

Backup and disaster recovery



Installation manual for system providers and tenants

6/1/2022

Product line Neo, version 7.x

The described functions can be used with the following ASC products:

EVOIP^{neo}

EVOLUTION^{neo} / XXL / eco

INSPIRATION^{neo}

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 © 2022 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.

Contents

1	Introduction.....	5
2	Preconditions.....	6
3	Backups.....	7
3.1	Quick guide - Backup.....	7
3.2	Create database backups.....	7
3.2.1	PostgreSQL database	7
3.2.1.1	Backup of the database	7
3.2.1.2	Backup of the configuration files.....	10
3.2.2	MSSQL database	10
3.2.2.1	Backup of the MSSQL database	10
3.3	Backup data directory	15
3.4	Read out machine ID	15
3.5	Backup call pool.....	15
3.6	Read out system configuration	16
3.7	List the names and number of tenants	17
3.8	Backup EML speech analysis server.....	17
4	Failure scenarios	18
5	Recovery.....	19
5.1	Quick guide - Recovery	19
5.2	Recovery of the recording software.....	20
5.3	Restore of the database	21
5.3.1	Restore PostgreSQL database.....	21
5.3.1.1	Apply configuration data	22
5.3.1.2	Restore of the PostgreSQL database.....	22
5.3.1.3	Start updater	23
5.3.2	Restore MSSQL database.....	24
5.3.2.1	Restore of the MSSQL database.....	25
5.3.2.2	Start updater	27
5.4	Rebuild of recordings.....	28
5.4.1	Configure import job	28
5.4.1.1	Tab Details.....	28
5.4.1.2	Tab Drives	30
5.4.2	Verifying functionality.....	31
5.5	Exchange drive	32
5.6	Restore of EML speech analysis server	32
5.7	Conclusive steps.....	32
5.7.1	Import certificates	33
6	Troubleshooting	34

Glossary	37
Index	38

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 actual communication data (audio, video, screen or chat). This data is archived on external media for long-term storage.
- *Backup of meta data*
This is the additional data corresponding to the calls. This data is stored in the database and is thus protected via the database backup.
- *Backup of the system configuration*
This refers to the configuration in the Setup module of the application *System Configuration*. The configuration can be backed up by means of the export functionality.



As long as the database is unavailable, the system cannot be used for administrative purposes or for search and replay.

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 5 complete backups are created before the oldest backup is deleted. This guarantees that the latest database backups of the last 5 days are available. These backups are stored in :VASC DATA. 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.

The system configuration of the Setup module can be reimported by using the import functionality.

Possible gaps from the latest backup to the latest recording can be filled with the import functionality Neo Rebuild.




For information about the import functionality Neo Rebuild refer to the administration manual for system providers *Rebuild of recordings*.



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. 15](#).
- *Backup of the data directory*
C:\Program Files (x86)\ASC\ASC Product Suite\data, see [chapter "Backup data directory", p. 15](#).
- *Name and number of tenants and PBXs*, see [chapter "List the names and number of tenants", p. 17](#)
- *Backup of the database*, see [chapter "Create database backups", p. 7](#).
- *Backup of the call data partition with the recordings*
\ASCDATA, see [chapter "Backup call pool", p. 15](#).
- *Backup of the system configuration for script adaptations by ASC*, see [chapter "Read out system configuration", p. 16](#).

Snapshots in VMWare

Snapshots do not qualify as full-fledged server backup but serve to temporarily backup the status quo before maintenance or software updates.



For further information refer to the installation manual for system provider *Software updates*.

3 Backups

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.

3.1 Quick guide - Backup

1. Create database backup, see [chapter "Create database backups", p. 7](#).
2. Backup data directory,
C:\Program Files (x86)\ASC\ASC Product Suite\data
see [chapter "Backup data directory", p. 15](#),
3. 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. 15](#).
4. Backup call pool
:\ASCDATA\CallPool
see [chapter "Backup call pool", p. 15](#).
5. Read out system configuration, see [chapter "Read out system configuration", p. 16](#).
6. List number and names of the tenants,
see [chapter "List the names and number of tenants", p. 17](#)
7. For systems working with transcription, you must backup the relevant files and directories for the decoder and for the server.
see [chapter "Backup EML speech analysis server", p. 17](#)

3.2 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. 7](#).
- See [chapter "MSSQL database", p. 10](#).

3.2.1 PostgreSQL database

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

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

- %ASCDATA%\DatabaseBackup\

The period for the backup job 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.

3.2.1.1 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 Windows Explorer.
2. Change to the installation directory and execute the script *database backup* as administrator.
`\ASC\ASC Product Suite\scripts>database backup`
3. During the routine, enter the user *postgres* and the database password.
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 % of the database.

3.2.1.1.1 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.

