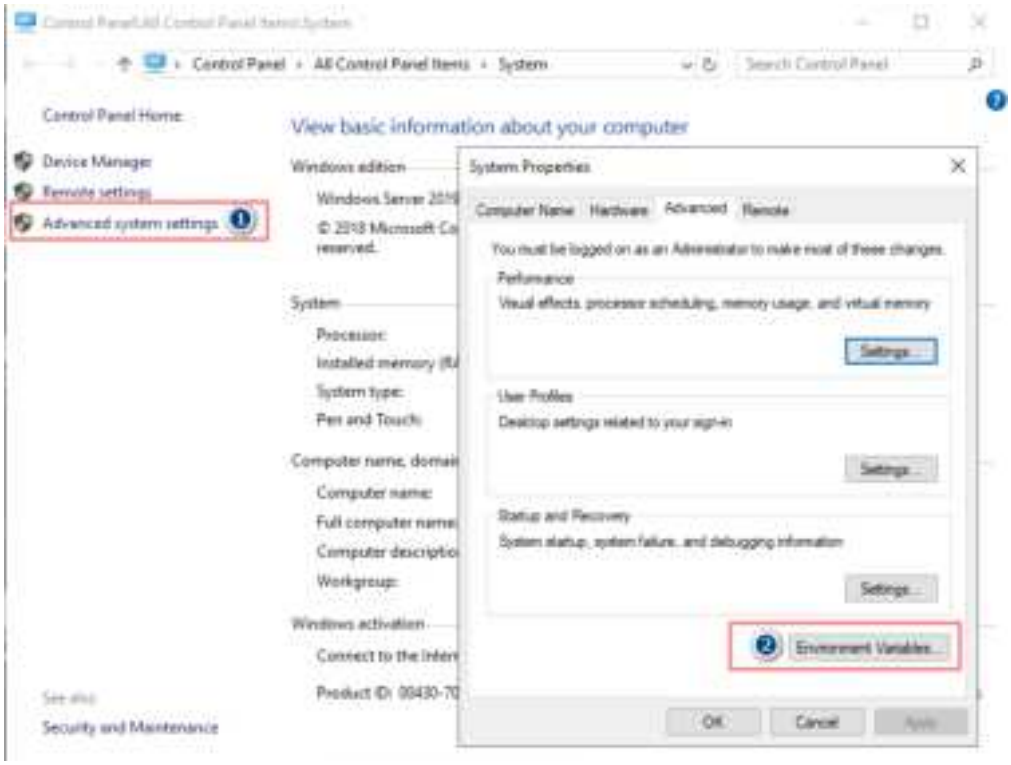

Fig. 1: System settings - Advanced settings - Open environment variable

4. Click on the button *Environment Variables*.
   ⇨ The window Environment Variables opens.

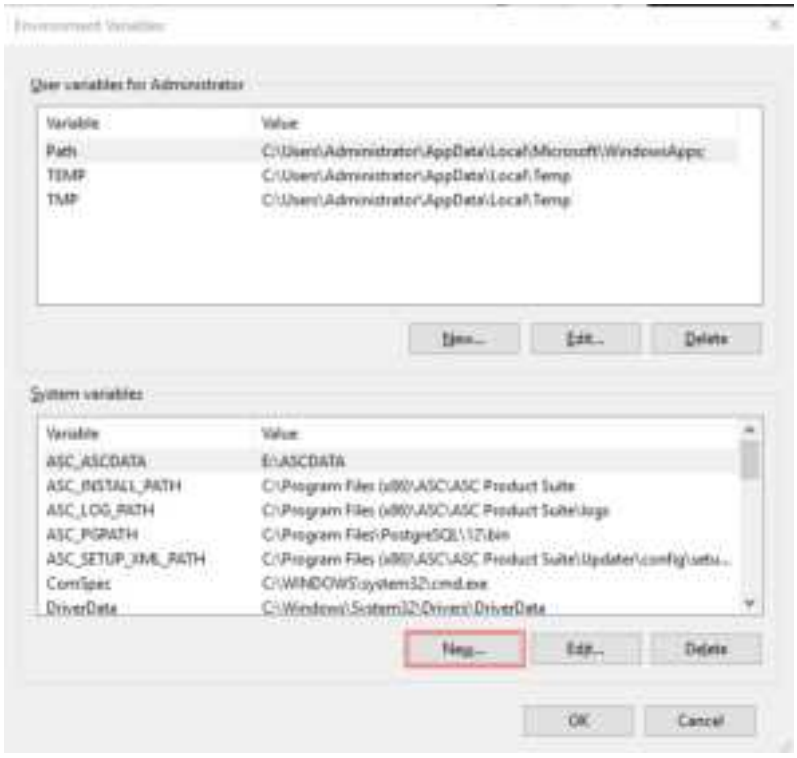

Fig. 2: System settings - Create new system variable

5. In the group field *System Variables*, click on the button *New*.
   ⇨ The dialog to configure the system variable opens.

Fig. 3: System settings - Name system variable and enter storage path

6. Enter the name for the variable, e. g. *ASC_PGBACKUPPATH*.
7. Enter the storage location for the backup or select the directory by clicking on the button *Browse Directory*. As path, you can either use the attached network drive or the UNC path name,
   e. g. `\\mybackuplocation\DBBACKUP`.

Please note that the Windows user *Postgres* must have read and write permissions for the directory so that the backup can be saved there.

8. Click on the button *OK* to save the entries and close the window.
   ⇨ The system variable appears in the list of system variables.

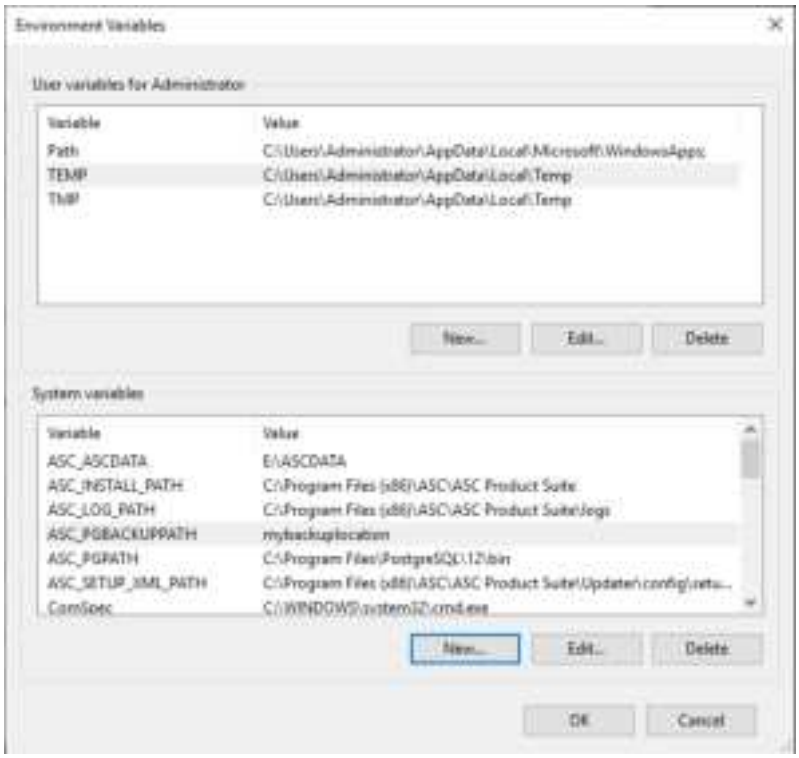

Fig. 4: System settings - Create system variable (example)

9. Click on the button *OK* to save the configuration.

4.1.1.2 Backup of the configuration files

NOTICE! The configuration files of the database are not backed up with the script.

1. To avoid extra configurations, make sure to separately back up the following configuration files at the beginning and after all changes:
   - *<<POSTGRES-DATA-FOLDER>>\pg_hba.conf*
   - *<<POSTGRES-DATA-FOLDER>>\postgresql.conf*

NOTICE! When using a failover database, back up the configuration files of the standby database, too.

For information about configuring a failover concept for databases and resetting failover operation refer to the installation manual for system providers *Failover operation for PostgreSQL databases*.

4.1.2 MSSQL database

4.1.2.1 Backup of the MSSQL database

1. Click on the Windows button.
2. Click on the arrow icon to display all programs.
3. Open the *Microsoft SQL Server Management Studio* and log in.

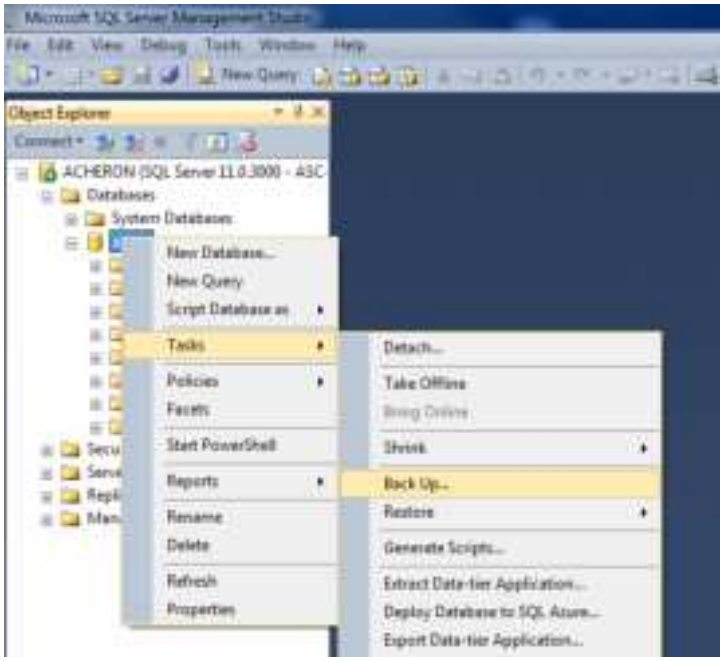

Fig. 5: Object explorer

4. Select the database *Databases* > *asc_rs* from the directory tree.
5. Right-click on the database *asc_rs*.
6. Select the menu item *Tasks* > *Back Up* from the context menu.
   ⇨ The following window appears:

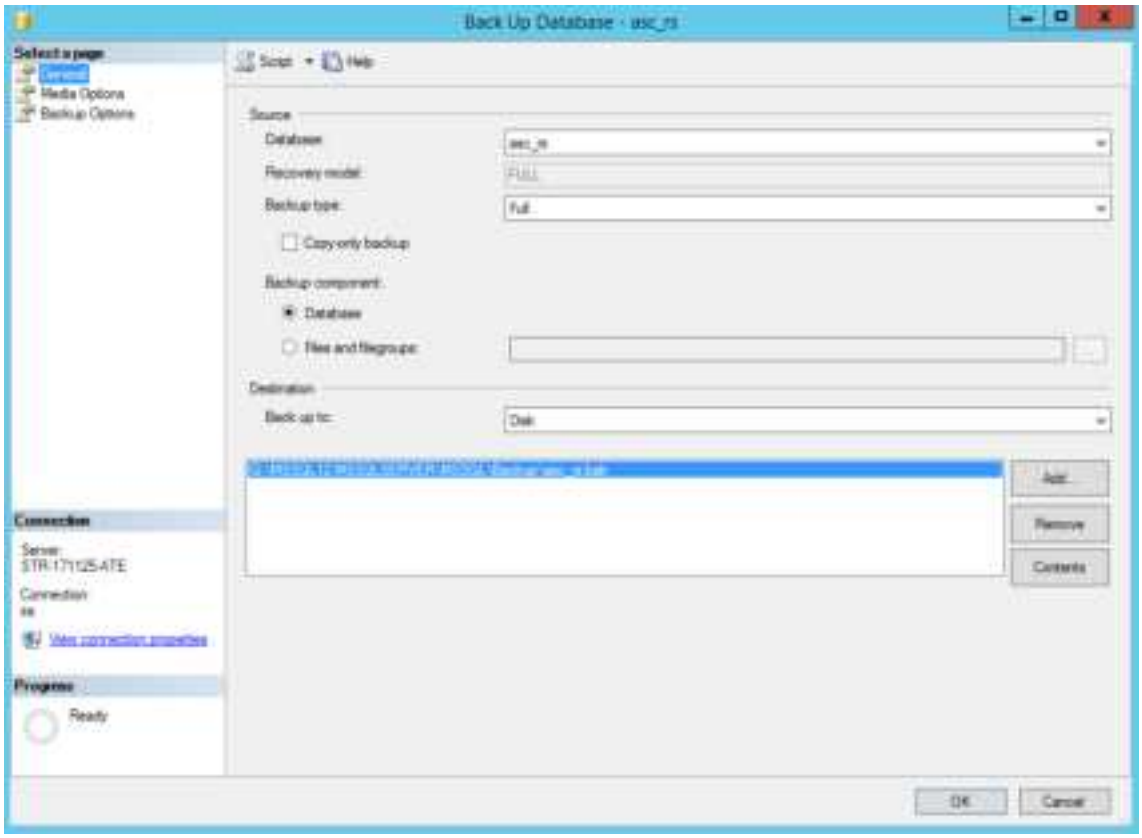

Fig. 6: Configure general backup options

7. Click on the menu item *General* in the navigation bar.
8. Select the following parameters:

Group field Source

Database	asc_rs
Backup type	full
Backup component	Database

Tab. 1: Configure backup options

Group field Destination

Back up to	From the drop-down list, select the medium on which you would like to store the backup. • *Disk* • *URL*

Tab. 2: Configure backup options

1. To change the path or add an additional one, click on the button *Add*.
   To remove a path, click on the button *Remove*.
2. To display the content of the path with the completed backup files, select the target path and click on the button *Contents*.

For information about other backup possibilities see
http://msdn.microsoft.com/en-us/library/ms187510.aspx.

3. Click on the menu item *Media Options* in the navigation bar.
   ⇨ The following options appear:

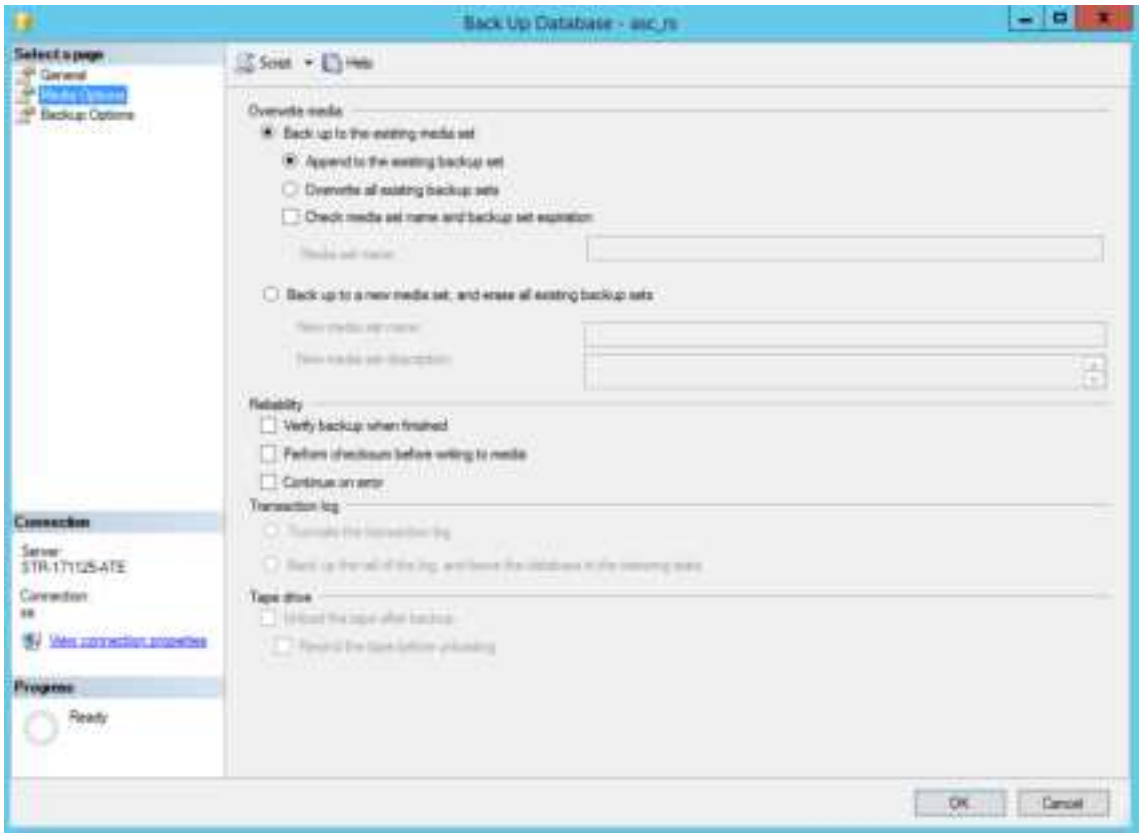

Fig. 7: Configure additional backup options

Group field Overwrite media

1. Select the way the backup is supposed to be saved.

◉ *Back up to the existing media set* By activating this option, you add the following options to the existing backup:	
	◉ *Append to the existing backup set* By activating this option, you attach the backup to the existing one.
	○ *Overwrite all existing backup sets* By activating this option, you overwrite all previous backups.
	☑ *Check media set name and backup set expiration* When activating this option, the entry field *Media set name* becomes active and you can enter a name for the media set.
○ *Back up to a new media set, and erase all existing backup sets* By activating this option, you delete all previous backup files and create a new backup set.	
	New media set name: Enter a name for the new media set.
	New media set description: Enter an optional description of the new media set.

Tab. 3: Options to overwrite medium

Group field Reliability

☑ *Verify backup when finished*	
	Activate this option if the completed backup is supposed to be subject to a check.

☑ *Perform checksum before writing to media*	
	Activate this option if a checksum is supposed to be reckoned up before writing the backup on the medium.
☑ *Continue on error*	
	Activate this option if you want to create a backup despite possible errors.

Tab. 4: Configure reliability

Group field Transaction log

This option is not active.

○ *Truncate the transaction log*	
○ *Back up the tail of the log, and leave the database in the restoring state*	

Tab. 5: Configure transaction log

Group field Tape drive

These options are not active if you have selected a hard disk as target for the backup on the *General* page.

☑ *Unload the tape after backup*	
	☑ *Rewind the tape before unloading*

Tab. 6: Configure tape drive

1. Click on the button *OK* to save the configuration.
2. Click on the menu item *Backup Options* in the navigation bar.
   ⇨ The following options appear:

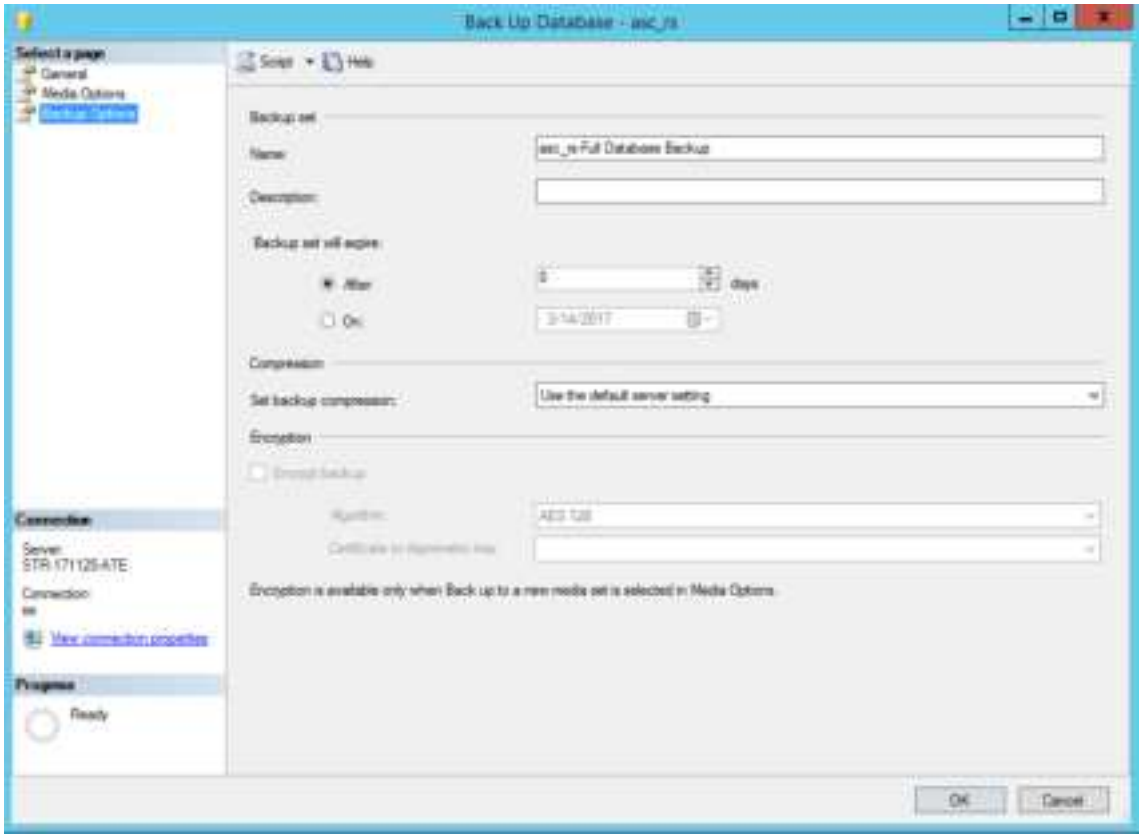

Fig. 8: Configure additional backup options

Group field Backup set

Name	Enter the name of the backup file.	
Description	Optional entry field	
Backup set will expire	Activate the option field.	
	◉ After:	Use the arrow keys to select the number of days until the backup set will expire.
	○ On:	Select the exact date in the calendar on which the backup set will expire.

Tab. 7: Configure file options

Group field Compression

Set backup compression:	Select the compression from the drop-down list. The following options are available: • *Use the default server settings* • *Compress backup* • *Do not compress backup*

Tab. 8: Configure compression

1. Click on the button *OK* to create the backup.

⇨ Once the backup has been completed, the following notification appears:

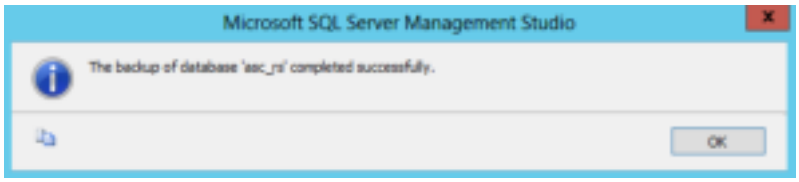

Fig. 9: Notification

You find the backup file in the previously defined path.

4.2 Backup data directory

Backup the data directory on a daily basis by saving a copy on a separate medium.

```
C:\Program Files (x86)\ASC\ASC Product Suite\data
```

The directory contains all customer-specific adjustments.

- *Keystore key*

  When Neo key management is used, this directory contains the subdirectory *Dongle Manager*.

  This directory contains the database where the keystore and the password have been saved.

- *Adjustment of the configuration files*

  The directory for the modules contains e. g. settings for connection timeouts, failover, recording, and deletion behaviors.

