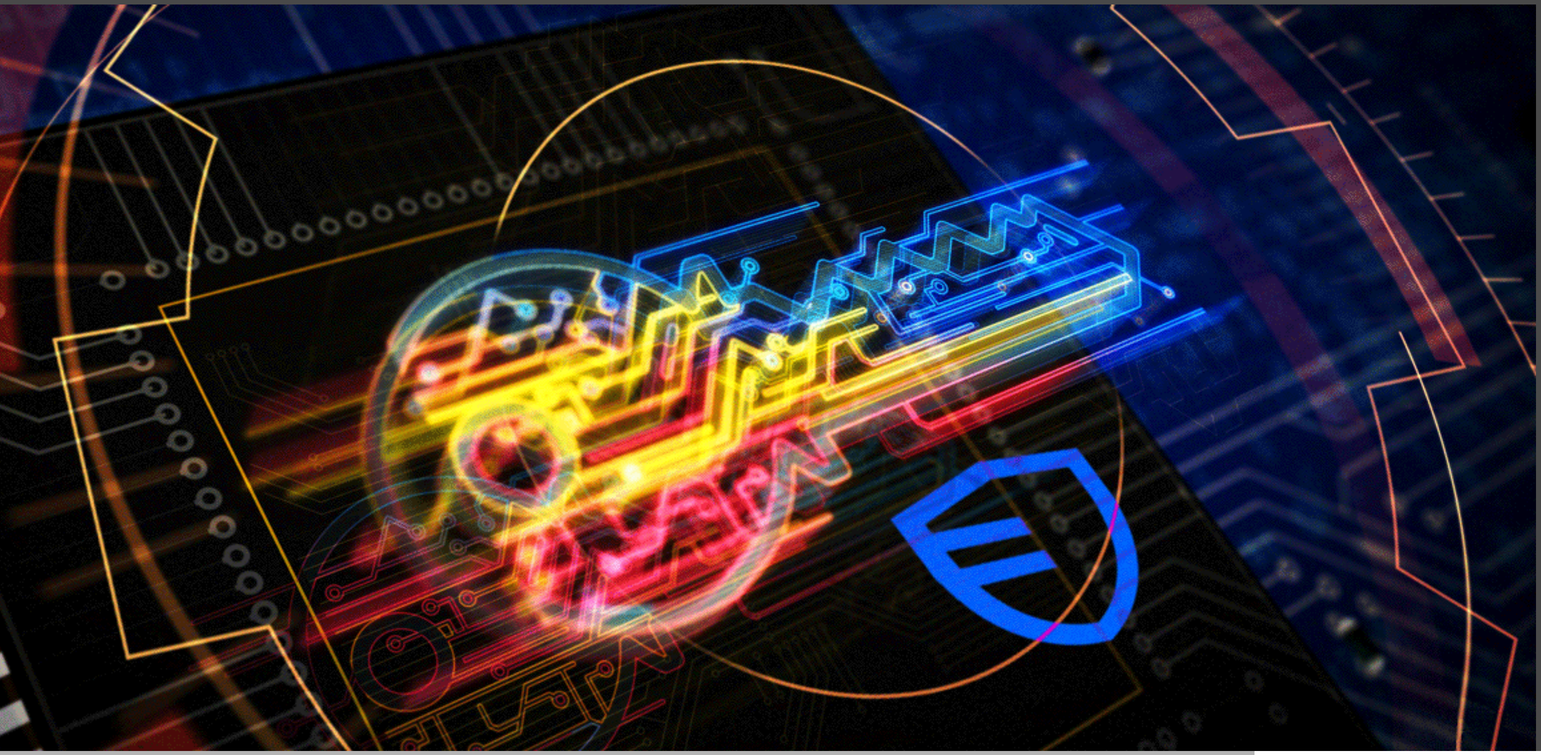
How to Export and Regenerate Encryption Keys in Devolutions Server



IN THE IT WORLD, PRODUCTIVITY AND EFFICIENCY ARE PRIORITIES — BUT NOTHING IS MORE IMPORTANT THAN SECURITY.

In the IT world, productivity and efficiency are priorities — but nothing is more important than security. The costs and consequences of breaches and leaks can be enormous. That is where encryption keys enter the picture.

In this article, we take a closer look at how to export and regenerate encryption keys in Devolutions Server. First, let us quickly summarize this solution for those who are unfamiliar with it.

About Devolutions Server

Devolutions Server is our globally-popular, full-featured **shared account and password management solution** with **add-on privileged access components**. It deploys rapidly, implements easily, and delivers the core features of a comprehensive PAM solution. Devolutions Server is designed to meet the ever-expanding security requirements of SMBs, while remaining very affordable. A free 30-day trial is available.