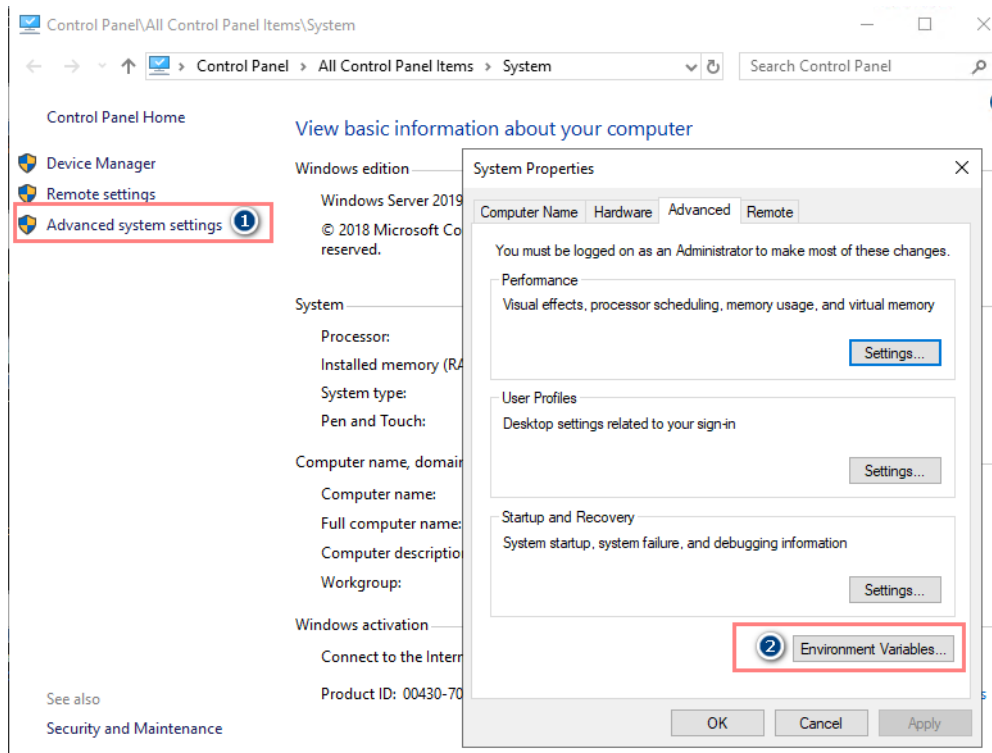


Fig. 1: System settings - Advanced settings - Open environment variable

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

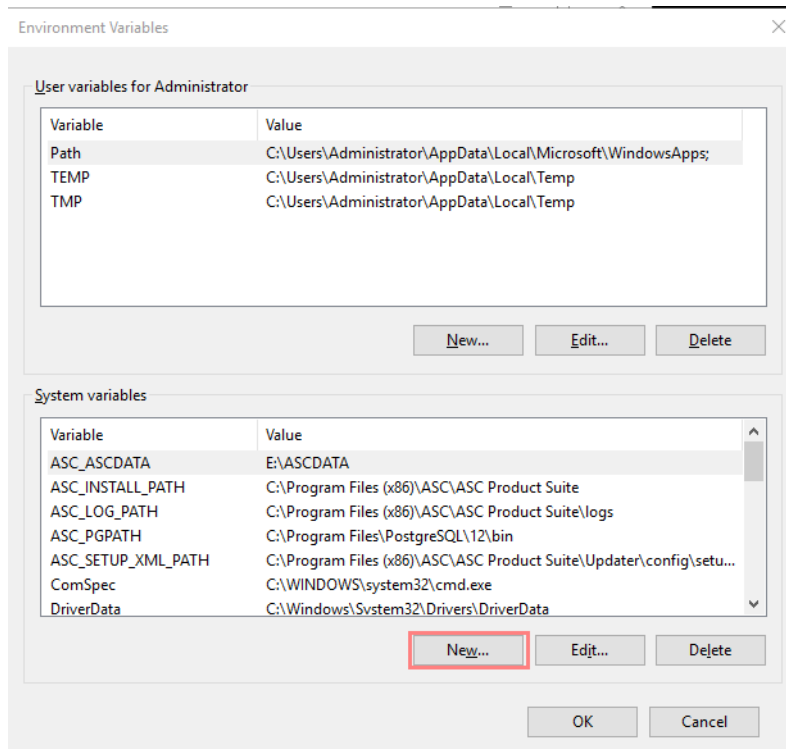


Fig. 2: System settings - Create new system variable

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

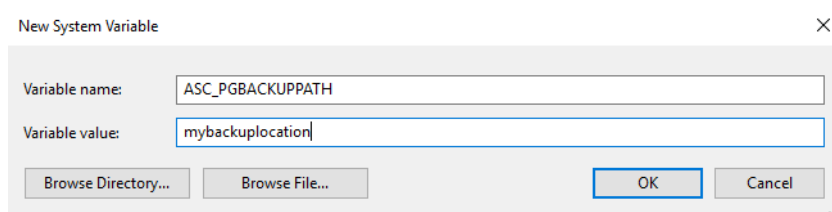


Fig. 3: System settings - Name system variable and enter storage path

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.

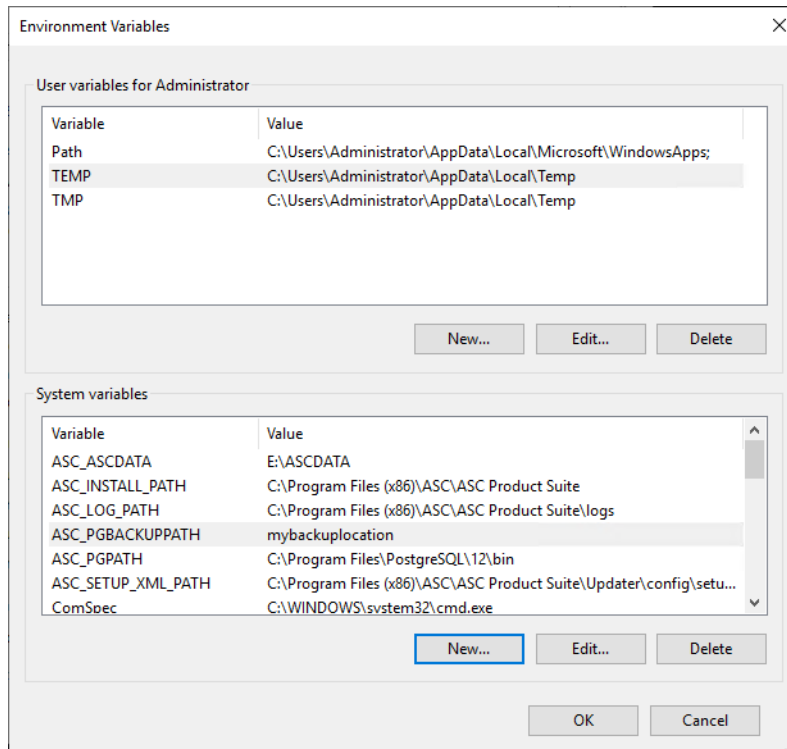


Fig. 4: System settings - Create system variable (example)

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

3.2.1.2 Backup of the configuration files

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

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

3.2.2 MSSQL database

3.2.2.1 Backup of the MSSQL database

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

NOTICE! If you do not have the database password, contact the ASC support by calling +49 700 27278776.

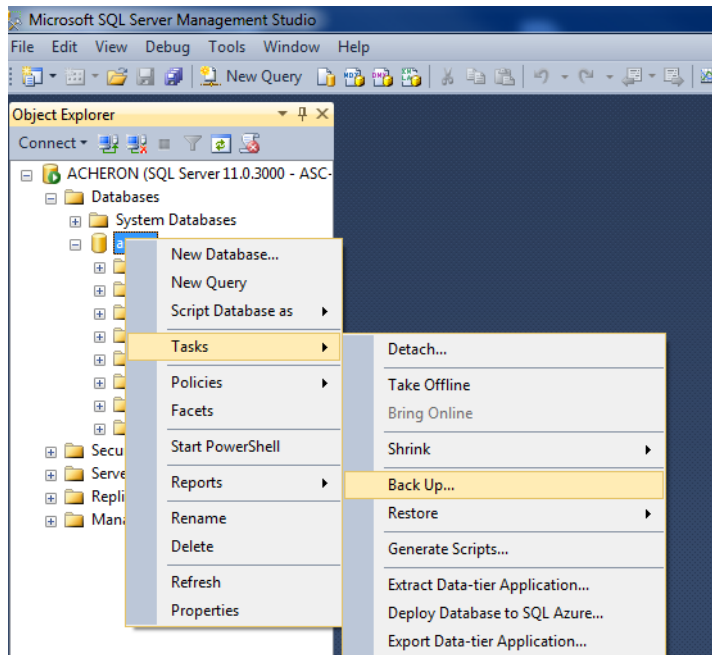


Fig. 5: Object explorer

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:

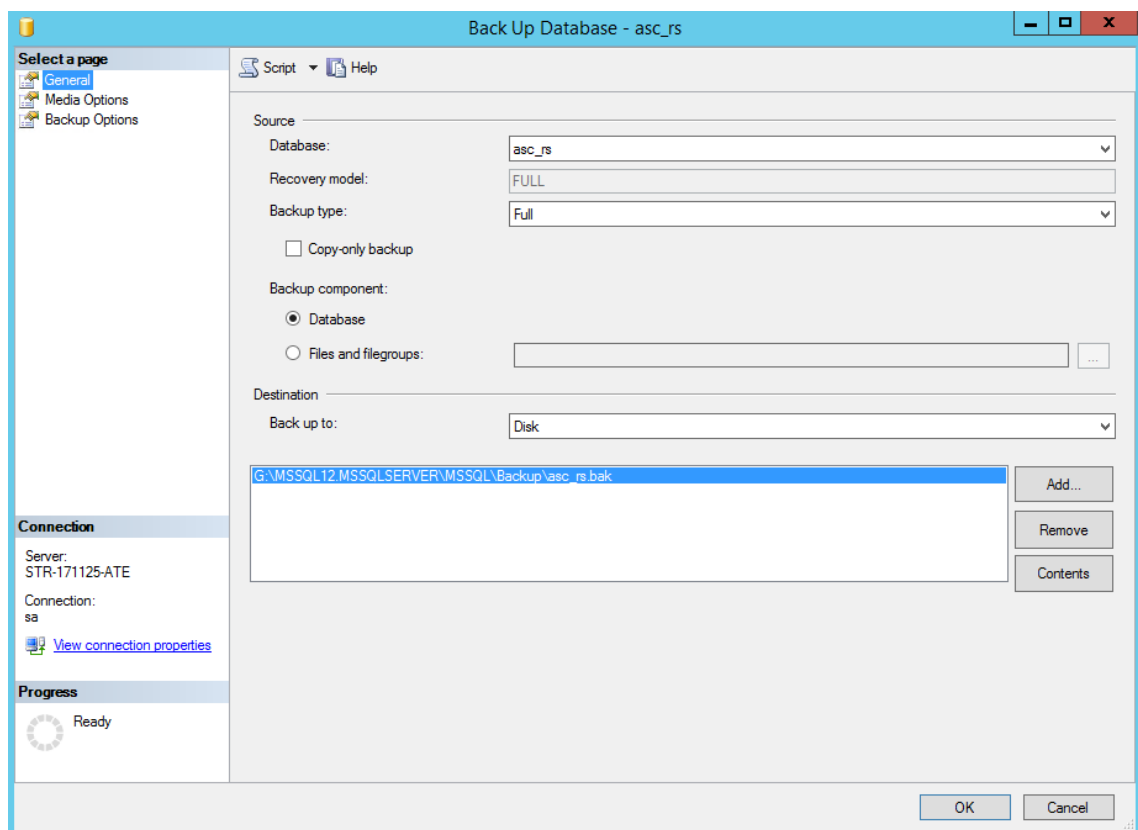


Fig. 6: Configure general backup options

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

Group field Source

<i>Database</i>	asc_rs
<i>Backup type</i>	full
<i>Backup component</i>	Database

Tab. 1: Configure backup options

Group field Destination

<i>Back up to</i>	From the drop-down list, select the medium on which you would like to store the backup. <ul style="list-style-type: none"> • <i>Disk</i> • <i>URL</i>
-------------------	---

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:

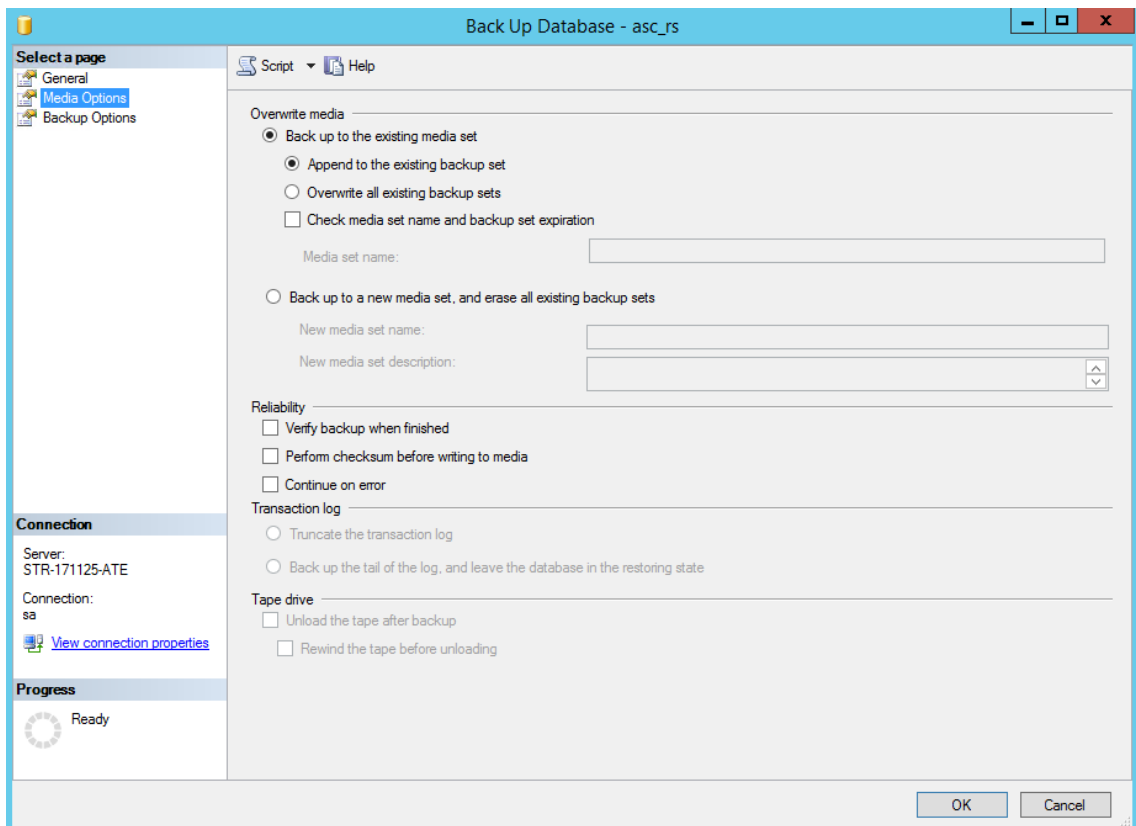


Fig. 7: Configure additional backup options

Group field Overwrite media

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

<input checked="" type="radio"/> <i>Back up to the existing media set</i> By activating this option, you add the following options to the existing backup:
<input checked="" type="radio"/> <i>Append to the existing backup set</i> By activating this option, you attach the backup to the existing one.
<input type="radio"/> <i>Overwrite all existing backup sets</i> By activating this option, you overwrite all previous backups.
<input checked="" type="checkbox"/> <i>Check media set name and backup set expiration</i> When activating this option, the entry field <i>Media set name</i> becomes active and you can enter a name for the media set.
<input type="radio"/> <i>Back up to a new media set, and erase all existing backup sets</i> By activating this option, you delete all previous backup files and create a new backup set.
<i>New media set name:</i> Enter a name for the new media set.
<i>New media set description:</i> Enter an optional description of the new media set.

Tab. 3: Options to overwrite medium

Group field Reliability

<input checked="" type="checkbox"/> <i>Verify backup when finished</i> Activate this option if the completed backup is supposed to be subject to a check.
<input checked="" type="checkbox"/> <i>Perform checksum before writing to media</i> Activate this option if a checksum is supposed to be reckoned up before writing the backup on the medium.
<input checked="" type="checkbox"/> <i>Continue on error</i> 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.

<input type="radio"/> <i>Truncate the transaction log</i>
<input type="radio"/> <i>Back up the tail of the log, and leave the database in the restoring state</i>

Tab. 5: Configure transaction protocol

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.

<input checked="" type="checkbox"/> <i>Unload the tape after backup</i>
<input checked="" type="checkbox"/> <i>Rewind the tape before unloading</i>

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:

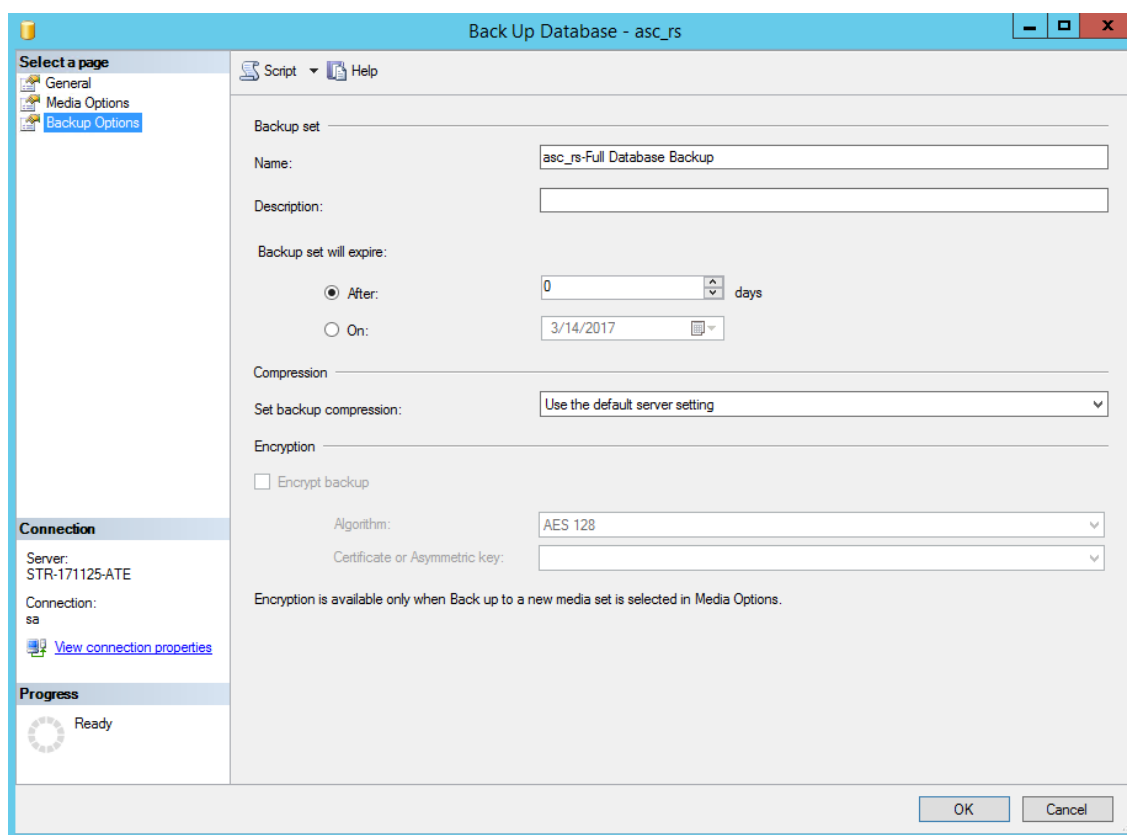


Fig. 8: Configure additional backup options

Group field Backup set

<i>Name</i>	Enter the name of the backup file.
<i>Description</i>	Optional entry field
<i>Backup set will expire</i>	Activate the option field.
<input checked="" type="radio"/> After:	Use the arrow keys to select the number of days until the backup set will expire.
<input type="radio"/> On:	Select the exact date in the calendar on which the backup set will expire.

Tab. 7: Configure file options

Group field Compression

<i>Set backup compression:</i>	Select the compression from the drop-down list. The following options can be selected: <ul style="list-style-type: none"> • <i>Use the default server settings</i> • <i>Compress backup</i> • <i>Do not compress backup</i>
--------------------------------	---

Tab. 8: Configure compression

1. Click on the button *OK* to create the backup.
- ⇒ Once the backup has been completed, the following notification appears:

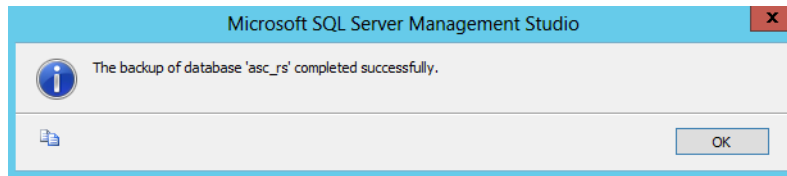


Fig. 9: Notification

You find the backup file in the previously defined path.

3.3 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 same 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.

3.4 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.

<i>Machine ID</i>	- <i>Identifies the server</i>
	You find the information about the machine ID either
	<ul style="list-style-type: none"> • <i>in the file name of the backup log file of the PostgreSQL database which is saved by default in the following directory:</i> \ASCDATA\DatabaseBackup
	or
	<ul style="list-style-type: none"> • <i>in the registry in the following path:</i> Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ASC\Common

3.5 Backup call pool

The call pool 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 call pool 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.

3.6 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 call pool, you can deploy the program for the backup of the call pool 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 call pool or 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 call pool 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 "D:\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.Asc-Tenant\YEAR_2015
```

```
Scan dir C:\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.Asc-Tenant\YEAR_2015\MONTH_11
```

```
Scan dir C:\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.Asc-Tenant\YEAR_2015\MONTH_11\DAY_21
```

```
Scan dir C:\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.Asc-Tenant\YEAR_2015\MONTH_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.Asc-Tenant\YEAR_2015\MONTH_11\DAY_23
```



```
Scan dir C:\ASCDATA\CallPool\90b3db81-6442-46d5-9dbf-66a3d550dc41.Asc-
Tenant\YEAR_2015\MONTH_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.

3.7 List the names and number of tenants

To restore the system, the number and the names of the tenants have to be the same as in the previous configuration.

1. Open the application *System Configuration*.
2. Select the menu item *Tenants* in the navigation bar.
3. Note down the names of the created tenants.

3.8 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.

4 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. 20](#)
- *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 the database", p. 21](#)
- *Last recordings are missing*,
if there is a gap between the latest backup and the current recordings, see [chapter "Rebuild of recordings", p. 28](#)
- *Drive is defective*,
if you have to exchange a drive and use the original letter of the drive, see [chapter "Exchange drive", p. 32](#)



During a restore, you must use the same drive letters that have been used during the initial installation. Otherwise the links will not work. Changing the letter of the drive will cause access issues and thus severe interferences with internal processes.

5.1

Quick guide - Recovery

Install recording server again

1. Carry out the setup of the installation medium with the following command in recovery mode:
`setup.exe /asc recovery_mode.`
 See also [chapter "Recovery of the recording software", p. 20.](#)
2. Follow the installation routine.
3. 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 ASC Updater!"
4. Confirm the message.
5. 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.
6. Recreate the required 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.

Recovery of the database

PostgreSQL databases

1. Open the program *pgAdmin*.
2. Create a new database with the name `asc_rs`.
3. Copy back the backed-up configuration files:
`: \ASCDB\pg_hba.conf`
`: \ASCDB\postgresql.conf`
`: \ASCDB\recovery.conf`
`: \ASCDB\DataBase.conf`
4. Install the database backup,
 see [chapter "Restore PostgreSQL database", p. 21.](#)
5. Start the Updater in the installation directory with the following command
`updater.exe --open`, see [chapter "Start updater", p. 23.](#)
6. Restart the server once the update has run through.
7. Check the system.

MSSQL databases

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. 24.](#)
4. Start the Updater in the installation directory with the following command
`updater.exe --open`, see [chapter "Start updater", p. 23.](#)
5. Restart the server once the update has run through.

Import certificates

1. To enable an encrypted connection, you must reimport the certificates, see [chapter "Import certificates", p. 33.](#)

Rebuild conversations

1. Carry out the import job NEO Rebuild to fill the gap from the latest database backup to the most recent recording,
see [chapter "Rebuild of recordings", p. 28.](#)
2. Check the replay of the conversations.

5.2

Recovery of the recording software

In case you have to exchange hardware components and set up the server again, there is a recovery functionality 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:

<i>Machine ID</i>	<p>- <i>Identifies the server</i></p> <p>You find the information about the machine ID either</p> <ul style="list-style-type: none"> • <i>in the file name of the backup log file of the PostgreSQL database which is saved by default in the following directory:</i> <code>\ASCDATA\DatabaseBackup</code> or • <i>in the registry in the following path:</i> <code>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ASC\Common</code>
<i>Data Directory</i>	<p>- <i>directory with the program modules, e. g.</i></p> <ul style="list-style-type: none"> • <i>C:\Program Files (x86)\ASC\ASC Product Suite\data</i>
<i>Calldata partition</i>	- <i>directory of the call pool, e. g. \ASCDATA</i>
<i>Database partition</i>	- <i>directory of the database, e. g. \ASCDB</i>

If operative hardware is available, proceed as follows:

1. Insert an installation medium of the recording software.
2. In the start menu, open the command line prompt as administrator.
3. Navigate to the drive of the installation medium.
4. Enter the following command to start the setup in recovery mode:
`setup.exe /asc recovery_mode`
5. Follow the installation routine.
6. 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 ASC Updater!"

7. Confirm the message and recreate the required directories:

\ASCDATA and
 \Program Files (x86)\ASC\ASC Product Suite\data.

