

Rebuild of recordings



Administration manual for system providers

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

EVO^{flex} (country-specific)

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.....	4
2	Restrictions	5
3	Rebuild of recordings.....	6
3.1	Configure import job	6
3.1.1	Tab Details.....	6
3.1.1.1	Assign tenant.....	8
3.1.2	Tab Drives	8
3.1.2.1	Assign drive	9
4	Restoration of the database	10
4.1	Restore PostgreSQL database.....	10
4.1.1	Apply configuration data	10
4.1.2	Restore of the PostgreSQL database.....	10
4.1.3	Start updater	12
4.2	Restore MSSQL database.....	13
4.2.1	Restore of the MSSQL database.....	13
4.2.2	Start updater	15
	Glossary	18
	Index	19

1 Introduction

This document describes the preconditions and the procedure to rebuild recordings after a recording server has failed.

In case, conversation data has been lost, there is the possibility to restore the recordings and the corresponding additional data.

During the initial installation, a backup is set up for the PostgreSQL database that you can fall back upon in case of loss of data. The import function *neo* rebuild is destined to rebuild recordings which have not yet been covered by the database backup.

The recordings are imported to the system storage and the corresponding meta data to the database. After the import, exclusively the tenant configured in the import configuration has access to the recordings.



For a rebuild with the import format *neo* rebuild no license is required for the import.



For information about the activation and administration of licenses refer to the administration manual for system providers *License administration*.



Chat recordings cannot be imported.

Conversations which exclusively consist of meta data cannot be imported either.



Data which has been encrypted with one of the following methods cannot be imported:

- Neo key management
 - vormetric key management
-

2

Restrictions

The following functions are not supported:

- Restoration of encrypted data if its key is not available anymore.
- Restoration of statistics of the Recording Planner as they are stored exclusively in the database.

The following types of drives are not supported for import and export:

- EMC Centera
- S3
- ASC FS (*with the exception of importing archiving media from V10*)

3

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*.

3.1

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:

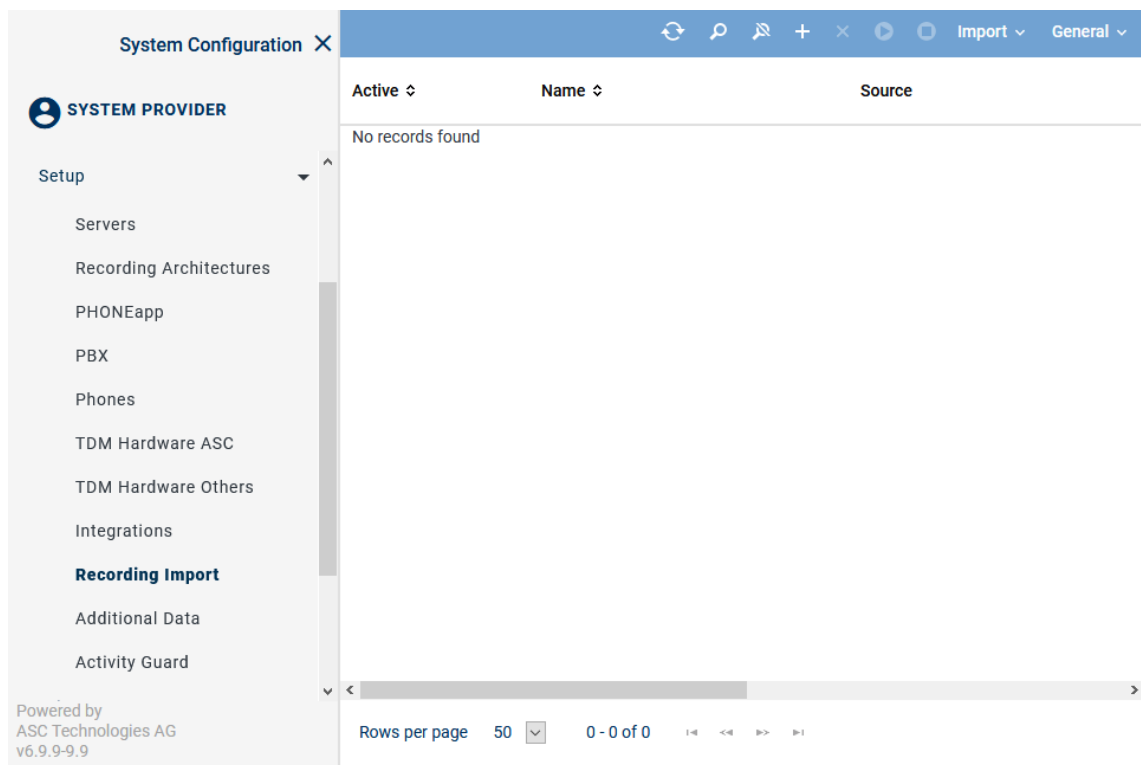



Fig. 1: Exemplary main view of import jobs

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

3.1.1

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.

