PasswordState Enterprise Password Management

Automatic Backups

Domain Account using Network Share

This document and the information controlled therein is the property of Click Studios. It must not be reproduced in whole/part, or otherwise disclosed, without prior consent in writing from Click Studios.

Table of Contents

1. OV	ERVIEW	3
2. BAG	CKUP PERMISSIONS AND PREREQUISITES	4
21	CREATE PASSWORD LIST WITH THE ENABLED FOR RESETS OPTION SELECTED	4
2.1	CREATE PASSWORD RECORD	5
2.3	POWERSHELL REQUIREMENTS ON DATABASE SERVER	
2.4	GRANT BACKUP ACCOUNT ACCESS TO THE REMOTE MANAGEMENT USERS GROUP .	6
2.5	Share Permissions	6
2.6	BACKUP FOLDER PERMISSIONS	8
2.7	SQL DATABASE AND SERVER PERMISSIONS/REQUIREMENTS	8
3 (0)	NEIGURE BACKLIPS SCREEN	10
5. 001		
4. FAC	2	12
4.1	Manual Backups	12
4.2	Session Recording Files	
4.3	PASSWORD PROTECTING THE BACKUP FILES	12
4.4	AUTOMATIC RESET OF BACKUP ACCOUNT	12
4.5	BACKUP SPLIT SECRETS	12
4.6	ACCESS DENIED ERRORS WHEN PERFORMING BACKUP TESTS	13
4.7	BACKUP FILE NAMING CONVENTION	15
4.8	SQL Server Express Considerations	15
4.9	Azure and Amazon SQL Databases	16
5. SER	VER PERMISSION MATRIX	17

1. Overview

Passwordstate is an application that communicates to, and stores all or your data in a Microsoft SQL Database. In the event of a disaster, you may need to restore your database and Passwordstate installation files, which will require you to have them backed up.

Passwordstate has a built-in automatic backup feature which can be configured to suit your requirements. For example, you may already have another solution for your SQL database backups, so you can set Passwordstate to not backup up your database, but maybe just the install files.

Not only is the SQL database critical to have a backup of, but there are also encryption keys which are located in your web.config file. These too are also critical to have a copy of in the event of a disaster, so setting up the Passwordstate automated Backup feature will ensure you have everything you need to restore your environment.

This document will help you configure Passwordstate to use an Active Directory Domain account for the backups, and will also use a Network Share to store the data.

Please Note: If using cloud-based database services like Azure SQL or Amazon RDS, you cannot perform database backups using our software, as those platforms do not support it.

2. Backup Permissions and Prerequisites

All examples below are using an account we have created specifically for backups in Active Directory called "**Passwordstate Backup**". The username for this account is **pback**. This account is a member of the **Domain Users** security group only.

The Windows server where SQL is installed and hosting the Passwordstate database is called **dbserver01**.

We have a Network Share called **\\StorageServer01\Backups** located on another server called **StorageServer01**. This network share is converted from a folder called **C:\Data\Backups**.

2.1 Create Password List with the Enabled for Resets Option Selected

You may already have a Password List that is enabled for resets, but if you don't then you'll need to create one. Creating a List with this option will allow you to add in a Password Record that can automatically reset and validate the Domain account you will be using for backups:

Password List Details	Permissions	Confirmation
Site Location:	Internal	
Password List: *	Privileged Domain Accounts	
Description :		
Template:	Enabled for Password Resets	*
Image:	passwordresets.png	*
Template Description:	Perform password resets on a scheduled, or on a accounts	demand, for many different types of
	□ Link this Password List to the selected Temp	late. Disable future use of this Wizard

2.2 Create Password Record

Once you have a Password List ready, you can now add in a new Password Record. When creating this record, deselect the option "**Enabled for Resets**". By deselecting this option, Passwordstate will not try to automatically reset the password for the account. More information about this in the FAQ at the end of this document.