8. Install the database backup.

- Restore of the PostgreSQL database, see [chapter "Restore PostgreSQL database", p. 21.](#)
- Restore of the MS SQL database, see [chapter "Restore MSSQL database", p. 24.](#)

5.3

Restore of the database

If operating system and hardware are intact, if the call pool 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. 21.](#)
- See [chapter "Restore MSSQL database", p. 24.](#)

5.3.1

Restore PostgreSQL database

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

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

- %ASCDATA%\DatabaseBackup\

The period for the backup job 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 defective database

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

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 and select the database entry *asc_rs*.
4. From the context menu, select the entry *Delete/Drop* and delete the database *asc_rs*.

Create new database

1. Right-click on *Server > Server Name > Databases*.
2. Select the menu item *New Database* from the context menu.
3. In the tab *Properties*, enter *asc_rs* as name.
4. From the drop-down list *Proprietor*, 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 *OK* to save the database.

5.3.1.1 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:

- Copy the saved configuration files of the database:
 - : \ASCDB\pg_hba.conf
 - : \ASCDB\postgresql.conf
 - : \ASCDB\recovery.conf
 - : \ASCDB\DataBase.conf

5.3.1.2 Restore of the PostgreSQL database



For a restore, the PostgreSQL server must be running.

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

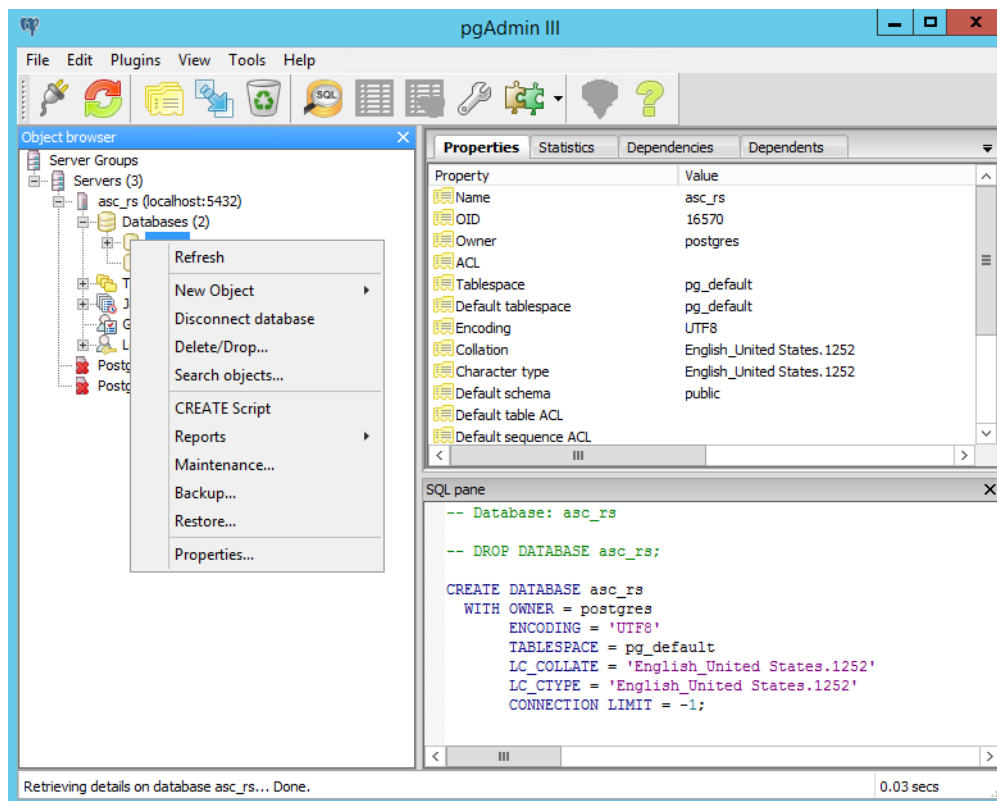


Fig. 10: Restore options

- From the context menu, select the menu item *Restore*.

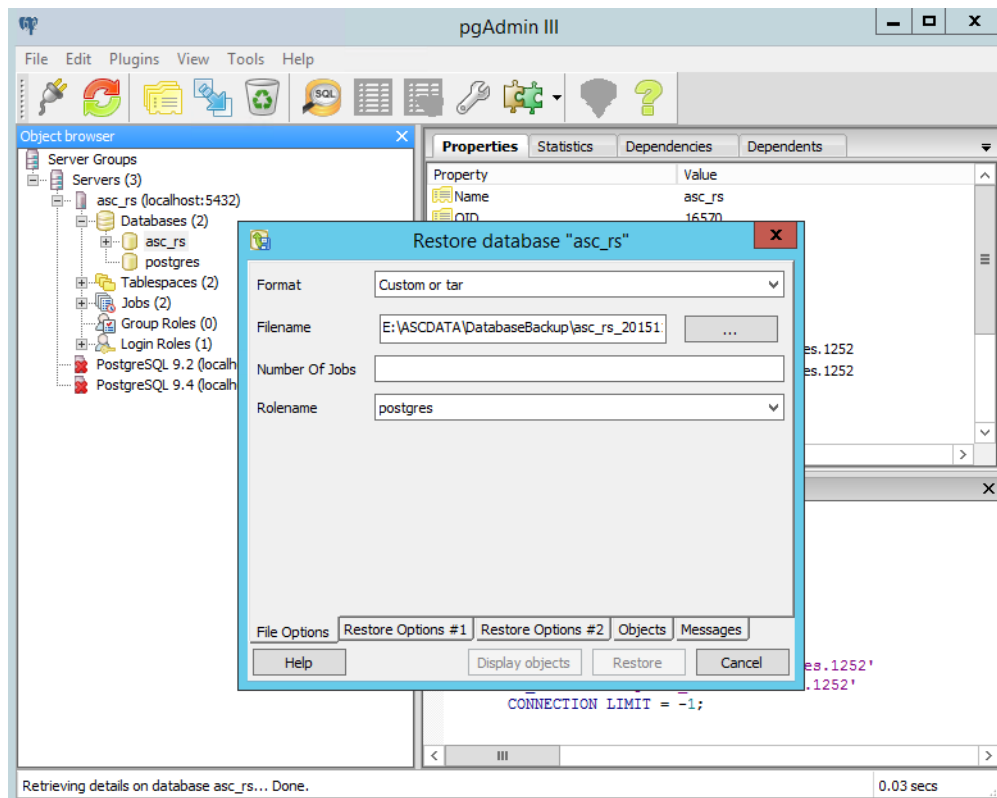



Fig. 11: Select restore file

4. Select the following options for the restore:

Format	From the drop-down list, select the entry <i>Custom or tar</i> .
Filename	Select the backup file from which you would like to restore the database by clicking on the button  .
Rolename	From the drop-down list, select the entry <i>postgres</i> .

Tab. 9: Select restore file

5. Click on the button *Restore*.
- ⇒ 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. Reboot the server after the restore.



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 provider *Failover operation for PostgreSQL databases*.

5.3.1.3 Start updater

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

There are 2 options for a restore with the ASC Updater:

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

Restore in simple mode

1. Change to the installation directory
C:\Program Files (x86)\ASC\ASC Product Suite\Updater
2. Start the ASC Updater with the following command
updater.exe --open
3. Restart the server once the Updater has run through.
4. Check the system.

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. Change to the installation directory
C:\Program Files (x86)\ASC\ASC Product Suite\Updater
2. Start the ASC Updater with the following parameter:
updater.exe --isolate
3. Restart the server once the Updater has run through.
4. Ensure that the ASC Updater process has been successful and that the configuration files have been applied.
5. To switch to the new server, you must shut down the previous server.
6. Then restart the ASC Updater on the new server but with the parameter:
updater.exe --open
to remove the blocking of the connections and open the firewall.
7. Check the system.

5.3.2 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 and create a new one.

5.3.2.1 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*.