About the Encryption Keys in Devolutions Server

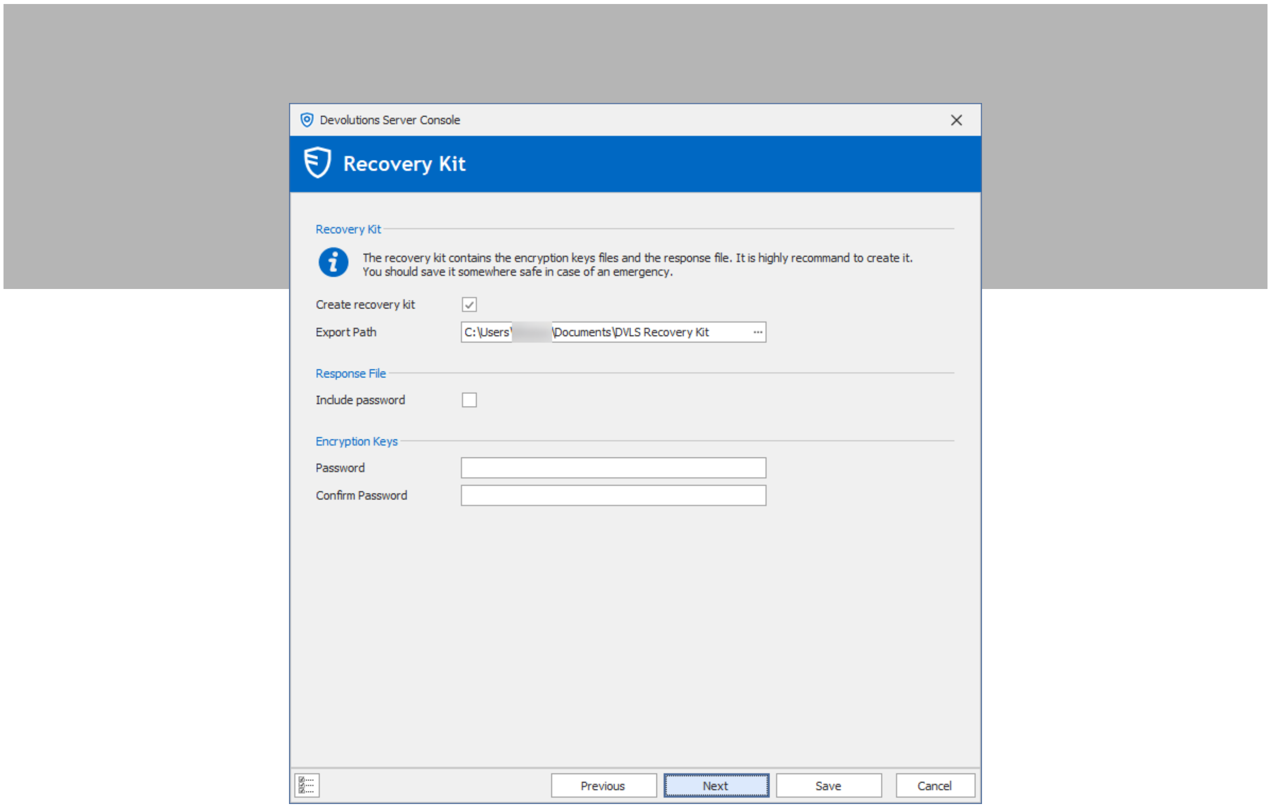
The encryption keys in Devolutions Server are used to encrypt data entries (connections, private vaults, documentation, and attachments). They are generated and stored in file “encryption.config”, which is stored on the server only. To encrypt data stored in the database, we use our open-source cryptography library that can be found at https://github.com/Devolutions/devolutions-crypto.

The encryption keys must be the same for each Devolutions Server instance of your High Availability/Load Balancing Topology that uses the same SQL database, or for a migration operation.

Important note: We strongly recommend storing your Recovery Kit or the encryption keys in a secure, yet easy-to-remember location outside of Devolutions Server, such as in Password Hub Business, Azure Key Vault, or AWS Key Management Service.

Creating and Storing a Recovery Kit

First of all, when you install your Devolutions Server instance, you will be promoted to create a Recovery Kit, which you will need in the event that you no longer have access to Devolutions Server, or for a load balancing topology. The Recovery Kit is a .ZIP folder generated by the Devolutions Server console, which contains **the encryption keys** and a response file (which can be used to re-install Devolutions Server with the same specifications as the initial install).



Devolutions Server Console

Recovery Kit

Recovery Kit

The recovery kit contains the encryption keys files and the response file. It is highly recommand to create it.
You should save it somewhere safe in case of an emergency.