- *Volume IDs*

  In the directory Fileman, information about the device IDs has been saved. If a drive is exchanged and receives the save drive letter again, then the FileMan can assign the IDs again. For successful assignment, the data directory must be available when the FileMan is started. Otherwise, the FileMan creates new IDs.

4.3 Read out machine ID

The machine ID of a server is an unambiguous identifier. As all internal links depend on this machine ID, it is mandatory to use this machine ID in new installations. Consequently, read out the machine IDs of every server directly after the installation of the software and ensure that the information is saved separately to have access in case of an error.

Machine ID	*- Identifies the server* You find the information about the machine ID either • *in the file name of the backup log file of the PostgreSQL database which is saved by default in the following directory:* `\ASCDATA\DatabaseBackup` or • *in the registry in the following path:* `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ASC\Common`

4.4 Back up CallPool

The CallPool contains the recordings of all tenants. By backing up this directory, you will be able to restore configuration data in case of an error.

1. Consequently copy the entire data directory to a separate medium to have access in case of an error.
   `\ASCDATA\CallPool`

A program enables you to scan the CallPool you have backed up and to read out the IDs. The information is issued in a CSV file and can be processed by ASC.

In case of a complete system failure without an available database backup, contact your local ASC support or call ASC support at +49 700 27278776. ASC can create a script based on this file which allows mapping the IDs to the tenants and PBXs.

4.5 Read out system configuration

Directly after the installation and configuration of a customer system, you can read out the system configuration by means of a program. If your system fails completely and no database backup is available, you can send ASC the file containing the information that has been read out.

If you have backed up the CallPool, you can deploy the program for the backup of the CallPool in case of a system failure, too, in order to read out the system configurations.

You call up this program by indicating the path of the CallPool or of the medium. By doing so, the directory tree is searched. From the found files, the PBX ID with the corresponding agent ID or extension is determined. If a new ID is found, it is issued together with the PBX ID in a CSV file. This information allows mapping the ID to the PBX.

ASC can create a script based on this CSV file which allows mapping the IDs to the tenants and the PBXs.

The program has to be run for each CallPool separately.

The scan can be canceled if required.

You can run the program again and back up information whenever you have made changes in the system.

1. In the command line *cmd* run the program *ASC.RecordingControl.exe* by entering the following syntax:

```
ASC.RecordingControl.exe --rebuild_scan [-l|-c] <path>
```

```
-l issues the currently scanned path by way of information.
-c creates the CSV file rebuild_scan.csv containing the scan results


Example:
ASC.RecordingControl.exe --rebuild_scan -l -c "\ASCDATA\CallPool"

Issued:
Scan dir C:\ASCDATA\CallPool
Scan dir C:\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant
Scan dir C:
\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant\YEAR_2015
Scan dir C:
\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant\YEAR_2015\MO
NTH_11
Scan dir C:
\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant\YEAR_2015\MO
NTH_11\DAY_21
Scan dir C:
\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant\YEAR_2015\MO
NTH_11\DAY_21\HOUR_08
TenantId 90b3db81-6442-46d5-9dbf-66a3d550dc41 8f431766-2a3e-4f52-9f14-
afa2a4b45a7b:6001 8f431766-2a3e-4f52-9f14-afa2a4b45a7b:6000
Scan dir C:
\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant\YEAR_2015\MO
NTH_11\DAY_23
Scan dir C:
\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.AscTenant\YEAR_2015\MO
NTH_11\DAY_23\HOUR_15 93976f3a-c0df-4736-a550-2dad40c69368:6001

CSV content: in the example, no PBXAgentId could be found.
TenantId,PBXId,Extension,PBXAgentId
90b3db81-6442-46d5-9dbf-66a3d550dc41,8f431766-2a3e-4f52-9f14-
afa2a4b45a7b,6001,,
90b3db81-6442-46d5-9dbf-66a3d550dc41,8f431766-2a3e-4f52-9f14-
afa2a4b45a7b,6000,,
90b3db81-6442-46d5-9dbf-66a3d550dc41,93976f3a-c0df-4736-
a550-2dad40c69368,6001,,
```

The file *rebuild_scan.csv* can be found in the directory
`C:\Program Files (x86)\ASC\ASC Product Suite\modules\RecordingControl`.

Contact your local ASC support or call ASC support at +49 700 27278776 and provide the file *rebuild_scan.csv*.

4.6 Backup EML speech analysis server

For systems using EML speech analysis, you must backup the following files and directories for the decoder and the server:

Backup decoder:

1. Change to the path
   `C:\Program Files\EML\emlDecoder`
   and backup the file *decoder.properties*.

Backup transcription server:

1. Change to the path
   `C:\ProgramData\EML\TranscriptionServer\`
   and backup the entire directory *streaming_config*.
   The directory is relevant for KWS and real time, too.
2. Change to the path
   `C:\Program Files\EML\TranscriptionServer\wildfly\bin\Service`.
   and backup the file *service_config.bat*.
3. Change to the path
   `C:\ProgramData\EML\TranscriptionServer`
   and backup the file *transcription-server.raw.txt*.

In case of a total failure, you can copy these backups back to the respective paths after having reinstalled the EML components.

When updating the EML software, the EML setup automatically updates the decoders.

When updating the transcription server, you must install the backups manually.

5 Failure scenarios

In the following, you find possible approaches to different failure scenarios.

- *Complete system failure*,
  if the hard disk is defective and you have to set up the recording server from scratch, see chapter "Recovery of the recording software", p. 24
- *Database is corrupted or defective*,
  if the database is corrupted or defective and you have to restore it from a backup see chapter "Restore of database", p. 25
- *Last recordings are missing*,
  if there is a gap between the latest backup and the current recordings, see chapter "Rebuild of recordings", p. 34
- *Drive is defective*,
  if you have to exchange a drive and use the original letter of the drive, see chapter "Exchange drive", p. 22

6 Quick guide - Recovery

6.1 Install recording server again

1. In the Windows Explorer, navigate to the directory in which the ISO image is located.
2. Mount the ISO image as a drive by double-clicking.
3. In the start menu, open the command line prompt as administrator.
4. Change in the command line prompt to the directory in which the ISO image is located.
5. Enter the following command to start the setup in recovery mode:
   `setupx.x.x-x.x.exe /asc recovery_mode`
   See also chapter "Recovery of the recording software", p. 24.
6. Follow the installation routine.
7. In the entry dialog, enter the current *Machine ID* as machine ID.
   ⇨ The following message appears:
   `"Recovery mode detected. Restore data directory, data partition and database. Then restart the system and start` Updater!"
8. Confirm the message.
   ⇨ The prompt to restart of the server appears.
9. **Do not restart the server yet!**
10. If you use Neo key management and the Dongle Manager on the original server has been deployed, you must install the Dongle Manager on the new system. After the installation you must stop the service ASC DongleMan.
11. Install the backup of the following directories:
    `\ASCDATA` and
    `\Program Files (x86)\ASC\ASC Product Suite\data`.

    NOTICE! The backup of these directories contains the password for the Neo key management, if deployed.

6.2 Restore of PostgreSQL database

The program *pgAdmin* requires a password. Contact your local ASC support or call ASC support at +49 700 27278776 for your password.

1. Open the program *pgAdmin*.
2. Log in.
3. Create a new database with the name `asc_rs`.
4. Install the backup of the configuration files in the database path:
   `\ASCDB\pg_hba.conf`
   `\ASCDB\postgresql.conf`
5. Install the database backup,
   see chapter "Restore PostgreSQL database", p. 25.
6. Restart the server now!
7. After restarting the server, mount the ISO image again with a double-click so that the Updater can access it.
8. Start the Updater in the installation directory with the following command
   `updater.exe --open`, see chapter "Updater", p. 29.
9. Restart the server again once the update has run through.

10. Proceed with the conclusive steps,
see chapter "Conclusive steps", p. 33.

6.3 Restore of MSSQL database

1. Open the program *Microsoft SQL Server Management Studio*.
2. Create a new database with the name `asc_rs`.
3. Install the database backup,
see chapter "Restore MSSQL database", p. 30.
4. Restart the server now!
5. After restarting the server, mount the ISO image again with a double-click so that the Updater can access it.
6. Start the Updater in the installation directory with the following command
`updater.exe --open`, see chapter "Updater", p. 29.
7. Restart the server again once the update has run through.
8. Proceed with the conclusive steps,
see chapter "Conclusive steps", p. 33.

6.4 Import certificates

1. To enable an encrypted connection, you must reimport the certificates, see chapter "Import certificates", p. 33.

6.5 Rebuild conversations

1. Carry out the import job XXX to fill the gap from the latest database backup to the most recent recording,
see chapter "Rebuild of recordings", p. 34.
2. Check the replay of the conversations.

⇨ Now, the recovery is complete.

7 Exchange drive

If a drive is defective and you have to exchange it, proceed as follows to move the CallPool:

1. Open the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts* and stop all ASC services with the command *stop.all*.
2. Add a new partition or drive and assign a temporary drive letter.
3. Copy or relocate the directory `\ASCDATA` to the new partition.
4. Remove the previous partition so that the drive letter is available again.
   NOTICE! It is not sufficient to just rename the partition.
5. Assign the drive letter which is now available again to the new partition.
6. Start the service *ASC ServiceMan* so that it starts all other services.
7. Check that all services are running and start services which have not started yet manually.
8. Start the recording.
9. Check that recordings can be replayed correctly.

8 Restore of EML speech analysis server (optional)

For systems using EML speech analysis, you must copy back the following files and directories after the restore for the decoder and the transcription server:

Restore decoder:

1. Copy the backup of the file *decoder.properties*
   back to path
   `C:\Program Files\EML\emlDecoder`

Restore transcription server:

1. Copy the backup of the directory *streaming_config*
   back to path
   `C:\ProgramData\EML\TranscriptionServer\`.
2. Copy the backup of the file *service_config.bat*
   back to path
   `C:\Program Files\EML\TranscriptionServer\wildfly\bin\Service`.
3. Copy the backup of the file *transcription-server.raw.txt*
   back to path
   `C:\ProgramData\EML\TranscriptionServer`.

When updating the EML software, the EML setup automatically updates the decoders.

When updating the transcription server, you must install the backups manually.

9 Recovery - step-by-step instructions

During a restore, you must use the same drive letters that have been used during the initial installation.

9.1 Download and deployment

1. In the ASC Partner Portal (https://partner.asc.de/), you can find the released software packages for download.
2. In the area *Software* > *neo suite*, open the corresponding directory, e. g. *NEO 7.3*.
3. Download the ISO image and the corresponding md5 file or the ZIP file.
4. In the area *Software* > *Tools* > *MD5-Checksum*, you will find the script `checksumcheck.ps1` to check the integrity of the downloaded file. By means of this script, you can compare the checksum of the ISO image with the value in the md5 file and thus check it for completeness and functionality.
5. Download the script, too, and save it in the folder where the ISO image and the md5 file have been saved.
   NOTICE! There must be no other files in the directory.
6. Right-click on the file `checksumcheck.ps1` and select the function *Execute with Powershell* in the context menu.
   ⇨ Powershell will subsequently display the check result. If the check fails, download the ISO image again.
   ⇨ If the result is correct, you can start the installation.

In the Windows Explorer mount the ISO image as a drive by double-clicking.

9.2 Recovery of the recording software

If you have to exchange hardware components and set up the server again, there is a recovery function for the installation routine.

For the new installation, use the ISO image with the same or a higher version that you had installed on your previous system. The ISO images of ASC are always full-fledged versions and contain a complete setup.