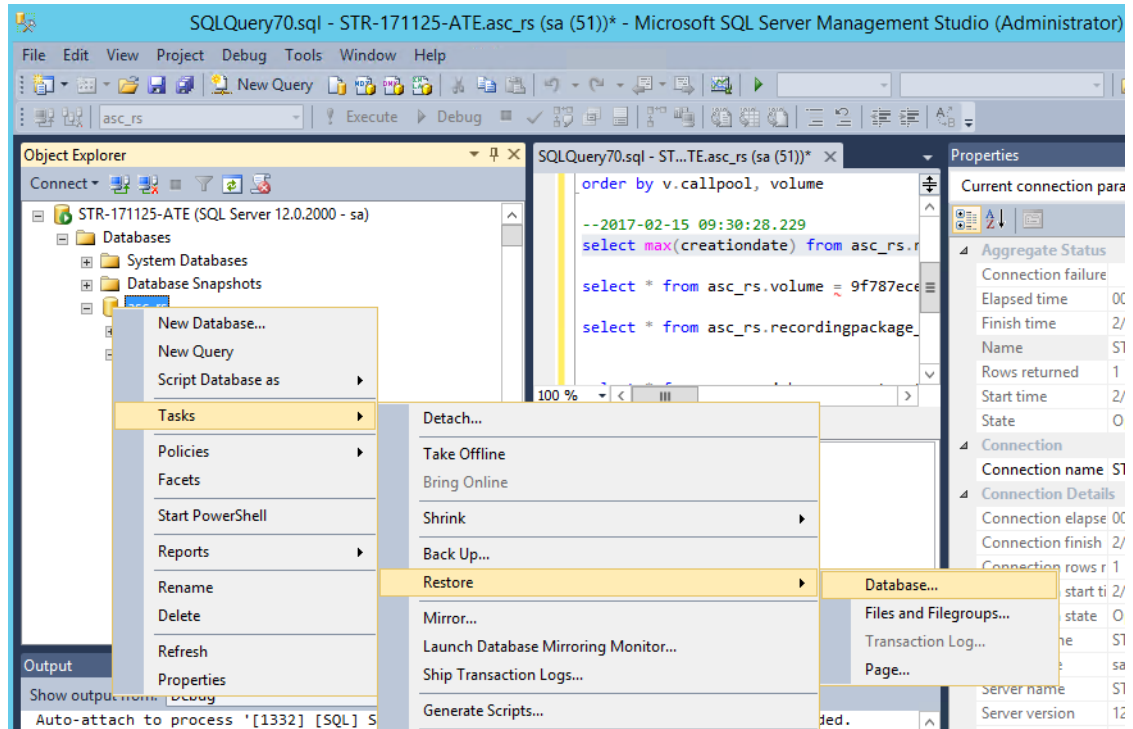


Fig. 12: Restore options

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

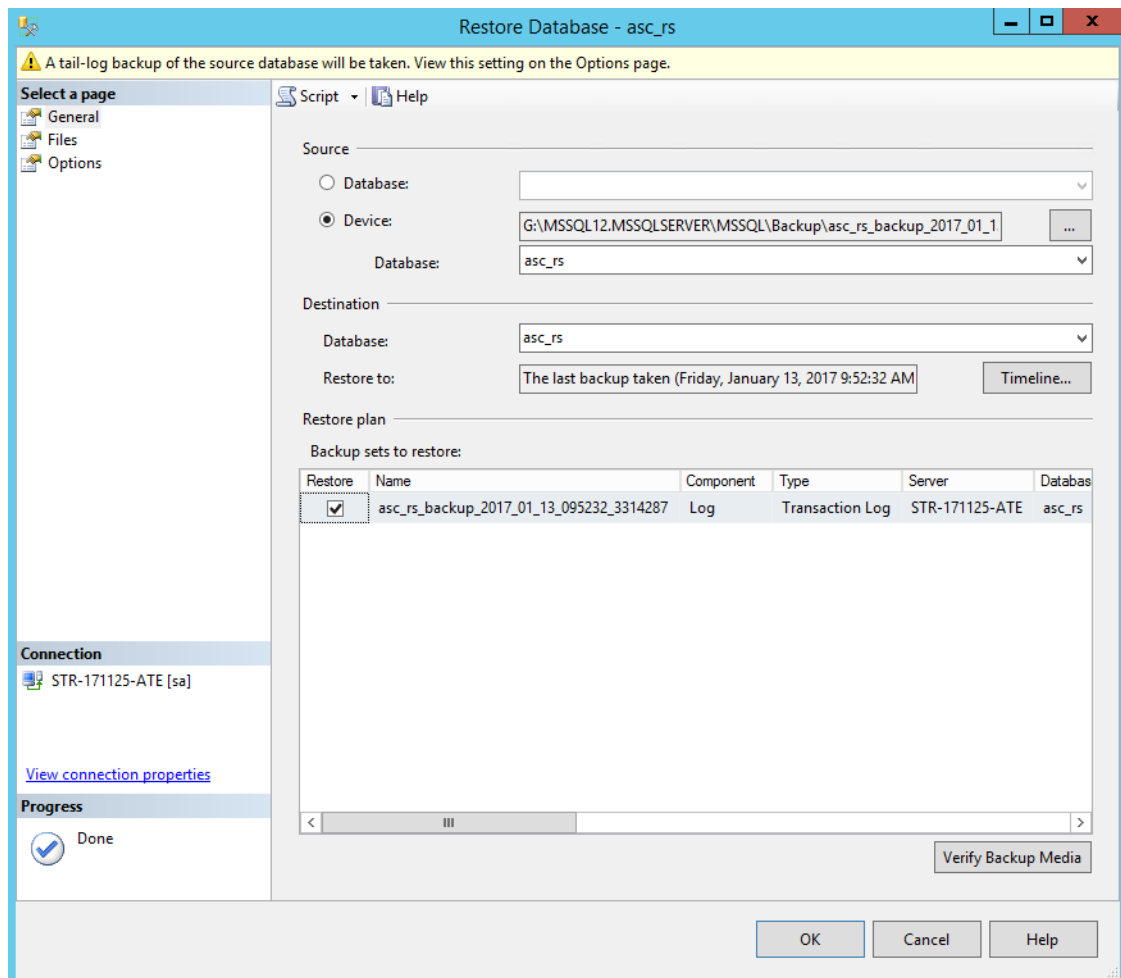


Fig. 13: Select restore file

4. Select the following options for the restore:

Source

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

Tab. 10: Select restore file

Destination

<i>Database</i>	From the drop-down list, select the database backup from which you would like to restore the database, e. g. <i>asc_rs</i> .
<i>Restore to</i>	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 <i>Timeline</i> .

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. Reboot the server after the restore.



For further information see <http://msdn.microsoft.com/en-us/library/ms187510.aspx>.

5.3.2.2 Start updater

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

There are 2 options for a restore with the ASC Updater:

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

Restore in simple mode

1. Change to the installation directory
C:\Program Files (x86)\ASC\ASC Product Suite\Updater
2. Start the ASC Updater with the following command
updater.exe --open
3. Restart the server once the Updater has run through.
4. Check the system.

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. Change to the installation directory
C:\Program Files (x86)\ASC\ASC Product Suite\Updater
2. Start the ASC Updater with the following parameter:
updater.exe --isolate
3. Restart the server once the Updater has run through.
4. Ensure that the ASC Updater process has been successful and that the configuration files have been applied.
5. To switch to the new server, you must shut down the previous server.
6. Then restart the ASC Updater on the new server but with the parameter:
updater.exe --open
to remove the blocking of the connections and open the firewall.
7. Check the system.

5.4 Rebuild of recordings



Depending on the extent of the data loss, you may have to install the backup of the database first.

To fill the gap from the latest database backup to the most recent recording, in the application System Configuration, you can use the import function Neo Rebuild.



Basic information about using the application System Configuration can be found in the user manual for administrators *System Configuration - General information*.