Create recovery kit ☑

Export Path: C:\Users\[redacted]\Documents\DVLS Recovery Kit

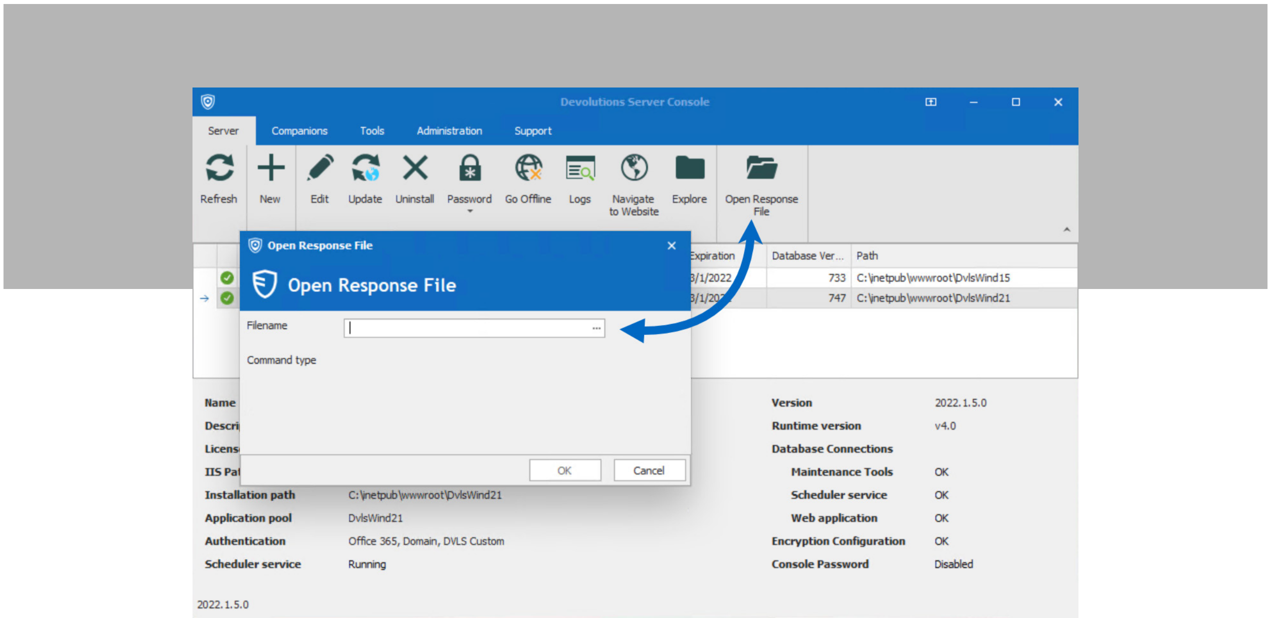
Response File

Include password □

Encryption Keys

Password

Confirm Password



Open Response File

Open Response File

Filename

Command type

Expiration	Database Ver...	Path
3/1/2022	733	C:\inetpub\wwwroot\DvlsWind15
3/1/202	747	C:\inetpub\wwwroot\DvlsWind21

Name		Version	2022.1.5.0
Descri		Runtime version	v4.0
Licens		Database Connections	
IIS Pat		Maintenance Tools	OK
Installation path	C:\inetpub\wwwroot\DvlsWind21	Scheduler service	OK
Application pool	DvlsWind21	Web application	OK
Authentication	Office 365, Domain, DVLS Custom	Encryption Configuration	OK
Scheduler service	Running	Console Password	Disabled