Carry out the new installation in recovery mode. A query appears where you can enter the previous hardware information so that the UUIDs can be mapped to the existing backup.

For the restore, the following hardware information is relevant:

Machine ID	*- Identifies the server* You find the information about the machine ID either • *in the file name of the backup log file of the PostgreSQL database which is saved by default in the following directory:* `\ASCDATA\DatabaseBackup` or • *in the registry in the following path:* `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ASC\Common`
Data Directory	*- directory of ASC services, e. g.* • *C:\Program Files (x86)\ASC\ASC Product Suite\data*
Calldata partition	*- directory of the CallPool, e. g. \ASCDATA*
Database partition	*- directory of the database, e. g. \ASCDB*

If operative hardware is available, proceed as follows:

1. Open the Windows Explorer.
2. Navigate to the directory in which the ISO image is located.
3. Mount the ISO image by double-clicking.
4. In the start menu, open the command line prompt as administrator.
5. Change in the command line prompt to the directory in which the ISO image is located.
6. Enter the following command to start the setup in recovery mode:
   `setupx.x.x-x.x.exe /asc recovery_mode`
7. Follow the installation routine. Install all the components that you had previously installed.
8. In the entry dialog, enter the current *Machine ID* as machine ID.
   ⇨ The following message appears:
   `"Recovery mode detected. Restore data directory, data partition and database. Then restart the system and start` Updater!"
9. Confirm the message.
10. **Do not restart the server yet!**
11. Before restoring the database restore the required directories:
    `\ASCDATA` and
    `\Program Files (x86)\ASC\ASC Product Suite\data`.
12. Install the database backup.

- Restore of the PostgreSQL database,
  see chapter "Restore PostgreSQL database", p. 25.
- Restore of the MS SQL database,
  see chapter "Restore MSSQL database", p. 30.

9.3 Restore of database

If operating system and hardware are intact, if the CallPool exists, and only the database is supposed to be restored, you can carry out a restore by means of the database backup.

If no database backup is available, get in touch with your sales contact at ASC to order a professional service to solve the problem.

To install a backup, continue with the respective instructions for the database you are using.

- See chapter "Restore PostgreSQL database", p. 25.
- See chapter "Restore MSSQL database", p. 30.

9.3.1 Restore PostgreSQL database

During the installation of the provided PostgreSQL database der Neo-recording software, a backup job is created for the PostgreSQL database which covers the database backups of the last 5 days (default value).

By default, you find the files in the following directory:

- `%ASCDATA%\DatabaseBackup\`

The retention time for the backups of the PostgreSQL database (default value: 5 days) can be changed by means of the administration tool for the database, if required.

To restore the database, proceed as follows.

Delete Neo database

Before you install the backup, you have to delete the existing database and create a new one.

The program *pgAdmin* requires a password. Contact your local ASC support or call ASC support at +49 700 27278776 for your password.

1. Stop the services *ASC ServiceMan* and *ASC ApplicationServer*.
   In multi-core systems, **all** Enterprise Cores must be stopped.
2. Open the program *pgAdmin*.
3. Log in.
4. Select the database entry *asc_rs*.
5. From the context menu, select the entry *Delete/Drop* and delete the database *asc_rs*.

Create new database

1. Right-click on *Servers* > *Servername* > *Databases*.
2. From the context menu, select the menu item *Create Database*.
3. In the tab *General*, enter *asc_rs* as name.
4. From the drop-down list *Owner*, select the value *postgres*.
5. In the tab *Definition* check whether the value for the coding has been set to *UTF8*.
6. Click on the button *Save* to save the database.

9.3.1.1 Apply configuration data

When deploying a PostgreSQL database, you can apply the saved configuration data.

Before restoring the database, copy the following files to the following path:

1. Install the saved configuration files of the database:
   ```
   \ASCDB\pg_hba.conf
   \ASCDB\postgresql.conf
   ```

9.3.1.2 Restore of the PostgreSQL database

For a restore, the PostgreSQL server must be running.

1. Before the restore, copy the saved configuration files to the database.
2. Right-click on the database instance *asc_rs* that you would like to restore.

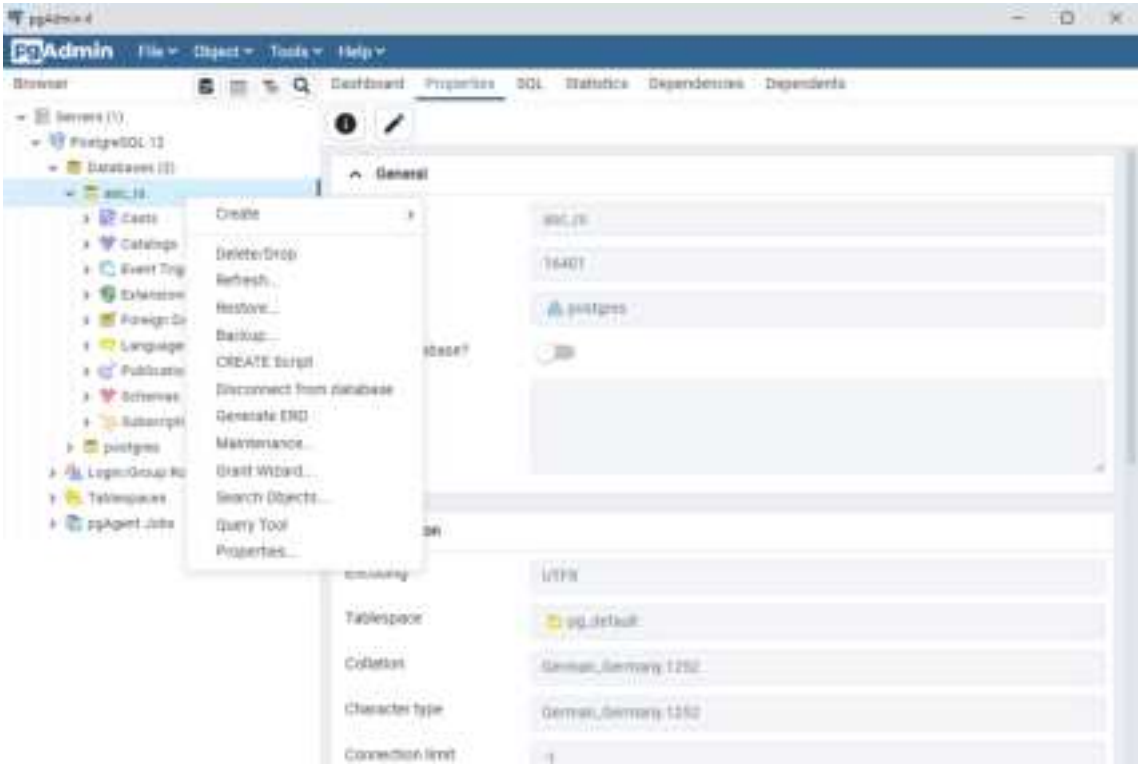

Fig. 10: Restore options

3. From the context menu, select the menu item *Restore*.
   ⇨ The input dialog to select the backup file opens.

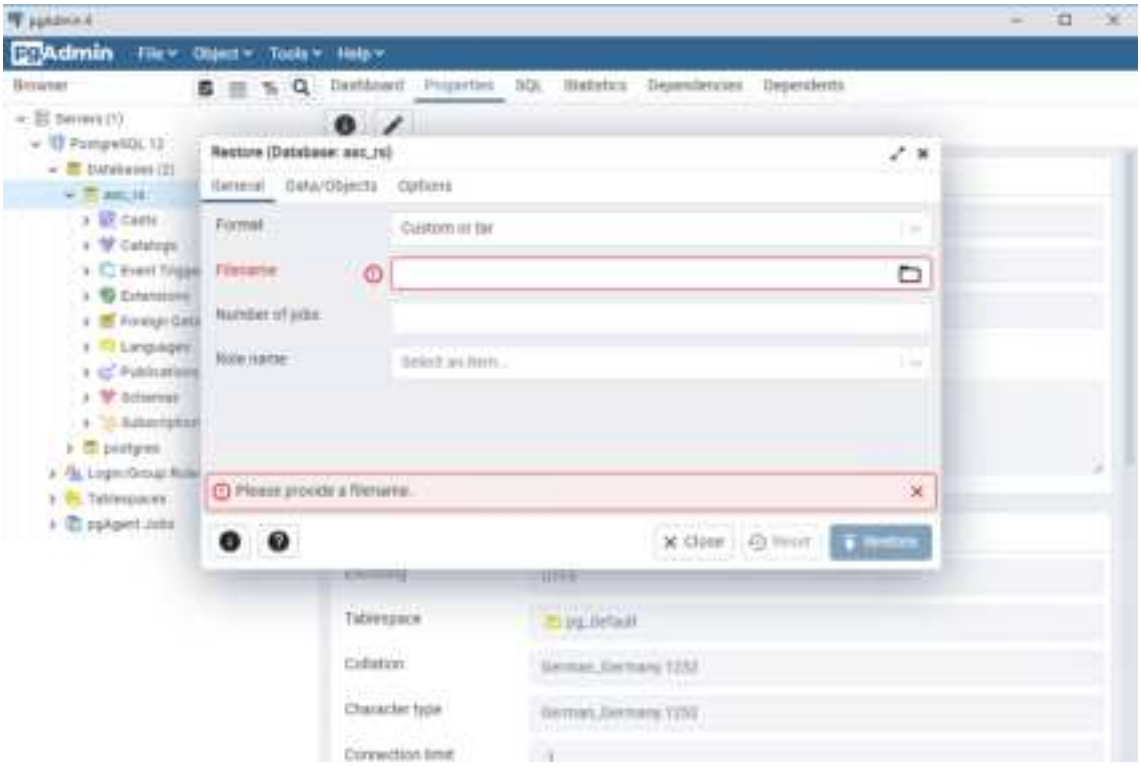

Fig. 11: Select restoration file

4. Select the following options for the restore:

Format	From the drop-down list, select the entry *Custom or tar*.

Filename	Select the backup file from which you would like to restore the database by clicking on the folder icon.
Rolename	From the drop-down list, select the entry *postgres*.

Tab. 9: Select restoration file

5. Click on the button *Restore*.
   ⇨ Once the restore has been completed, the tab *Messages* becomes active. Here, you can check the result. An error message is always displayed.
6. Click on the icon *View Details* and check whether only the following error message is displayed.
   ⇨ If this is the case, the restore was successful.

Fig. 12: Error message of restore of PostgreSQL

After the restore, the notification to configure the binary path for the database appears.