5.4.1 Configure import job

To be able to use Neo Rebuild, you must 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:

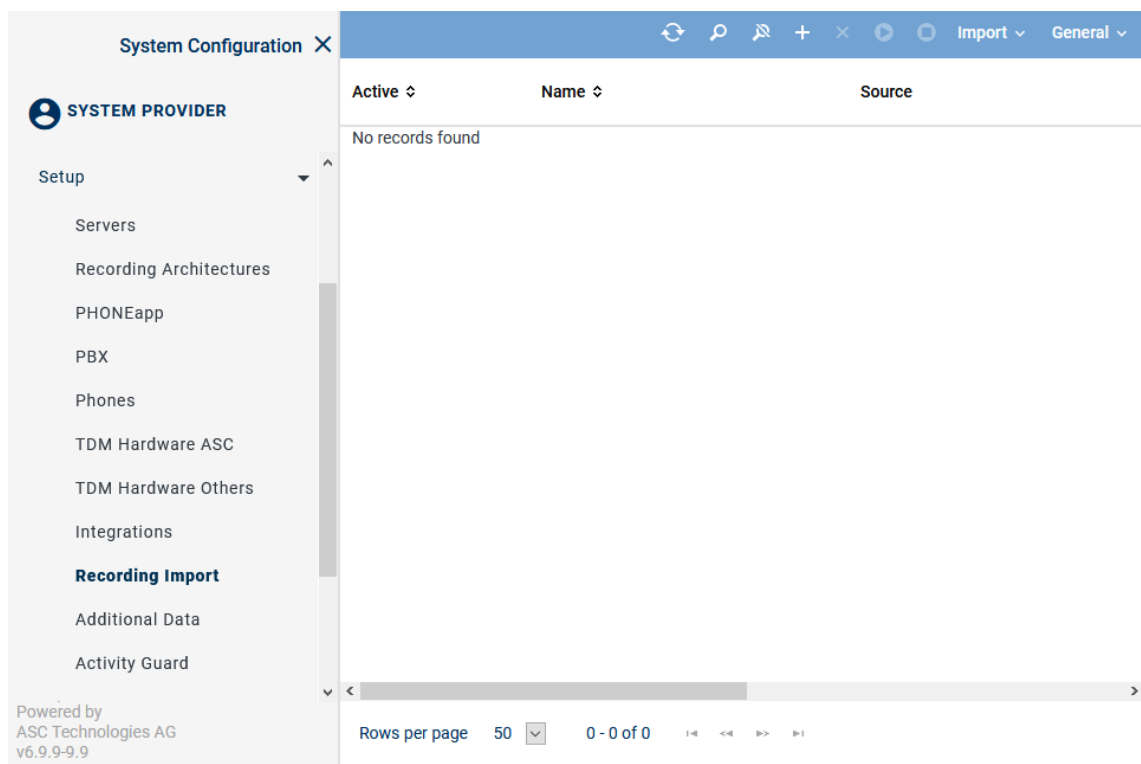

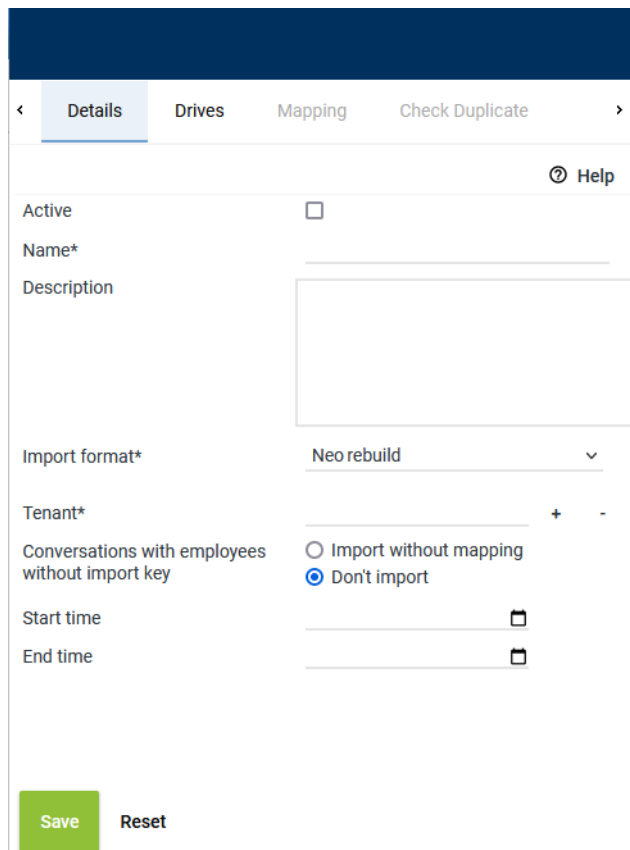


Fig. 14: Exemplary main view of import jobs

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

5.4.1.1 Tab Details

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




The screenshot shows the 'Details' tab of a configuration interface. At the top, there are tabs: 'Details' (selected), 'Drives', 'Mapping', and 'Check Duplicate'. Below the tabs is a 'Help' icon. The form contains the following fields:

- Active:** A checkbox.
- Name*:** A text input field.
- Description:** A large text area.
- Import format*:** A dropdown menu with 'Neo rebuild' selected.
- Tenant*:** A text input field with '+' and '-' buttons.
- Conversations with employees without import key:** Two radio buttons: 'Import without mapping' (unselected) and 'Don't import' (selected).
- Start time:** A date/time picker.
- End time:** A date/time picker.

At the bottom left, there are two buttons: 'Save' (green) and 'Reset'.

Fig. 15: Tab Details - Configure import format NEO Rebuild


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

Active	<p>Tick the check box to activate the import configuration.</p> <p><input checked="" type="checkbox"/> = Configuration is active; the import is started directly upon saving.</p> <p><input type="checkbox"/> = Configuration is not active; no import is carried out. A running import can be stopped that way.</p>
Name	Enter the name of the import configuration.
Description	Here, you can enter a description for the import configuration.
Import format	Select the import format from the drop-down list NEO Rebuild.
Codec	The codec cannot be changed for this import format.
Execution mode	This import job is always executed only once. This setting has been preselected and cannot be changed for this import format. If the import has to be executed once again for some reason, you have to deactivate the import job, activate it again and save it.
Tenant	<p>Click on the button  to select the tenant that you would like to map the imported data to, see chapter "Assign tenant", p. 30.</p> <p>The rebuild functionality has to be carried out for each tenant separately.</p>
Conversations with employees without import key	<ul style="list-style-type: none"> • 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 /	If you have selected the import format NEO Rebuild, you can limit the period from which recordings are supposed to be imported.

End time

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.

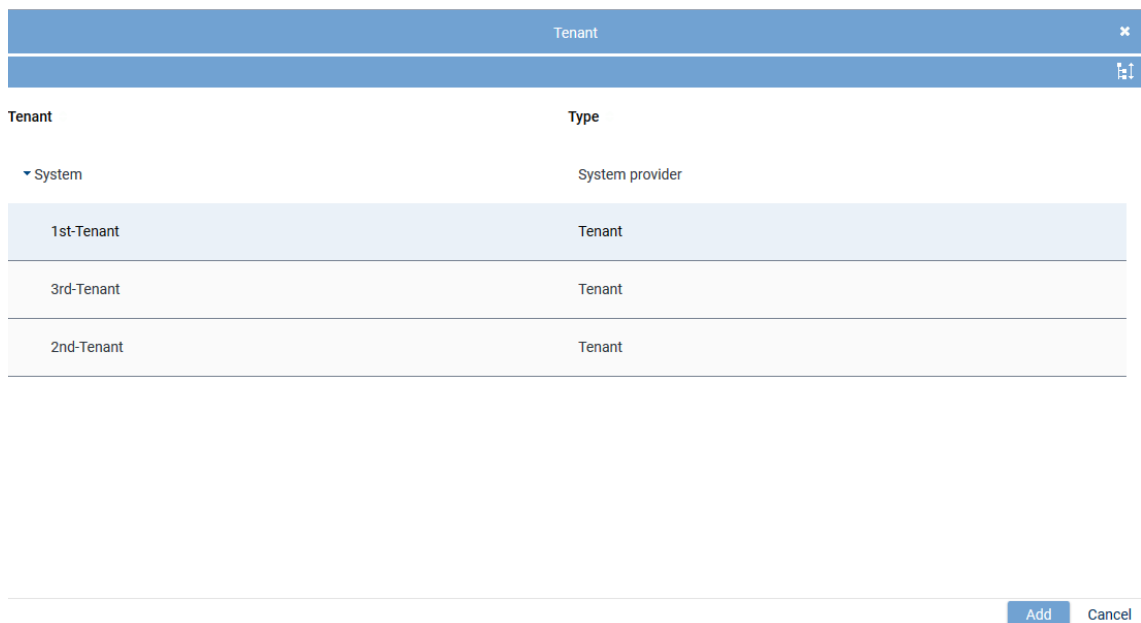
You can enter the date directly in both entry fields via the keyboard or by clicking on the icon .