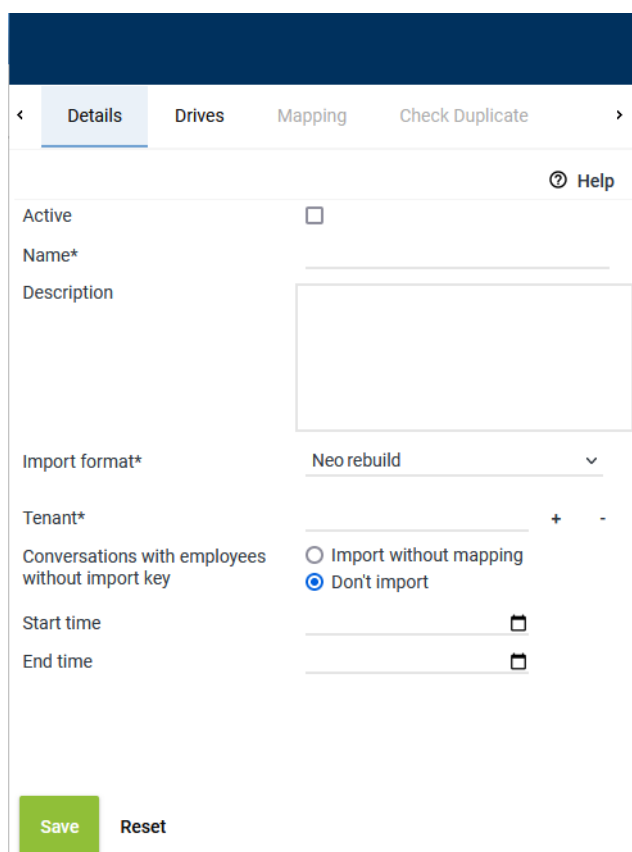




Fig. 2: Tab Details - Configure import format NEO Rebuild

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. 8.</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.

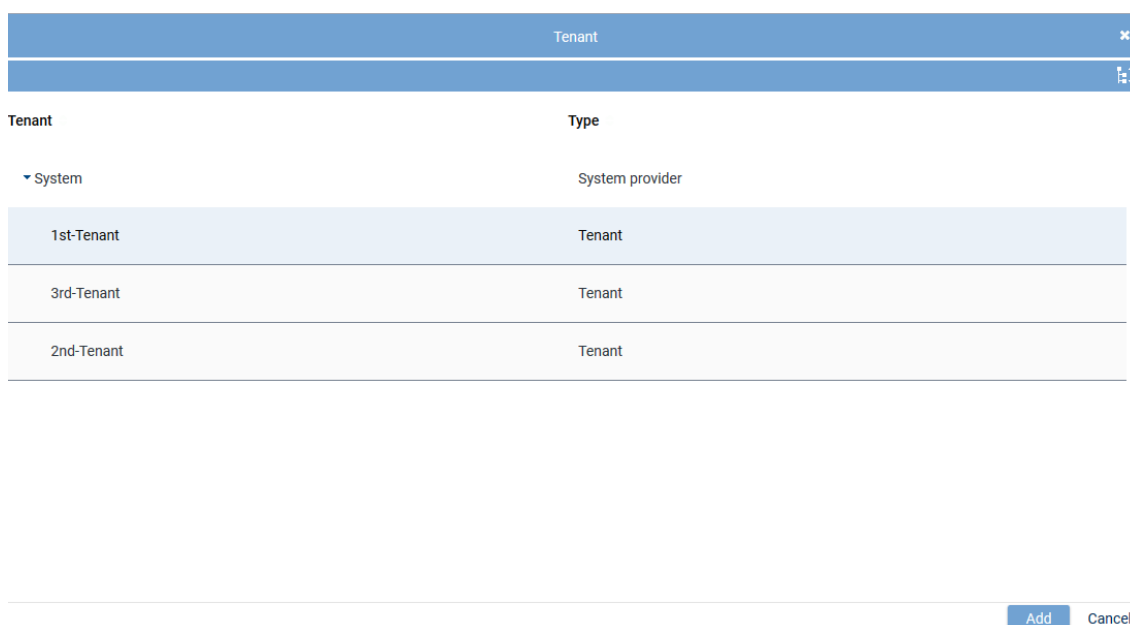
You can enter the date directly in both entry fields via the keyboard or by clicking on the icon .