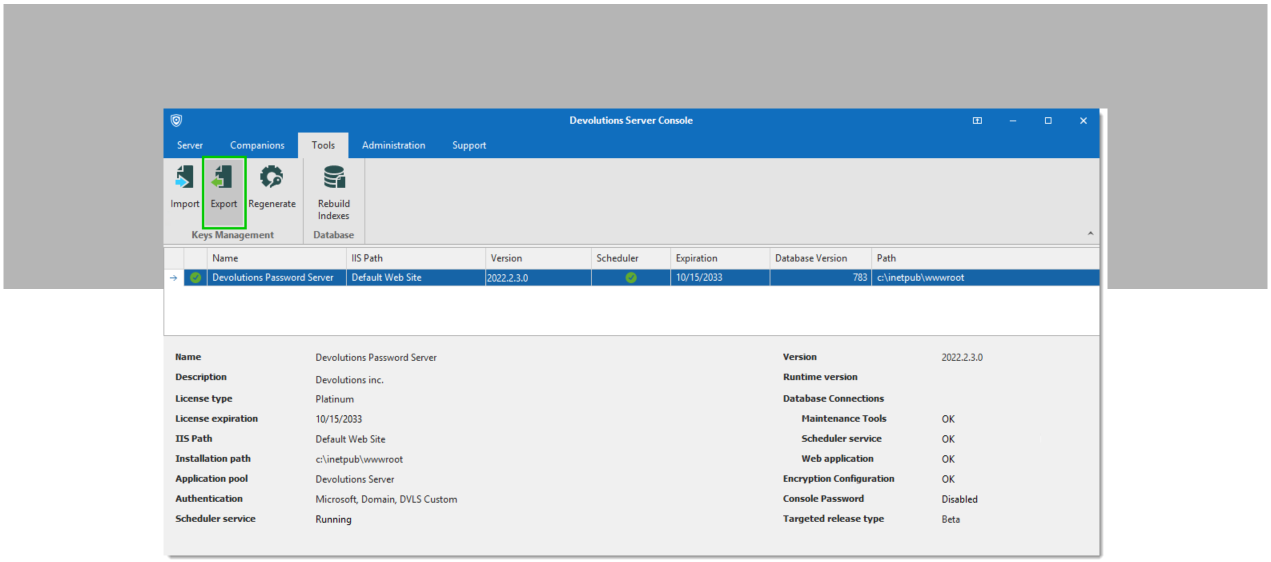
2022.1.5.0

Exporting the Encryption Key

Here are the steps for exporting the encryption keys. Please Note: if you need to upgrade Devolutions Server, please upgrade one instance at a time.

Step 1: Open the Devolutions Server Console.

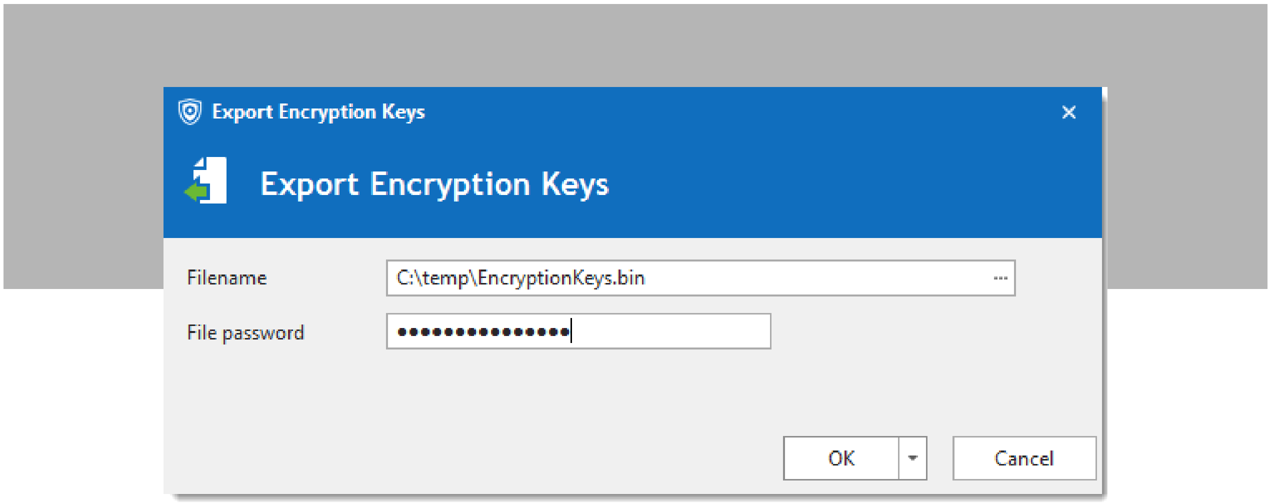
Step 2: Go in the Tools tab and click on the ***Export*** button.



Name	IIS Path	Version	Scheduler	Expiration	Database Version	Path
Devolutions Password Server	Default Web Site	2022.2.3.0	✓	10/15/2033	783	c:\inetpub\wwwroot

Name	Devolutions Password Server	**Version**	2022.2.3.0
Description	Devolutions inc.	**Runtime version**	
License type	Platinum	**Database Connections**	
License expiration	10/15/2033	**Maintenance Tools**	OK
IIS Path	Default Web Site	**Scheduler service**	OK
Installation path	c:\inetpub\wwwroot	**Web application**	OK
Application pool	Devolutions Server	**Encryption Configuration**	OK
Authentication	Microsoft, Domain, DVLS Custom	**Console Password**	Disabled
Scheduler service	Running	**Targeted release type**	Beta

Step 3: Select a destination file name and set a password to protect the file. Then click ***OK.***



Filename C:\temp\EncryptionKeys.bin

File password •••••••••••••••

Regenerating the Encryption Keys

There may be scenarios where you need to regenerate the encryption keys, such as if you suspect that your data base has been breached. Before we look at the steps for this process, please note: the regenerate operation will alter and re-encrypt the inner data of the SQL database of the Devolutions Server. This operation must be undertaken with the utmost care.