NOTICE!

You do not have to select a **PBX**; the conversations of all PBXs assigned to the selected tenant are imported.

5.4.1.1.1 Assign tenant

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



Tenant	Type
▼ System	System provider
1st-Tenant	Tenant
3rd-Tenant	Tenant
2nd-Tenant	Tenant

Add Cancel

Fig. 16: 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**.

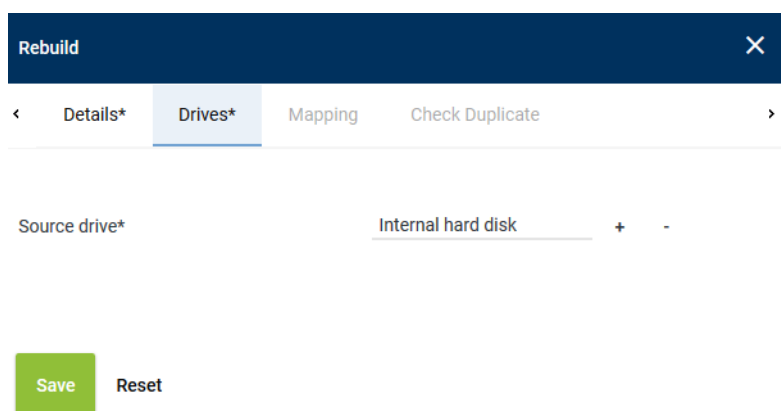
5.4.1.2 Tab Drives

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.



Rebuild [X]

< Details* **Drives*** Mapping Check Duplicate >

Source drive* Internal hard disk + -

Save Reset

Fig. 17: Tab Drives - Select source drive

Time zone Select the time zone from the drop-down list that the time indicated in the data to be imported refers to.

Source drive Select the drive from which the data is supposed to be imported, see [chapter "Assign drive", p. 31](#).

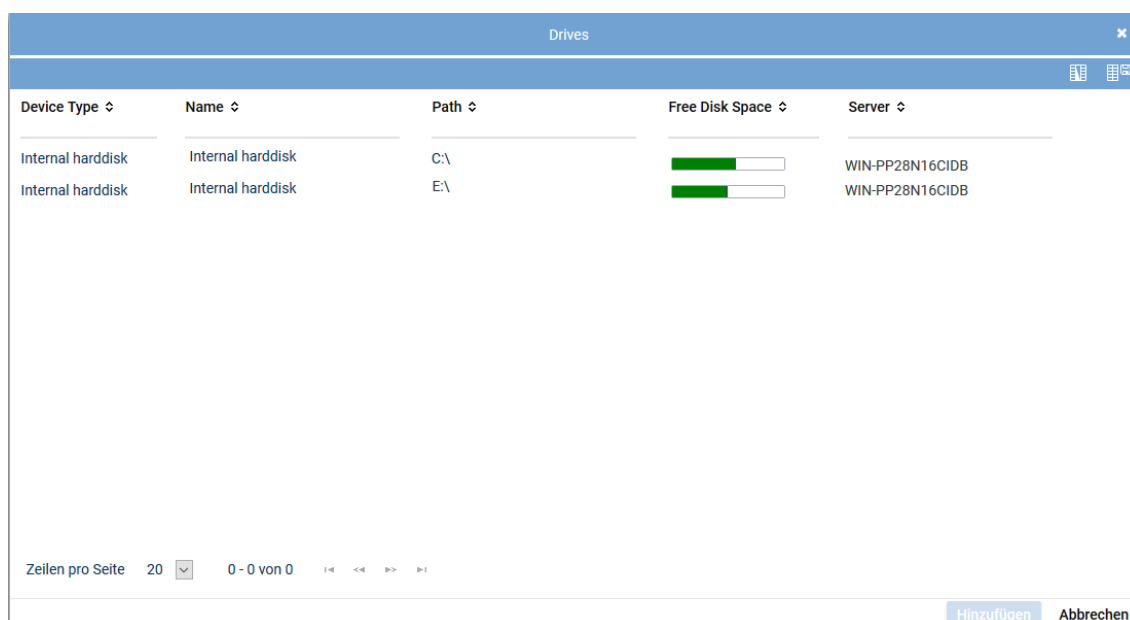


The import job only works for the local call pool.

1. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

5.4.1.2.1 Assign drive

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



Device Type	Name	Path	Free Disk Space	Server
Internal harddisk	Internal harddisk	C:\	<div style="width: 100%;"></div>	WIN-PP28N16CIDB
Internal harddisk	Internal harddisk	E:\	<div style="width: 100%;"></div>	WIN-PP28N16CIDB

Zeilen pro Seite 20 0 - 0 von 0

Hinzufügen Abbrechen

Fig. 18: 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*.

5.4.2 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.

5.5 Exchange drive

If a drive is defective and you have to exchange it, proceed as follows to migrate the call pool.

1. Stop all ASC service.
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.

5.6 Restore of EML speech analysis server

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.

5.7 Conclusive steps

1. Check that all licenses are available again after the restore processes and request new ones if required.
2. Reimport the certificates to enable encrypted connections.
3. Check whether recording is working correctly.
4. Check the replay of the recordings.

5.7.1 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 and generate the certificate on the recording server again.
4. If you would like to use external certificates, import the required certificates with *Certificate Import Tool*.



For detailed information about importing certificates refer to the installation manual for system providers *Installation of the recording software of ASC*.

6 Troubleshooting

If the conversations have not been imported correctly, check the log files. The logfiles can be found in directory *C:\Program Files (x86)\ASC\ASC Product Suite\logs*.

- *RecordingControl\ASC.RecordingControl.log*
- *EnterpriseCore\ASC.EnterpriseCore.log*
- *FileMan\ASC.FileMan.log*

List of figures

Fig. 1	System settings - Advanced settings - Open environment variable	8
Fig. 2	System settings - Create new system variable	9
Fig. 3	System settings - Name system variable and enter storage path	9
Fig. 4	System settings - Create system variable (example)	10
Fig. 5	Object explorer	11
Fig. 6	Configure general backup options	11
Fig. 7	Configure additional backup options	12
Fig. 8	Configure additional backup options	14
Fig. 9	Notification	15
Fig. 10	Restore options	22
Fig. 11	Select restore file	23
Fig. 12	Restore options	25
Fig. 13	Select restore file	26
Fig. 14	Exemplary main view of import jobs	28
Fig. 15	Tab Details - Configure import format NEO Rebuild	29
Fig. 16	Add tenant	30
Fig. 17	Tab Drives - Select source drive	31
Fig. 18	Add drive	31

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 protocol	13
Tab. 6	Configure tape drive	13
Tab. 7	Configure file options	14
Tab. 8	Configure compression	14
Tab. 9	Select restore file	23
Tab. 10	Select restore file	26
Tab. 11	Select destination	26

Glossary

CSV

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

PBX

Private Branch Exchange

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)