NOTICE!

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

3.1.1.1 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. 3: 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*.

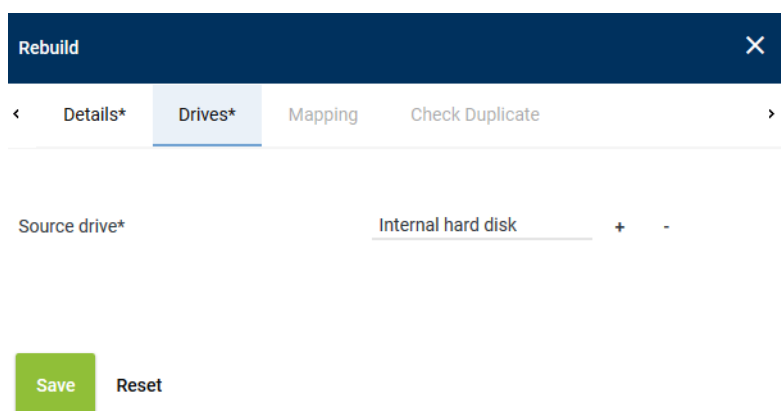
3.1.2 Tab Drives

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

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

Source drive* Internal hard disk + -

Save Reset

Fig. 4: 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. 9 .

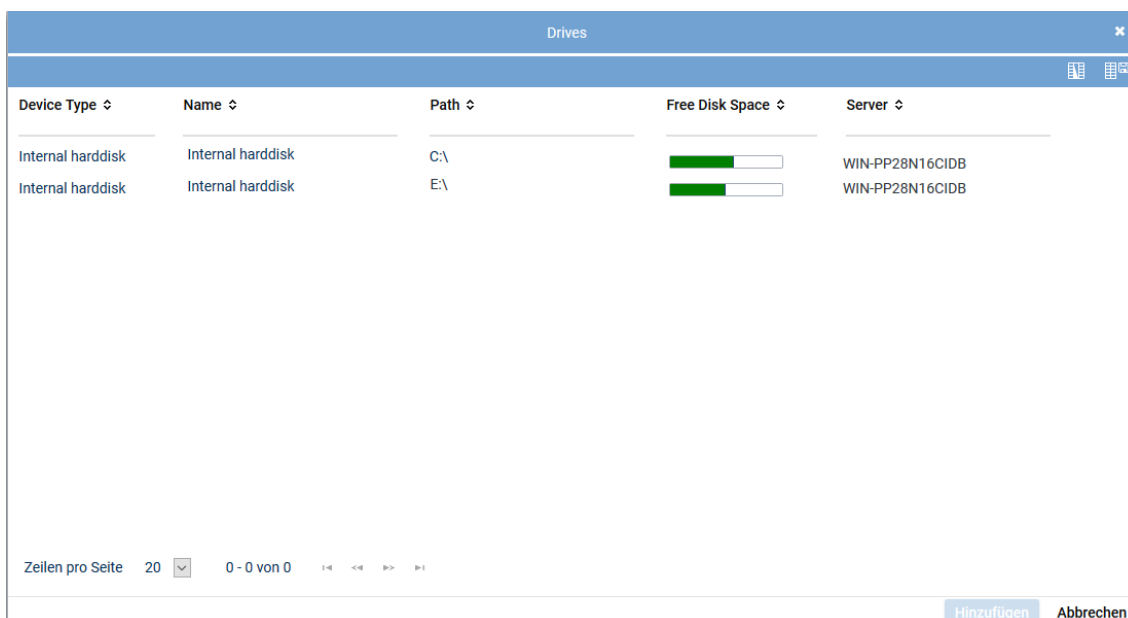


The import job only works for the local call pool.