Step 1: Create a full database backup, and confirm that the backup is fully operational.

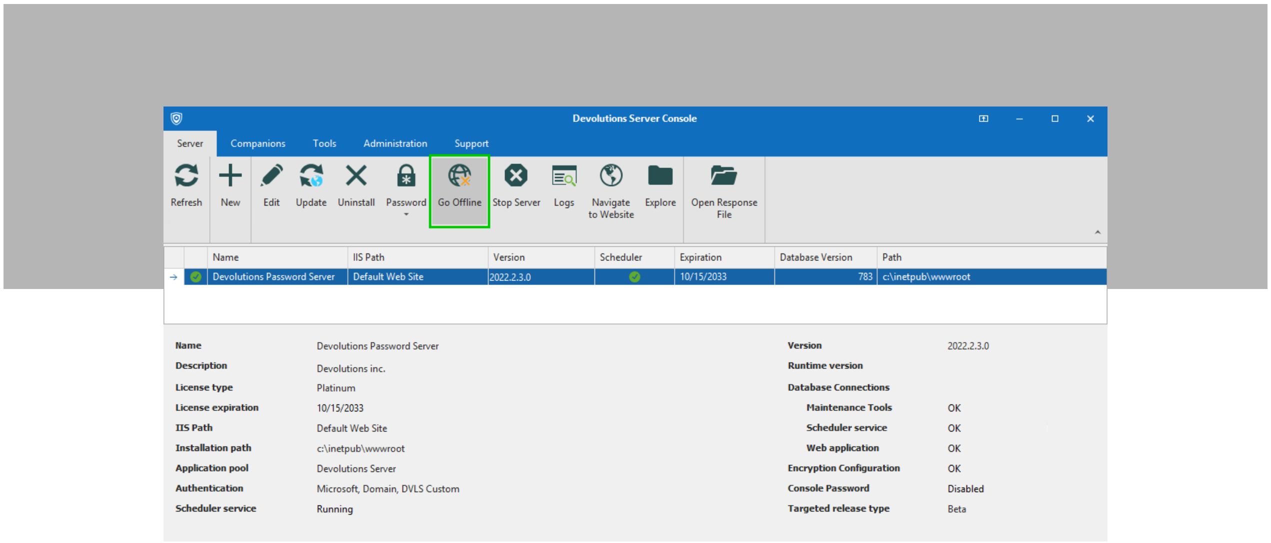
Backup the Database

Before performing any operation that could modify information in the SQL database, we highly recommend completing a backup of the SQL database. To avoid data loss, during the backup process all users must be in offline mode or disconnected from the Devolutions Server data source.

Step 2: Create a backup of the Devolutions Server web application folder.

Step 3: Export the existing encryption keys (see above steps 1 to 3 in the Exporting the Encryption Keys section.)

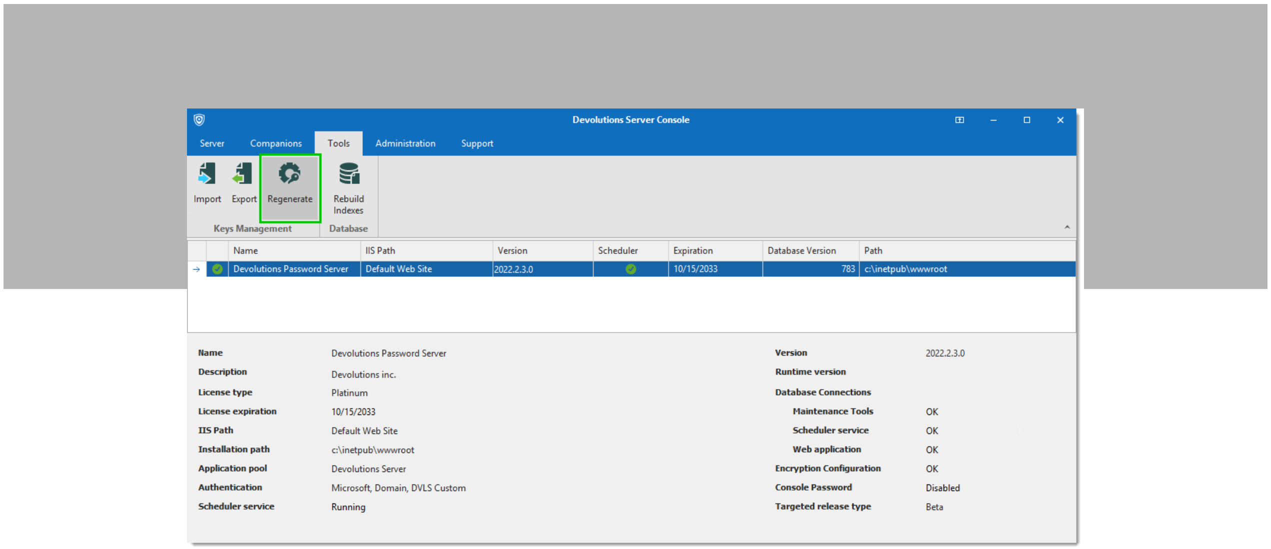
Step 4: Switch the Devolutions Server instance to offline mode using the ***Go Offline*** button.