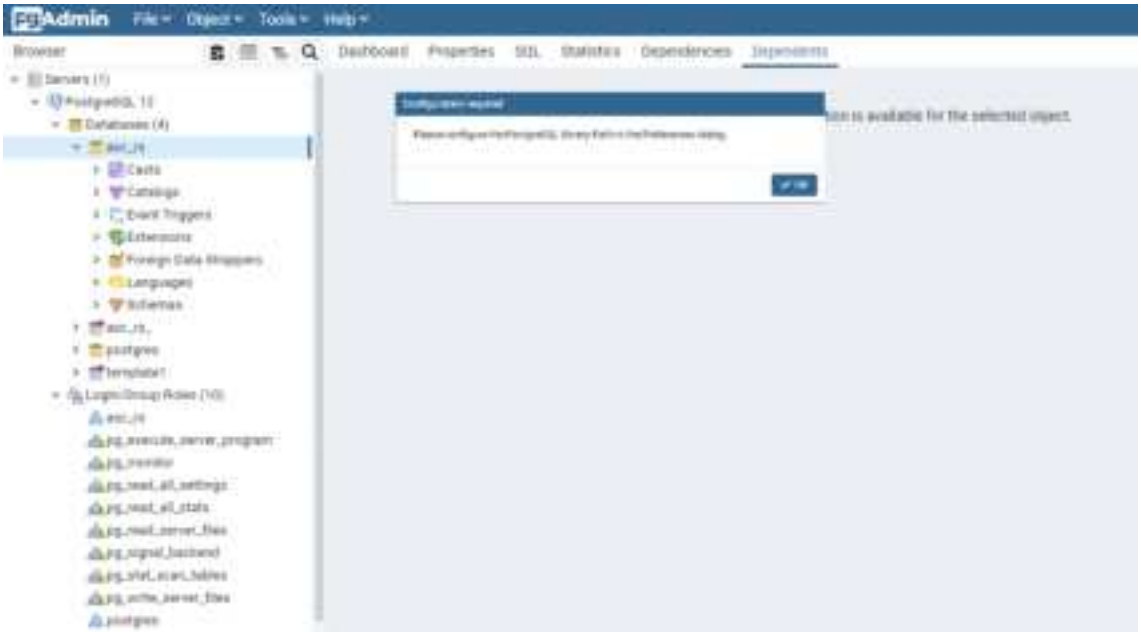

Fig. 13: Notification to configure the binary path of PostgreSQL

7. Select the menu item *File* > *Preferences* to enter the binary path for the database.

Fig. 14: Call up dialog preferences

8. In the line of the respective PostgreSQL version, click on the folder icon to select the path to the binary files.

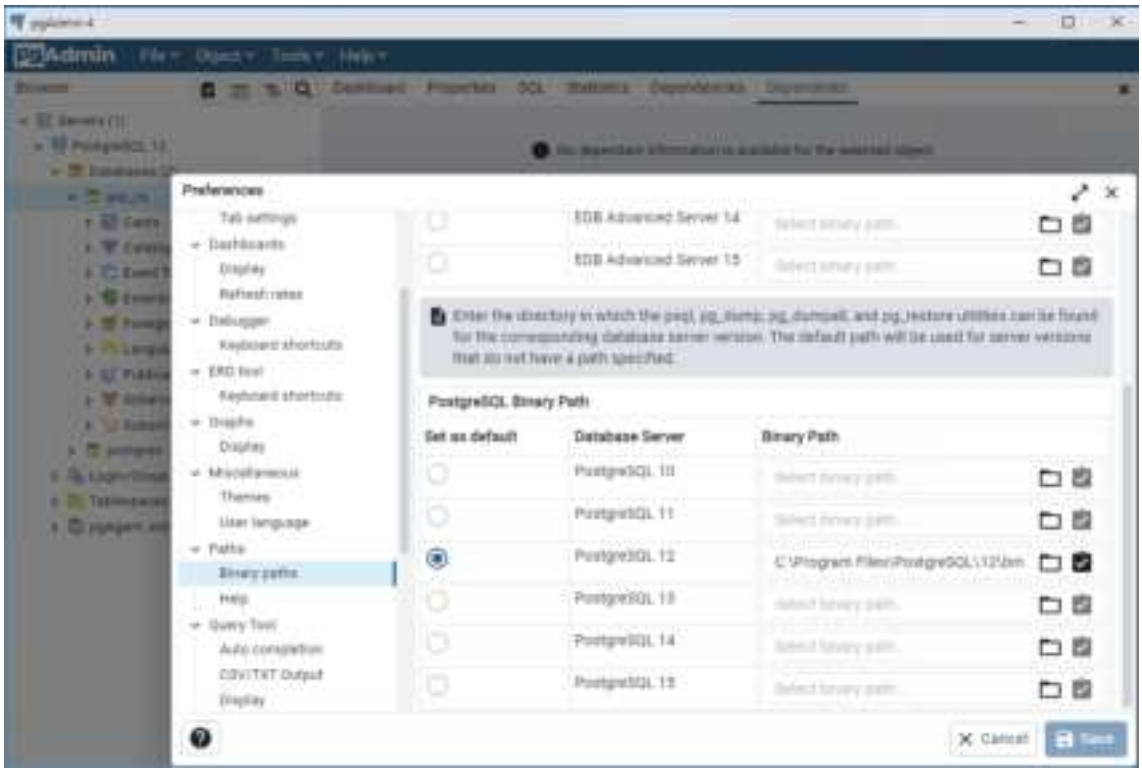

Fig. 15: Select binary path in browser

If you have to restore a failover configuration on the standby server, copy the configuration files back into the database directory. For further information refer to the installation manual for system providers *Failover operation for PostgreSQL databases*.

9. Click on the button *Save* to apply the settings.
10. **Restart the server now!**

9.3.1.3 Updater

After the database restore, you must start the Updater so that the general program parts can be installed subsequently.

There are 2 options for a restore with the Updater:

1. Start *Updater in simple mode*
2. Start *Updater in isolation mode*

Restore in simple mode

1. In the Windows Explorer, navigate to the directory in which the ISO image is located.
2. Mount the ISO image as a drive by double-clicking.
3. Open the command line prompt as administrator.
4. Change to the installation directory
   ```
   C:\Program Files (x86)\ASC\ASC Product Suite\Updater
   ```
5. Start the Updater with the following command:
   ```
   updater.exe --open
   ```
6. Restart the server once the Updater has run through.
7. Proceed with the conclusive steps,
   see chapter "Conclusive steps", p. 33.

Restore in isolation mode

An installation in isolation mode serves to install one or several Neo servers in parallel with an existing Neo system on a new server. By blocking the connections in the firewall, this server will be unable to connect with existing network drives or communication platforms until the user opts for switching off the existing system and releasing the system installed in isolation mode.

During a restore in isolation mode, the firewall is not opened during the updater routine but the rule `ASC_BLOCK_ALL_OUTBOUND` is activated blocking all outbound connections with the exception of:

- TCP 389, 636 (LDAP),
- TCP 1433 MS SQL (for the external database),
- TCP 3389 RDP (Remote access),
- TCP 5432 PostgreSQL (for external DB)
- UDP 123 NTP

Afterwards, you must remove the rule `ASC_BLOCK_ALL_OUTBOUND` and open the firewall.

To do so, proceed as follows:

1. In the Windows Explorer, navigate to the directory in which the ISO image is located.
2. Mount the ISO image as a drive by double-clicking.
3. Open the command line prompt as administrator.
4. Change to the installation directory
   ```
   C:\Program Files (x86)\ASC\ASC Product Suite\Updater
   ```
5. Start the Updater with the following parameter:
   ```
   updater.exe --isolate
   ```
6. Restart the server once the Updater has run through.
7. Ensure that the Updater process has been successful and that the configuration files have been applied.
8. To switch to the new server, you must shut down the previous server.
9. Then restart the Updater on the new server but with the parameter:
   ```
   updater.exe --open
   ```
   to remove the blocking of the connections and open the firewall.
10. Restart the server again once the update has run through.
11. Proceed with the conclusive steps,
    see chapter "Conclusive steps", p. 33.

9.3.2 Restore MSSQL database

1. Stop the services *ASC ServiceMan* and *ASC ApplicationServer*.
   In multi-core systems, **all** Enterprise Cores must be stopped.
2. Open the program *Microsoft SQL Server Management Studio*.
3. Log in and select the database entry *asc_rs*.
4. Check the properties and the files of the database.

The MSSQL database can be restored by means of the existing database. It is not necessary to delete the existing database ad create a new one.

9.3.2.1 Restore of the MSSQL database

For a restore, the Microsoft SQL server must be running.