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

3.1.2.1 Assign drive

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



Drives

Device Type ↕	Name ↕	Path ↕	Free Disk Space ↕	Server ↕
Internal harddisk	Internal harddisk	C:\	<div><div></div></div>	WIN-PP28N16CIDB
Internal harddisk	Internal harddisk	E:\	<div><div></div></div>	WIN-PP28N16CIDB

Zeilen pro Seite 20 0 - 0 von 0

Hinzufügen Abbrechen

Fig. 5: 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*.

4 Restoration of the database

4.1 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.

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

4.1.2 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.

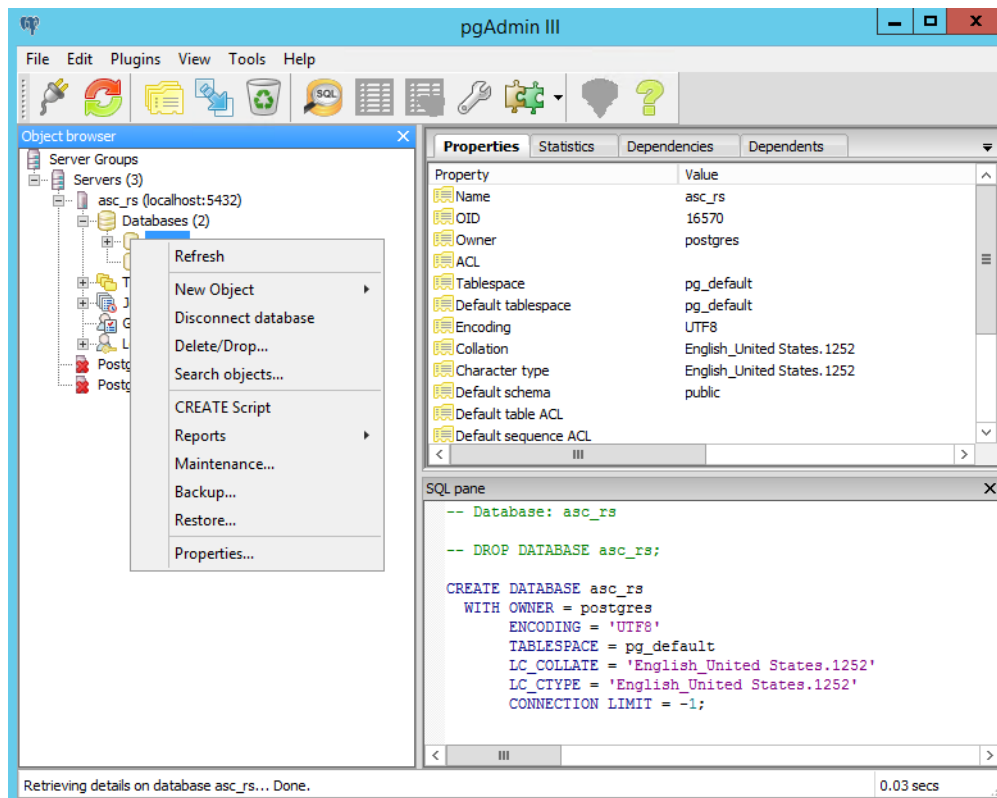


Fig. 6: Restore options

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

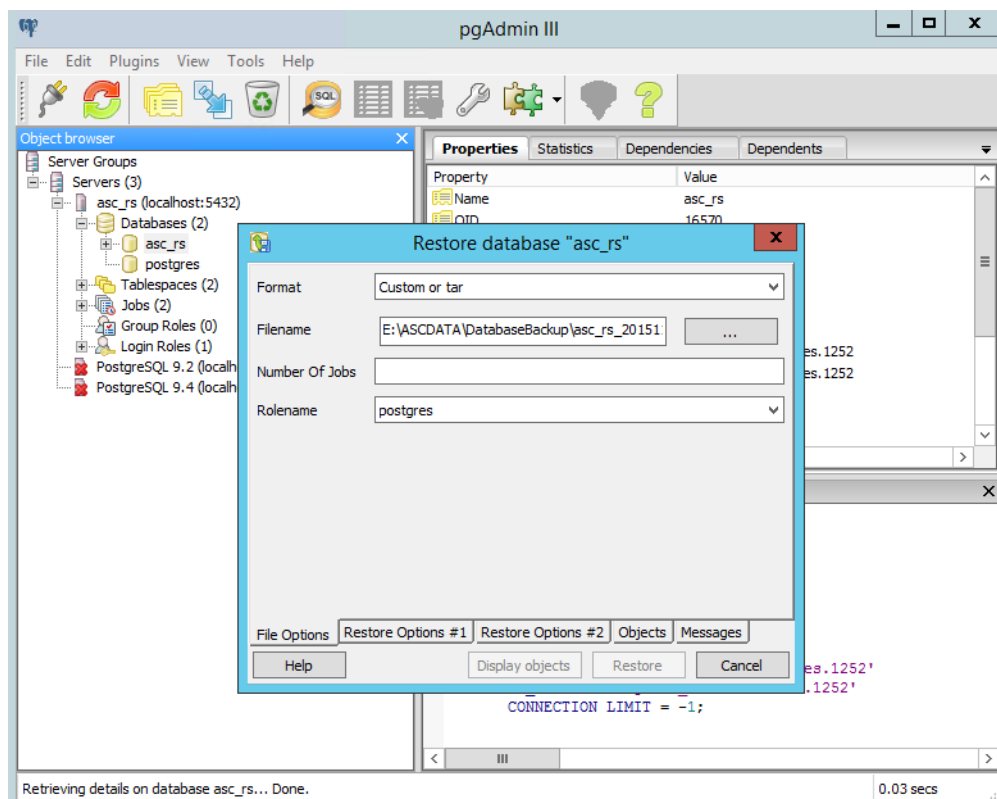



Fig. 7: Select restore file

- Select the following options for the restore:

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

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

Tab. 1: 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*.

4.1.3 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.

4.2 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.

4.2.1 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*.