		Name	IIS Path	Version	Scheduler	Expiration	Database Version	Path
→	✓	Devolutions Password Server	Default Web Site	2022.2.3.0	✓	10/15/2033	783	c:\inetpub\wwwroot

Name	Devolutions Password Server	**Version**	2022.2.3.0
Description	Devolutions inc.	**Runtime version**	
License type	Platinum	**Database Connections**	
License expiration	10/15/2033	**Maintenance Tools**	OK
IIS Path	Default Web Site	**Scheduler service**	OK
Installation path	c:\inetpub\wwwroot	**Web application**	OK
Application pool	Devolutions Server	**Encryption Configuration**	OK
Authentication	Microsoft, Domain, DVLS Custom	**Console Password**	Disabled
Scheduler service	Running	**Targeted release type**	Beta

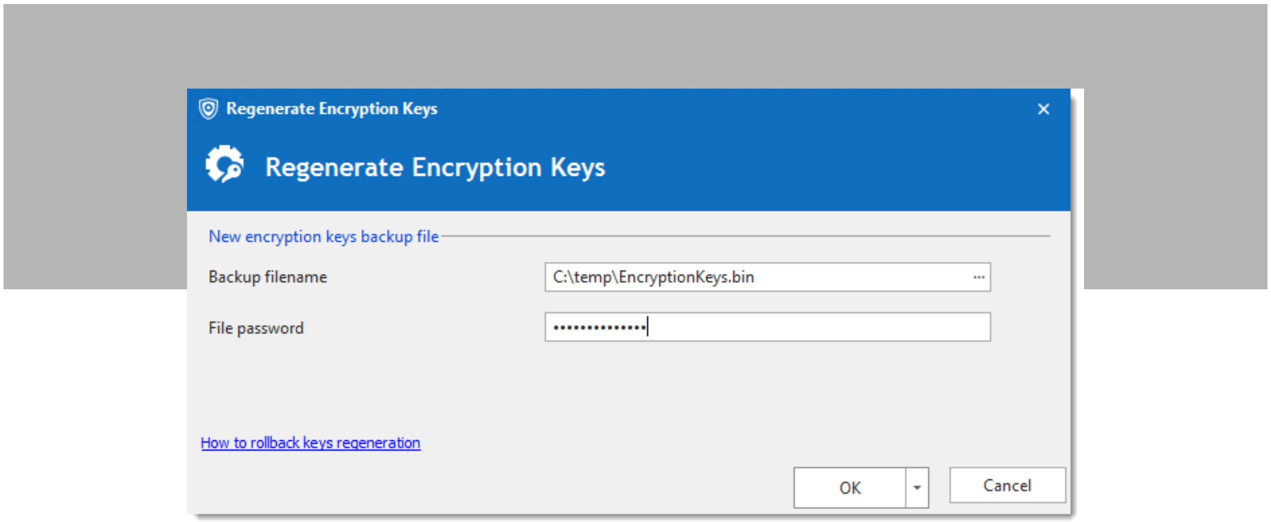
Step 5: From the Tools menu click the ***Regenerate*** button.



	Name	IIS Path	Version	Scheduler	Expiration	Database Version	Path
→	Devolutions Password Server	Default Web Site	2022.2.3.0	✓	10/15/2033	783	c:\inetpub\wwwroot

Name	Devolutions Password Server	**Version**	2022.2.3.0
Description	Devolutions inc.	**Runtime version**	
License type	Platinum	**Database Connections**	
License expiration	10/15/2033	**Maintenance Tools**	OK
IIS Path	Default Web Site	**Scheduler service**	OK
Installation path	c:\inetpub\wwwroot	**Web application**	OK
Application pool	Devolutions Server	**Encryption Configuration**	OK
Authentication	Microsoft, Domain, DVLS Custom	**Console Password**	Disabled
Scheduler service	Running	**Targeted release type**	Beta

Step 6: Set the destination filename and the password to protect the file that contains a backup of the regenerated encryption keys.