1. Right-click on the database instance that you would like to restore.

2. From the context menu, select the menu item *Task* > *Restore* > *Database*.

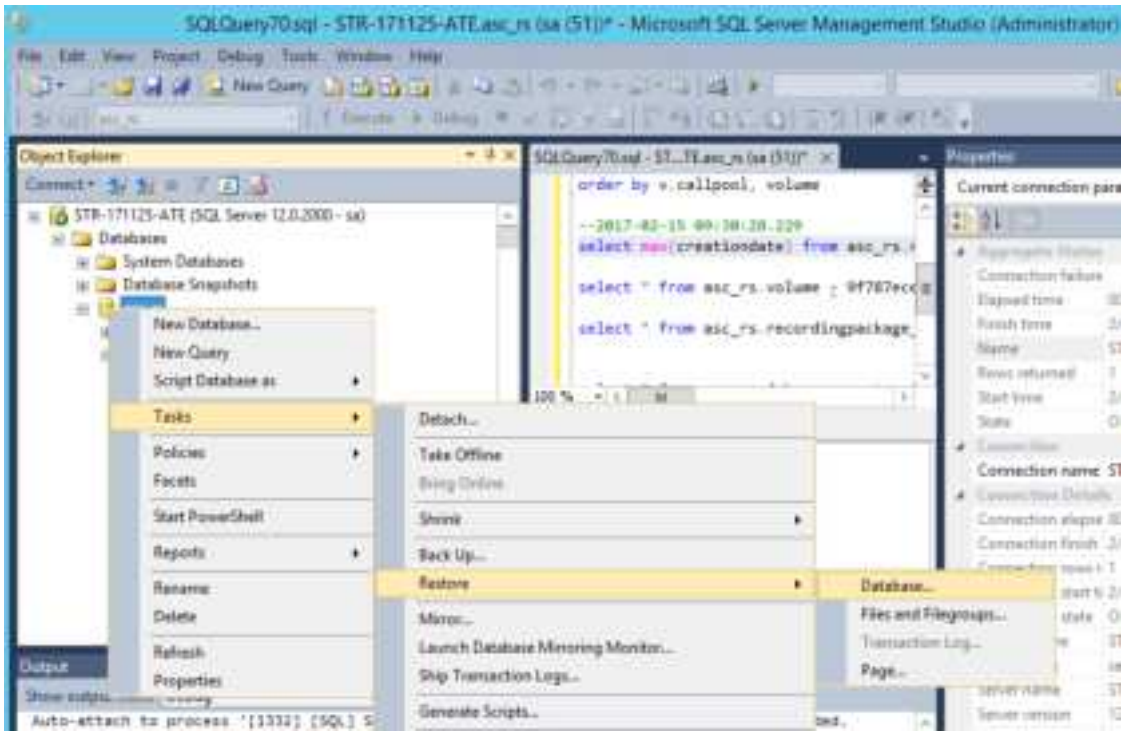

Fig. 16: Restore options

3. Click on the menu item *General* in the navigation bar.

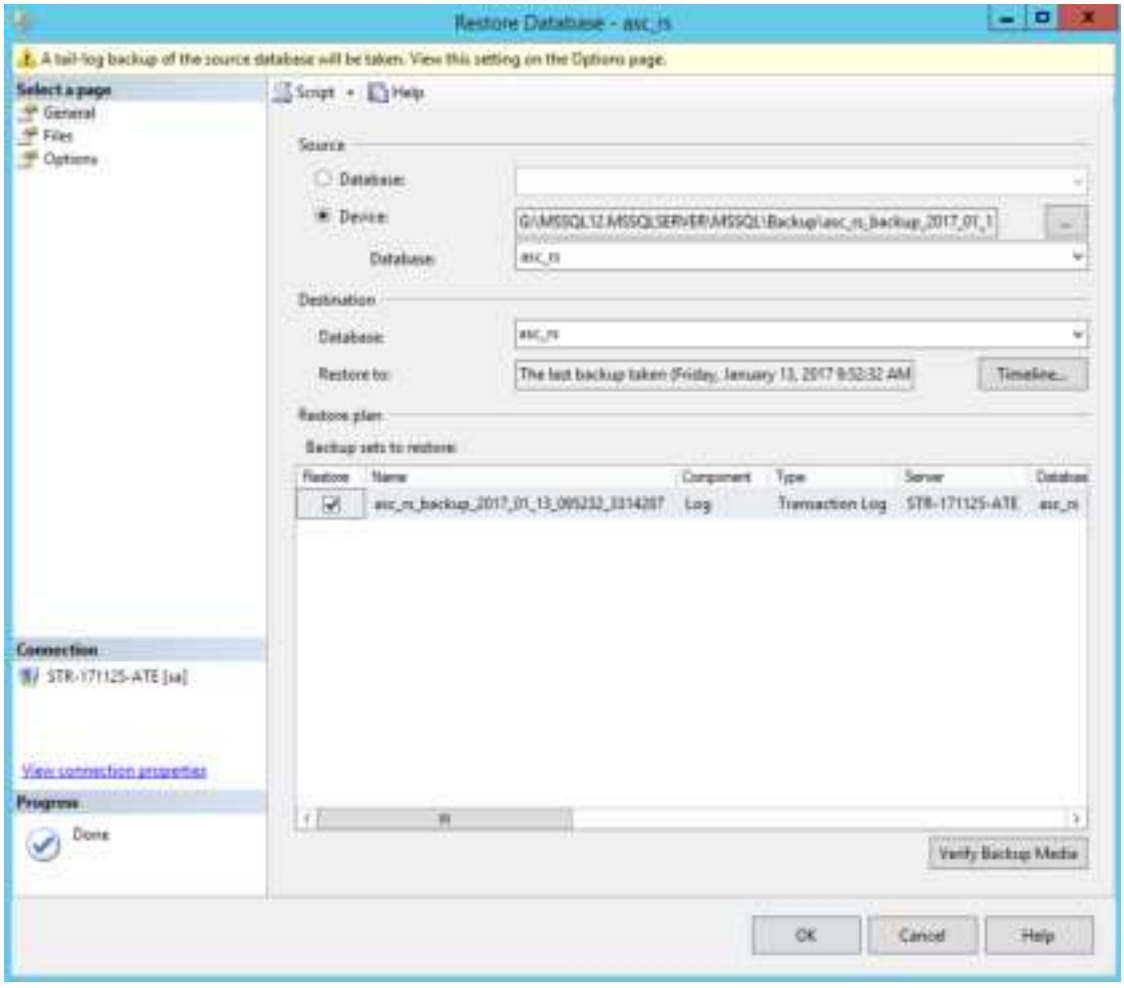

Fig. 17: Select restoration file

4. Select the following options for the restore:

Source

Device	Activate this option if the backup has been stored on a different medium.
Database	From the drop-down list, select the database backup from which you would like to restore the database, e. g. *asc_rs*.

Tab. 10: Select restoration file

Destination

Database	From the drop-down list, select the database you would like to restore, e. g. *asc_rs*.
Restore to	Select the backup that you would like to use for the restore. If you do not want to use the suggested backup for the restore, you can select a different backup by clicking on the button *Timeline*.

Tab. 11: Select destination

5. Click on the button *OK*.
   ⇨ Once the restore has been completed, the tab *Messages* becomes active. Here, you can check the result.
   Status 0 indicates that there are no messages and that the restore has been successful.
6. After the restore, check the properties and the files of the database.
7. **Restart the server now!**

Information about the restoration of the Microsoft SQL database can be found at http://msdn.microsoft.com/en-us/library/ms187510.aspx.

9.3.2.2 Updater

After the database restore, you must start the Updater so that the general program parts can be installed subsequently.

There are 2 options for a restore with the Updater:

1. Start *Updater in simple mode*
2. Start *Updater in isolation mode*

Restore in simple mode

1. In the Windows Explorer, navigate to the directory in which the ISO image is located.
2. Mount the ISO image as a drive by double-clicking.
3. Open the command line prompt as administrator.
4. Change to the installation directory
   ```
   C:\Program Files (x86)\ASC\ASC Product Suite\Updater
   ```
5. Start the Updater with the following command:
   ```
   updater.exe --open
   ```
6. Restart the server once the Updater has run through.
7. Proceed with the conclusive steps,
   see chapter "Conclusive steps", p. 33.

Restore in isolation mode

An installation in isolation mode serves to install one or several Neo servers in parallel with an existing Neo system on a new server. By blocking the connections in the firewall, this server will be unable to connect with existing network drives or communication platforms until the user opts for switching off the existing system and releasing the system installed in isolation mode.

During a restore in isolation mode, the firewall is not opened during the updater routine but the rule `ASC_BLOCK_ALL_OUTBOUND` is activated blocking all outbound connections with the exception of:

- TCP 389, 636 (LDAP),
- TCP 1433 MS SQL (for the external database),
- TCP 3389 RDP (Remote access),
- TCP 5432 PostgreSQL (for external DB)
- UDP 123 NTP

Afterwards, you must remove the rule `ASC_BLOCK_ALL_OUTBOUND` and open the firewall.

To do so, proceed as follows:

1. In the Windows Explorer, navigate to the directory in which the ISO image is located.
2. Mount the ISO image as a drive by double-clicking.
3. Open the command line prompt as administrator.
4. Change to the installation directory
   ```
   C:\Program Files (x86)\ASC\ASC Product Suite\Updater
   ```
5. Start the Updater with the following parameter:
   ```
   updater.exe --isolate
   ```
6. Restart the server once the Updater has run through.
7. Ensure that the Updater process has been successful and that the configuration files have been applied.
8. To switch to the new server, you must shut down the previous server.
9. Then restart the Updater on the new server but with the parameter:
   ```
   updater.exe --open
   ```
   to remove the blocking of the connections and open the firewall.
10. Restart the server again once the update has run through.
11. Proceed with the conclusive steps,
    see chapter "Conclusive steps", p. 33.

9.4 Conclusive steps

1. After the recovery process, request a new Neo license, as it will become invalid when you recover to a new server.
2. Reimport the certificates to enable encrypted connections.
3. Check whether recording is working correctly.
4. Check the replay of the recordings.

9.4.1 Import certificates

To be able to use an encrypted connection, you must import the respective certificated to the Truststore again. To do so, proceed like in a new installation. Use ASC's Certificate Import Tool.

1. Open the Windows Explorer.
2. Change to folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
3. Execute the file *certimporter.exe* as administrator.

4. For HTTPS certificates: Either regenerate the self-signed certificate or import customer certificate.
5. For PBX certificates: Check certificates if required for secure PBX communication and reload (or accept) Neo certificate on the PBX side.
6. If Secure LDAP is used, open HTTPS Trust and import the AD certificate.

For detailed information about importing certificates refer to the installation manual for system providers *Installation of Neo Suite*.

9.5 Rebuild of recordings

In case of disaster recovery, you can use the import function Neo Rebuild to close the gap between the latest database backup and the most current recording.

The recordings are imported to the CallPool and the corresponding metadata to the database. After the import, exclusively the tenant configured in the import configuration has access to the recordings.

9.5.1 Configure import job

To be able to use Neo Rebuild, you must have configured an import job.

The following configuration has to be carried out as system administrator.

In a multi-tenant system, you have to run a separate import job for each tenant.

1. Open the application System Configuration.
2. Log in as system administrator.
3. Select the menu item *Setup > Recording Import*.
   ⇨ The following main view appears:

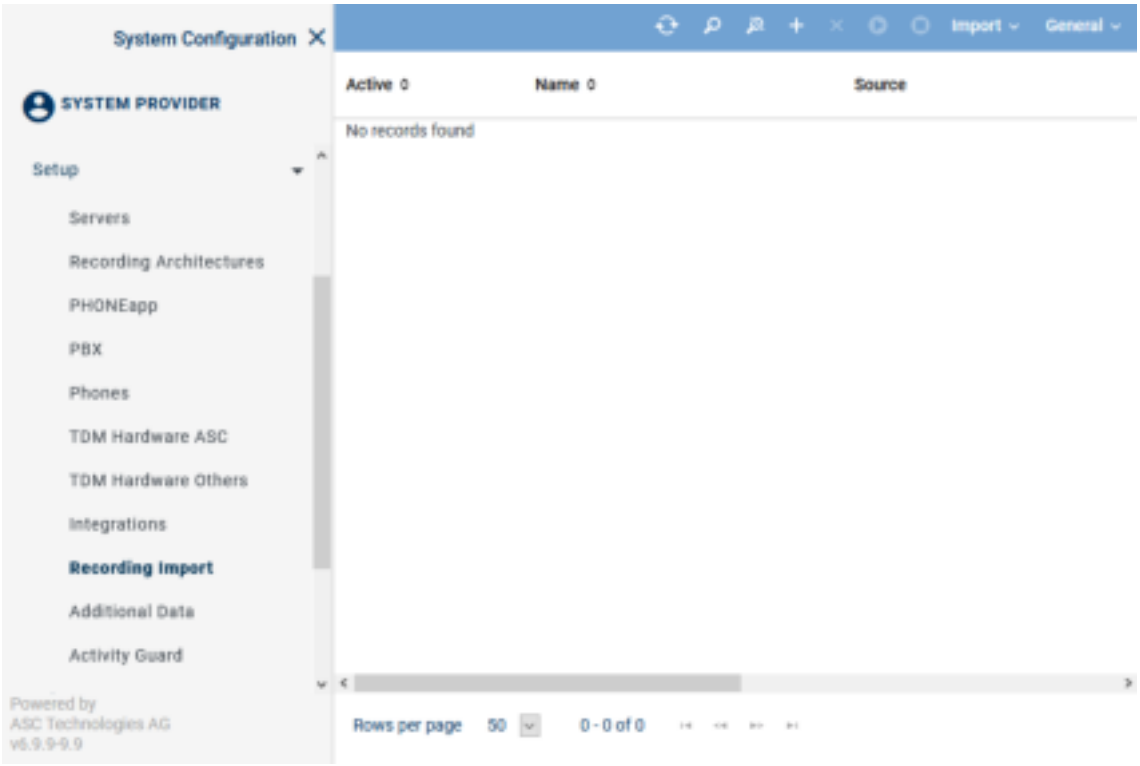

Fig. 18: Exemplary main view of import jobs

4. Click on the icon *(Create)* in the toolbar of the main view to configure the import format for Neo Rebuild.

9.5.1.1 Tab Details

Select the tab *Details* to select the tenant that you would like to carry out the Neo Rebuild for and to configure the import format.