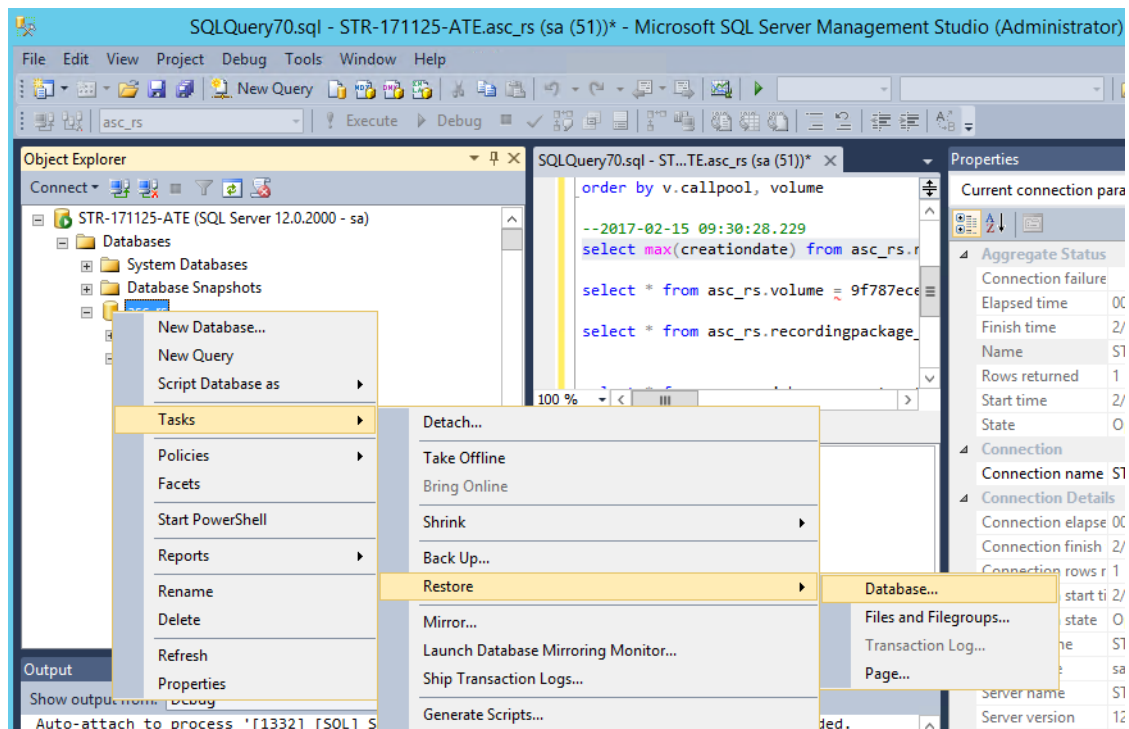


Fig. 8: Restore options

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

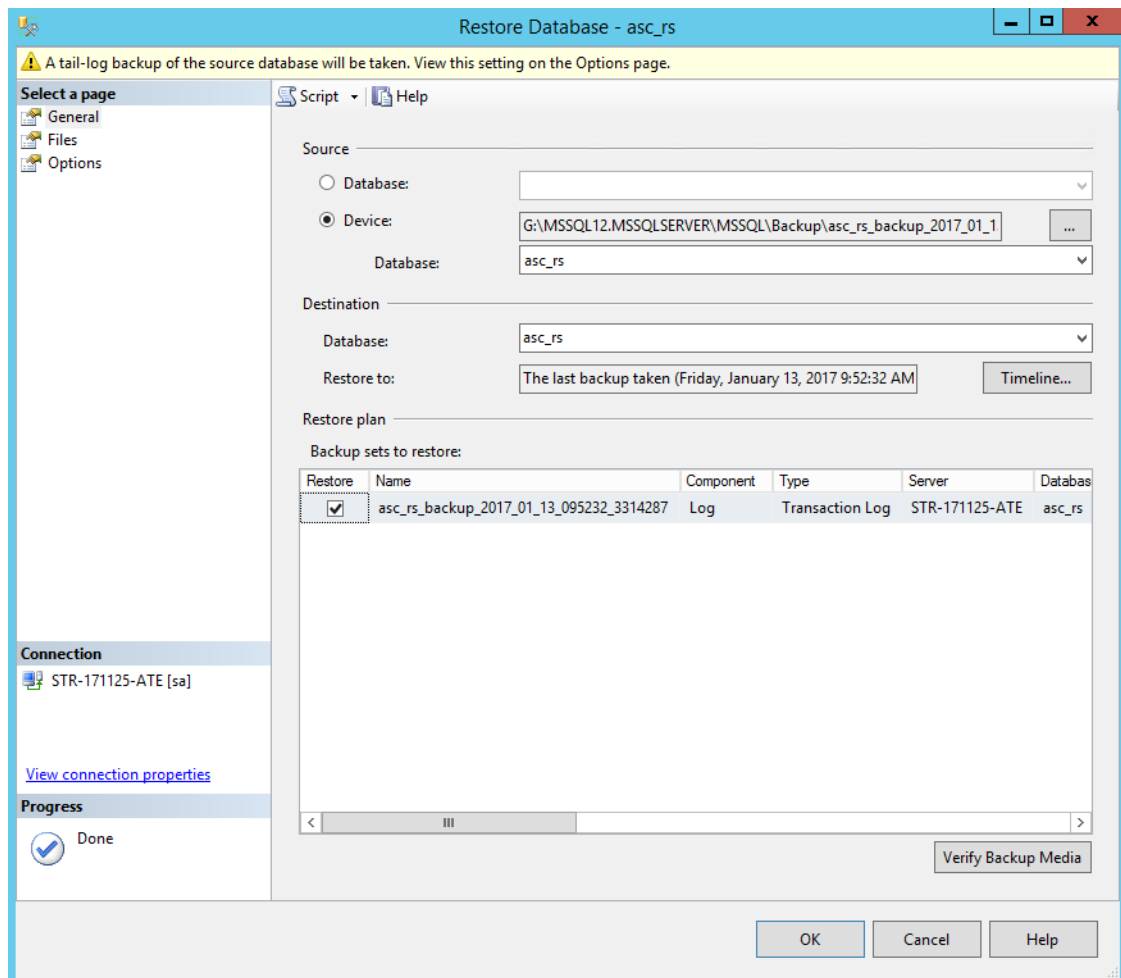


Fig. 9: Select restore file

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. 2: 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. 3: 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>.

4.2.2 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.

List of figures

Fig. 1	Exemplary main view of import jobs	6
Fig. 2	Tab Details - Configure import format NEO Rebuild.....	7
Fig. 3	Add tenant	8
Fig. 4	Tab Drives - Select source drive.....	9
Fig. 5	Add drive.....	9
Fig. 6	Restore options	11
Fig. 7	Select restore file	11
Fig. 8	Restore options	13
Fig. 9	Select restore file	14



List of tables

Tab. 1 Select restore file 11

Tab. 2 Select restore file 14

Tab. 3 Select destination 14

Glossary

PBX

Private Branch Exchange

Index