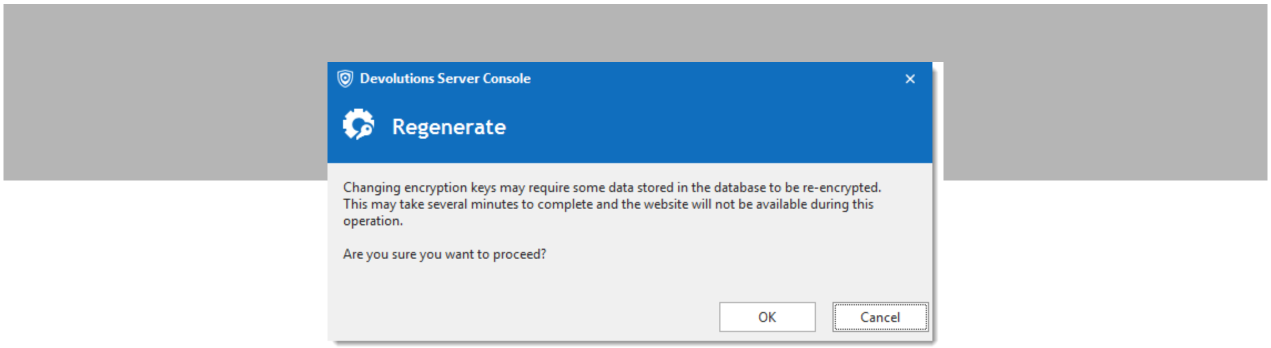

Regenerate Encryption Keys
Regenerate Encryption Keys
How to rollback keys regeneration
OK
Cancel

New encryption keys backup file

Backup filename: C:\temp\EncryptionKeys.bin

File password: ••••••••••••••

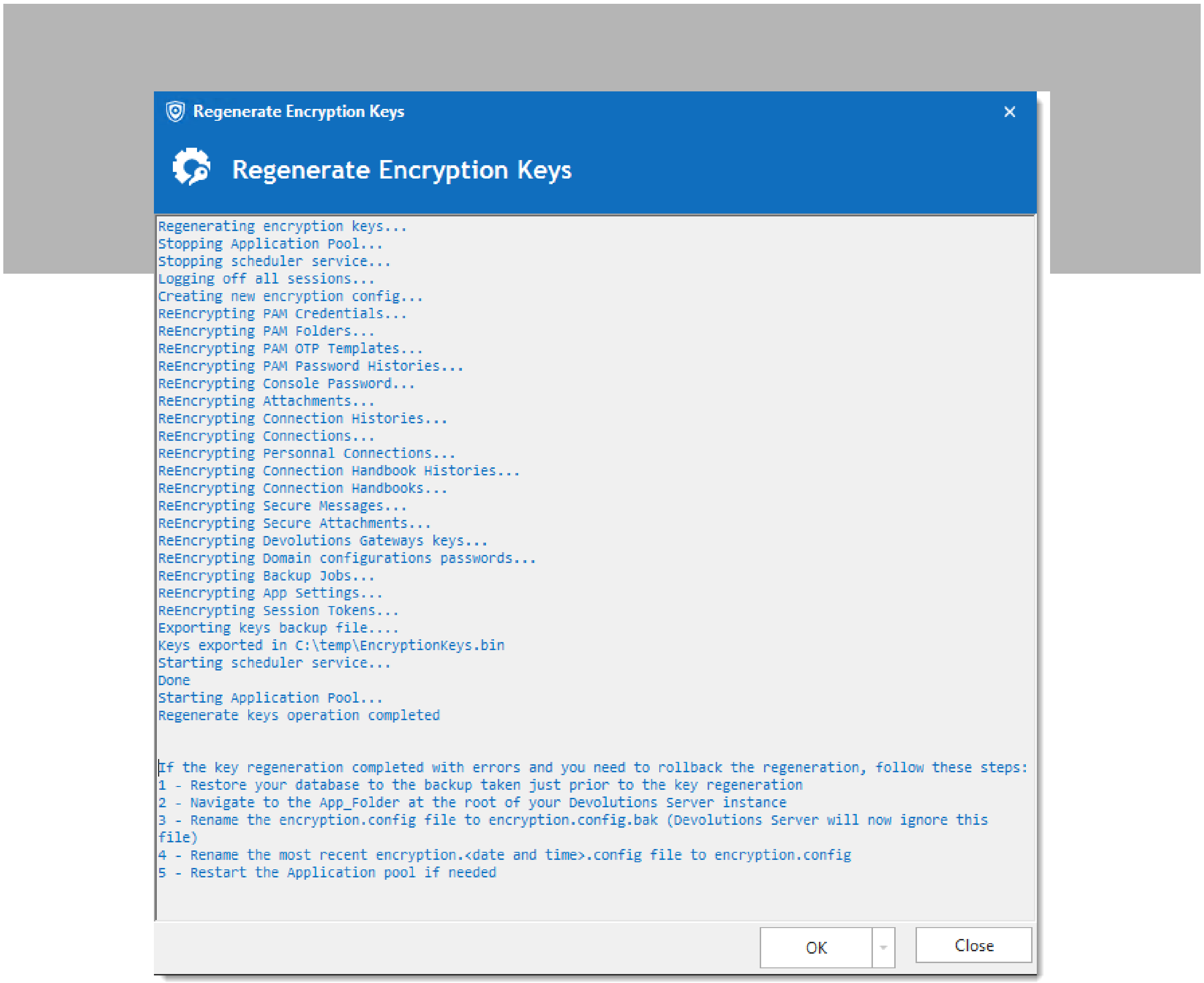
Step 7: A final warning will display before the regeneration process launches. Once you are ready to proceed, click OK.