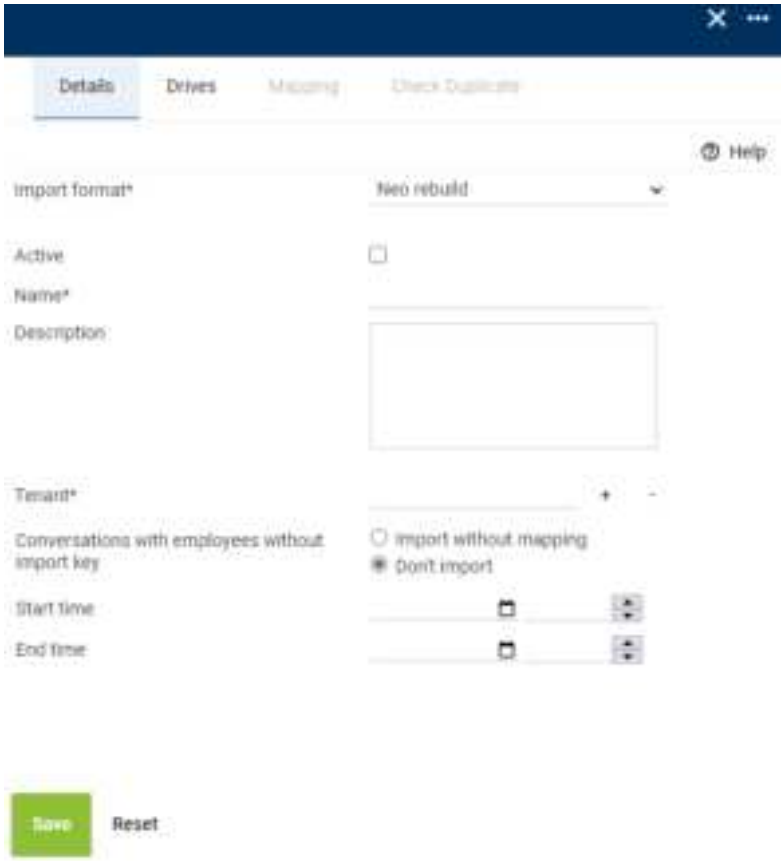

Fig. 19: Tab Details - configure import format Neo Rebuild

1. In the tab *Details*, enter the following parameters:

Import format	Select the import format Neo Rebuild from the drop-down list.
Active	Tick the check box to activate the import configuration. ☑ = Configuration is active; the import is started directly upon saving. ☐ = Configuration is not active; no import is carried out. A running import can be stopped that way.
Name	Enter the name of the import configuration here.
Description	Here, you can enter a description for the import configuration.
Tenant	Click on the button to select the tenant that you would like to map the imported data to, see chapter "Assign tenant", p. 36. The function Neo Rebuild has to be carried out for each tenant separately.
Conversations with employees without import key	• Import without mapping The conversations without mapping are imported but cannot be mapped to an agent, i. e. only the superuser can see the recordings. • Don't import The conversations are not imported into the destination system.

Start time / *End Time*	If you have selected the import format Neo Rebuild, you can limit the period from which recordings are supposed to be imported. Define the *start time* and the *end time* to limit the import to the exact period during which data was lost. You can set the period generously; already existing conversations are not imported again. Alternatively, you can enter either only the start time or the end time. If you enter neither a start time nor an end time, the import period is unlimited. You can enter the date directly in both entry fields via the keyboard or by clicking on the icon 🗖.

A recording architecture must have been configured on the server where the Neo Rebuild is carried out. If necessary, configure a separate All-in-one Basic Recording recording architecture with a *Universal Import* PBX for the Neo Rebuild import. The drive must have been mapped to this server, too.

9.5.1.1.1 Assign tenant

1. Click on the button ▸ on the right of the entry field.
2. Select a tenant from the list.

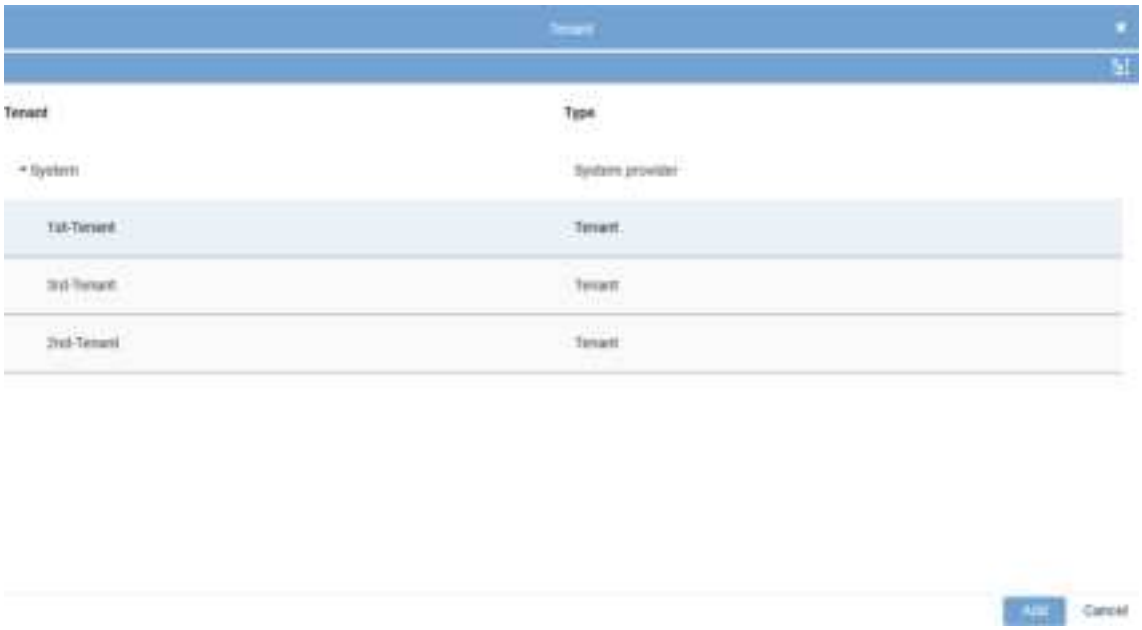

Fig. 20: Add tenant

3. To apply the selection, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

9.5.1.2 Tab Drives

Select the tab *Drives* to select the source drive from which the data is supposed to be imported.

A drive can be used in several job configurations as long as the drive is not used actively by a configuration.

If a drive is currently used actively by a job, no additional job which uses the same drive can be released or activated. This behavior includes all modules, i. e. regardless of the module that the configuration belongs to.

Fig. 21: Tab Drives - Select source directory

Source drive	Select the drive from which the data is supposed to be imported, see chapter "Assign drive", p. 37.

The import function Neo Rebuild only works for the local CallPool.

Other storage expansions are not supported here.

1. Click on the button *Save* to save the settings.
   Click on the button *Reset* to discard the settings.

9.5.1.2.1 Assign drive

1. Click on the button on the right of the entry field.
2. Select a drive from the list.

Fig. 22: Add drive

3. To apply the selection, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

9.5.2 Verifying functionality

1. Check System Monitoring for possible error messages.
2. To check whether the conversations have been imported successfully, open a player and check whether the conversations are displayed and whether they can be replayed.

9.6 Rebuild of recordings without database backup

If you carry out a restore without a database backup, some information will not be available for the import function Neo Rebuild.

Thereby, the following restrictions apply to the import function Neo Rebuild.

The recordings are imported to the CallPool and the corresponding metadata to the database. After the import, exclusively the tenant configured in the import configuration has access to the recordings.

When Neo key management is used and there is no backup of the database, the Neo Rebuild function cannot be used. It is not possible to restore encrypted data if its key is not available anymore.

For information about setting up and configuring drives refer to the administration manual for system providers *Configuration drives*.

9.6.1 Configure import job

To be able to use the Neo Rebuild function, you have to configure an import job.

The following configuration has to be carried out as system administrator.

In a multi-tenant system, you have to run a separate import job for each tenant.

1. Open the application System Configuration.
2. Log in as system administrator.
3. Select the menu item *Setup* > *Recording Import*.
   ⇨ The following main view appears:

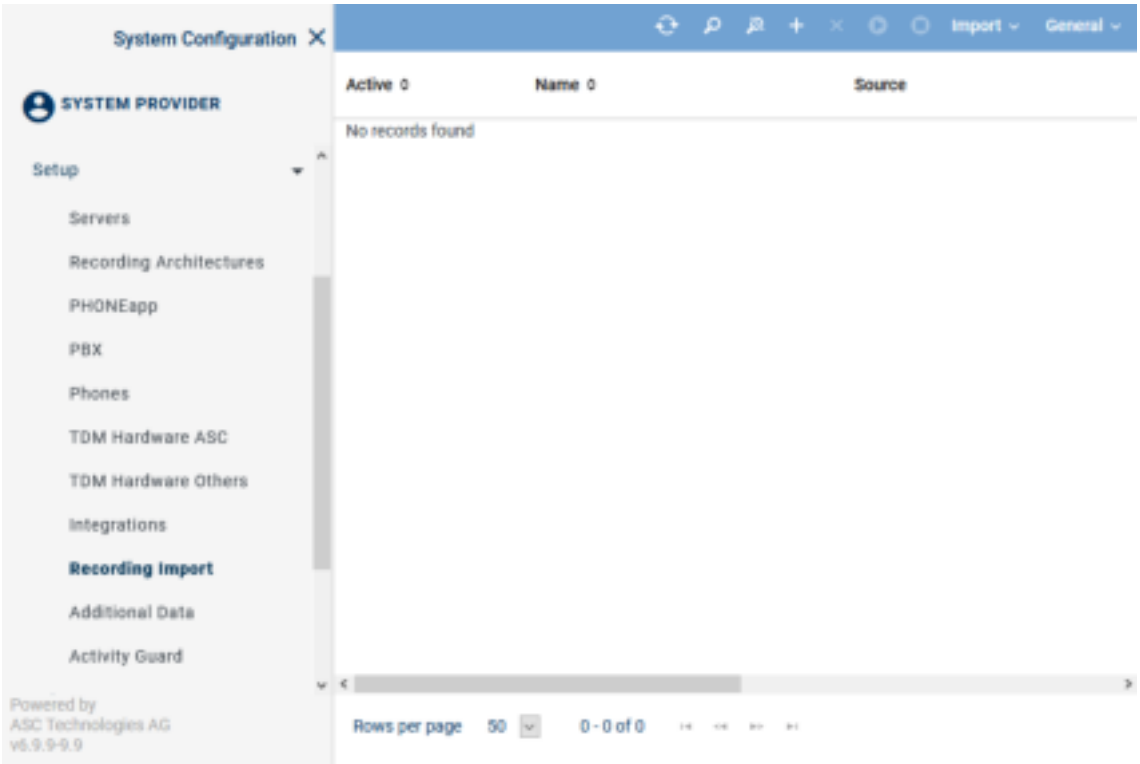

Fig. 23: Exemplary main view of import jobs

4. Click on the icon *(Create)* in the toolbar of the main view to configure the import format for Neo Rebuild.

9.6.1.1 Tab Details

Select the tab *Details* to select the tenant that you would like to carry out the Neo Rebuild for and to configure the import format.

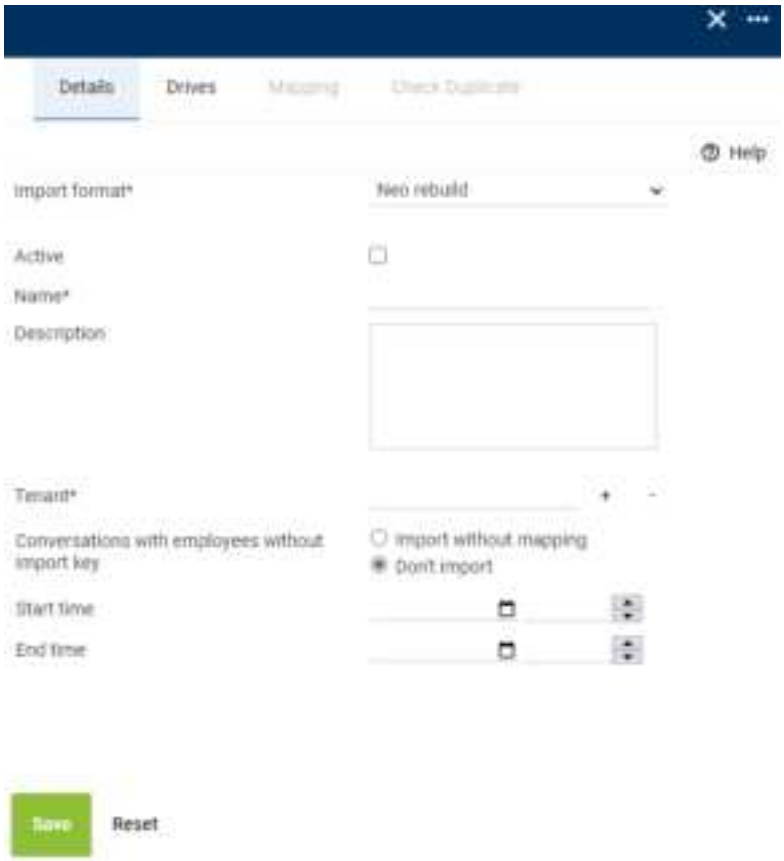

Fig. 24: Tab Details - configure import format Neo Rebuild

1. In the tab *Details*, enter the following parameters:

Import format	Select the import format Neo Rebuild from the drop-down list.
Active	Tick the check box to activate the import configuration. ☑ = Configuration is active; the import is started directly upon saving. ☐ = Configuration is not active; no import is carried out. A running import can be stopped that way.
Name	Enter the name of the import configuration here.
Description	Here, you can enter a description for the import configuration.
Tenant	Click on the button to select the tenant that you would like to map the imported data to, see chapter "Assign tenant", p. 40. The function Neo Rebuild has to be carried out for each tenant separately.
Conversations with employees without import key	• Import without mapping The conversations without mapping are imported but cannot be mapped to an agent, i. e. only the superuser can see the recordings. • Don't import The conversations are not imported into the destination system.
Start time / *End Time*	If you have selected the import format Neo Rebuild, you can limit the period from which recordings are supposed to be imported.