Changing encryption keys may require some data stored in the database to be re-encrypted. This may take several minutes to complete and the website will not be available during this operation.

Are you sure you want to proceed?

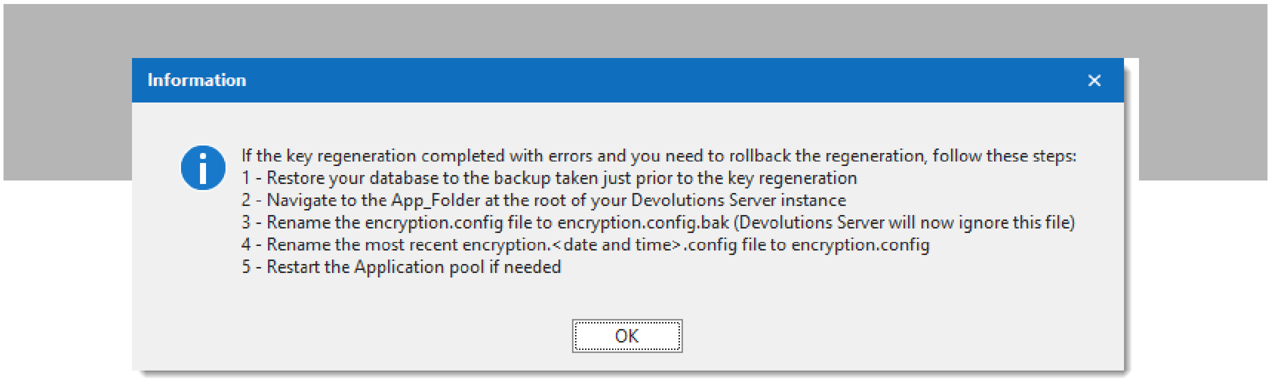
Once the process is complete, the following status message will display:



```
Regenerating encryption keys...
Stopping Application Pool...
Stopping scheduler service...
Logging off all sessions...
Creating new encryption config...
ReEncrypting PAM Credentials...
ReEncrypting PAM Folders...
ReEncrypting PAM OTP Templates...
ReEncrypting PAM Password Histories...
ReEncrypting Console Password...
ReEncrypting Attachments...
ReEncrypting Connection Histories...
ReEncrypting Connections...
ReEncrypting Personnal Connections...
ReEncrypting Connection Handbook Histories...
ReEncrypting Connection Handbooks...
ReEncrypting Secure Messages...
ReEncrypting Secure Attachments...
ReEncrypting Devolutions Gateways keys...
ReEncrypting Domain configurations passwords...
ReEncrypting Backup Jobs...
ReEncrypting App Settings...
ReEncrypting Session Tokens...
Exporting keys backup file....
Keys exported in C:\temp\EncryptionKeys.bin
Starting scheduler service...
Done
Starting Application Pool...
Regenerate keys operation completed


If the key regeneration completed with errors and you need to rollback the regeneration, follow these steps:
1 - Restore your database to the backup taken just prior to the key regeneration
2 - Navigate to the App_Folder at the root of your Devolutions Server instance
3 - Rename the encryption.config file to encryption.config.bak (Devolutions Server will now ignore this
file)
4 - Rename the most recent encryption.<date and time>.config file to encryption.config
5 - Restart the Application pool if needed
```

Note: In the unlikely event that an error occurs during the process, then please follow the instructions in the graphic below to restore your Devolutions Server instance to its previous state:



If the key regeneration completed with errors and you need to rollback the regeneration, follow these steps:
1 - Restore your database to the backup taken just prior to the key regeneration
2 - Navigate to the App_Folder at the root of your Devolutions Server instance
3 - Rename the encryption.config file to encryption.config.bak (Devolutions Server will now ignore this file)
4 - Rename the most recent encryption.<date and time>.config file to encryption.config
5 - Restart the Application pool if needed

Tell Us What You Think

We hope that you found this tutorial useful. Please let us know your thoughts by commenting below. Please also tell us what other tutorials you would like us to publish in the future.