Define the *start time* and the *end time* to limit the import to the exact period during which data was lost. You can set the period generously; already existing conversations are not imported again.

Alternatively, you can enter either only the start time or the end time. If you enter neither a start time nor an end time, the import period is unlimited.

You can enter the date directly in both entry fields via the keyboard or by clicking on the icon .

A recording architecture must have been configured on the server where the Neo Rebuild is carried out. If necessary, configure a separate All-in-one Basic Recording recording architecture with a *Universal Import* PBX for the Neo Rebuild import. The drive must have been mapped to this server, too.

9.6.1.1.1 Assign tenant

1. Click on the button on the right of the entry field.
2. Select a tenant from the list.

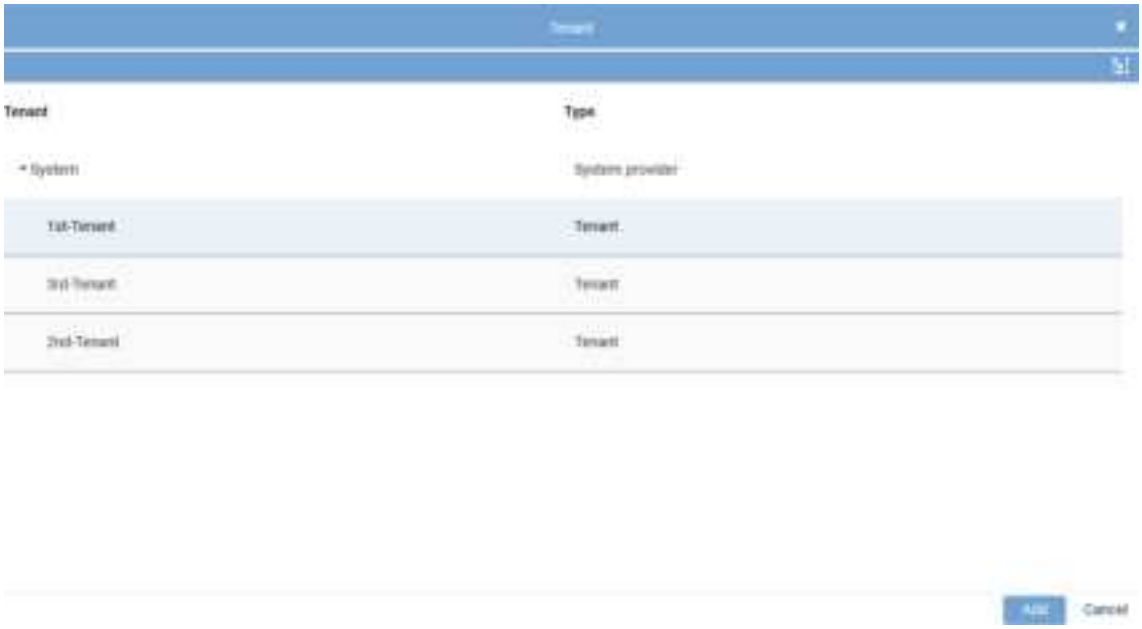

Fig. 25: Add tenant

3. To apply the selection, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

9.6.1.2 Tab Drives

Select the tab *Drives* to select the source drive from which the data is supposed to be imported.

A drive can be used in several job configurations as long as the drive is not used actively by a configuration.

If a drive is currently used actively by a job, no additional job which uses the same drive can be released or activated. This behavior includes all modules, i. e. regardless of the module that the configuration belongs to.

Fig. 26: Tab Drives - Select source directory

Source drive	Select the drive from which the data is supposed to be imported, see chapter "Assign drive", p. 41.

If no database backup is available, the following drives are supported for the import with the Neo Rebuild function:

- *CallPool*
- *NAS drives*
- *Azure Blob Storage*
- *Google Cloud Storage*

For information about setting up and configuring drives refer to the administration manual for system providers *Configuration drives*.

1. Click on the button *Save* to save the settings.
   Click on the button *Reset* to discard the settings.

9.6.1.2.1 Assign drive

1. Click on the button on the right of the entry field.
2. Select a drive from the list.

Fig. 27: Add drive

3. To apply the selection, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

9.6.2 Verifying functionality

1. Check System Monitoring for possible error messages.
2. To check whether the conversations have been imported successfully, open a player and check whether the conversations are displayed and whether they can be replayed.

9.7 Rebuild Solr Database (optional)

To be able to use the functions of the full-text search, you have to rebuild the Solr database. This option only appears in the Database Manager module if you have reinstalled the Solr database during the recovery installation process.

1. Log in to the application System Configuration as system administrator of the system provider (system-admin).
2. Select the menu item *Database Manager*.

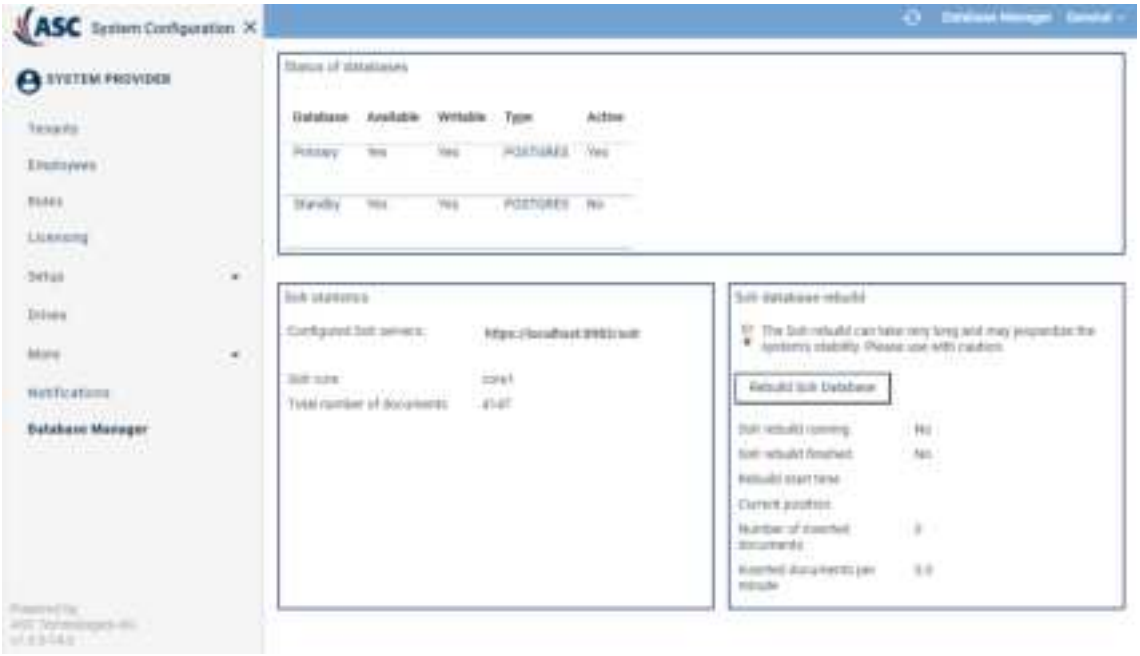

Fig. 28: Database Manager - rebuild Solr database

3. In the group field *Solr database rebuild*, click on the button *Rebuild Solr Database*.
   ⇨ The full text search is indexed and is available now.

For information about the installation of the Solr database refer to the installation manual for system providers *Software updates*.

List of figures

Fig. 1 System settings - Advanced settings - Open environment variable 9
Fig. 2 System settings - Create new system variable 9
Fig. 3 System settings - Name system variable and enter storage path 10
Fig. 4 System settings - Create system variable (example) 10
Fig. 5 Object explorer 11
Fig. 6 Configure general backup options 12
Fig. 7 Configure additional backup options 13
Fig. 8 Configure additional backup options 14
Fig. 9 Notification 15
Fig. 10 Restore options 27
Fig. 11 Select restoration file 27
Fig. 12 Error message of restore of PostgreSQL 28
Fig. 13 Notification to configure the binary path of PostgreSQL 28
Fig. 14 Call up dialog preferences 28
Fig. 15 Select binary path in browser 29
Fig. 16 Restore options 31
Fig. 17 Select restoration file 31
Fig. 18 Exemplary main view of import jobs 34
Fig. 19 Tab Details - configure import format Neo Rebuild 35
Fig. 20 Add tenant 36
Fig. 21 Tab Drives - Select source directory 37
Fig. 22 Add drive 37
Fig. 23 Exemplary main view of import jobs 38
Fig. 24 Tab Details - configure import format Neo Rebuild 39
Fig. 25 Add tenant 40
Fig. 26 Tab Drives - Select source directory 41
Fig. 27 Add drive 41
Fig. 28 Database Manager - rebuild Solr database 42

List of tables

Tab. 1 Configure backup options 12
Tab. 2 Configure backup options 12
Tab. 3 Options to overwrite medium 13
Tab. 4 Configure reliability 13
Tab. 5 Configure transaction log 14
Tab. 6 Configure tape drive 14
Tab. 7 Configure file options 15
Tab. 8 Configure compression 15
Tab. 9 Select restoration file 27
Tab. 10 Select restoration file 32
Tab. 11 Select destination 32

Glossary

CSV

Comma-separated values is a file format which stores tabular data in plain text form.

UNC

The Microsoft Windows UNC, short for Universal Naming Convention or Uniform Naming Convention, specifies a common syntax to describe the location of a network resource, such as a shared file, directory, or printer. The UNC syntax for Windows systems has the generic form: \\ComputerName\SharedFolder\Resource. Microsoft often refers to this as a "network path". Some Microsoft Windows interfaces also allow or require UNC syntax for WebDAV share access, rather than a URL. The UNC syntax is extended[7] with optional components to denote use of SSL and TCP/IP port number, a WebDAV URL of http[s]://HostName[:Port]/SharedFolder/Resource becomes \\HostName[@SSL][@Port]\SharedFolder\Resource When viewed remotely, the "SharedFolder" may have a name different from what a program on the server sees when opening "\SharedFolder". Instead, the SharedFolder name consists of an arbitrary name assigned to the folder when defining its "sharing". (Source: Wikipedia 05.05.2022)

VM

Virtual machine

ZIP

ZIP is an archive file format that supports lossless data compression. A ZIP file may contain one or more files or directories that may have been compressed. (Source: Wikipedia 10.11.2021)

Index