You should then choose the "Active Directory" account type, set the **Domain**, **Username** and current password for the account. You can test the password is valid by clicking the heartbeat icon.

ease edit the password	below, stored within the 'Privileged Domain Accounts' Password List	(Tree Path = $\)$.
password Vetails	notes security reset options heartbeat options	
Title *	Passwordstate Backup Acocunt	Q
Managed Account	Enabled for Resets Enabled for Heartbeat	
Account Type	2 Active Directory	•
Domain	contoso ×	Q
UserName	pback	2
Description		
Expiry Date		Ē
Password Generator	Default Password Generator	-
Password *	•••••	😫 🔍 🖩 🖖 🔚 🧡
Confirm Password *		
Password Strength	\bigstar	
Strength Status:		
Reset Tasks (0)	🛛 Added via Discovery 🛛 🖾 Compliance Mandatory 📝 Prevent	Bad Password

2.3 PowerShell Requirements on Database Server

As a once off process, the SQL Server PowerShell module must be installed on your Passwordstate database server, which in this guide is **dbserver01**. This module can be installed by opening an elevated PowerShell ISE session on your server, and execute the following lines of PowerShell code:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls -bor
[Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::Tls12
Install-Module sqlserver -Scope AllUsers -Force -AllowClobber
```

Installing this module will reach out to some online Microsoft repositories to which you should agree to any prompts to ensure a successful install. More information about this can be found here: https://docs.microsoft.com/en-us/sql/powershell/download-sql-server-ps-module?view=sql-server-ver15

2.4 Grant Backup Account Access to the Remote Management Users Group

Whilst still logged into your Database Server, open **Computer Management** and add your backup account (**pback** in this example), to the **Remote Management Users** group. This will allow the backup account to perform Powershell connections to the Database server, which will then execute back up commands:



2.5 Share Permissions

The Network Share will need the following **Change** permissions for the **backup** account, but also the **SQL Server** computer object. To create the Share if you haven't already, right click your folder and select **Properties** -> **Sharing** tab, then click **Advanced Sharing**. Tick the "**Share this Folder**" option and click the **Permissions** button:



Now you should grant your **backup** account and the **SQL Server Computer** object **Change** access as per these two screenshots – Note, your SQL Server object will end with a **\$** symbol:

Permissions for Backups			×	Permissions for Backups		×
Share Permissions Group or user names: DBSERVER01 \DBSERVER01s) Passwordstate Backup (pback@)				Share Permissions Group or user names: DBSERVER01 (Passwordstate Backup (pback)	DBSERVER01\$) ck@)	
Pemissions for DBSERVER01 Full Control Change Read	Add	Remove Deny		Permissions for Passwordstate Backup Full Control Change Read	Add	Remove Deny
ОК	Cancel	Apply		ОК	Cancel	Apply

When searching for your SQL server, ensure you tick the Computer Object Type so you can find it easily:

Select Users, Computers, Service Accounts, o	×	
Select this object type:		
Users, Groups, or Built-in security principals	Object Types	
From this location:		
dense de	Locations	
Enter the object names to select (<u>examples</u>):		Object Types
	Check Names	Select the types of objects you want to find.
Advanced OK Read	Cancel	Object types:
OK Cancel Apply		OK Cancel

2.6 Backup Folder Permissions

Even though you are using a Network Share, we need to grant the Backup Account **Modify** access to the folder that the Share is converted from. This is due to the way we impersonate the account when performing the backup operations:



2.7 SQL Database and Server Permissions/Requirements

Using SQL Management Studio tools, connect to your database server with any SQL admin account of your choice, and add in the backup account user under **Security** -> **Logins**. When adding this user, ensure you give it **db_backupoperator** permissions to the Passwordstate database:

Screenshot #1:

Object Explorer 🔹 👎 🗙							
Connect 🕶 🛱 🔲 🝸 🖒 🚸							
⊟ 📾 dbserver01. (SQL Server 15.0.2000.5 - \lsand)							
🗄 📫 Databases							
E Security							
🗄 🗐 Logins							
🗄 🖬 Serv New Login							
E Cred Filter							
⊞ = Cry; Start PowerShell							
E Aud Reports							
E Serv							
⊞ = Server Refresh							
⊞ ⁼ Replication							
🗄 💻 PolyBase							
🗄 🖷 Always On High Availability							
🗄 🖷 Management							
🗄 🖷 Integration Services Catalogs							
县 SQL Server Agent (Agent XPs disabled)							
🗄 🗉 XEvent Profiler							

Screenshot #2



Screenshot #3



3. Configure Backups Screen

In Passwordstate, go to Administration -> Backups -> Settings and add in the backup account that you previously set up in Step 2.2 of this document. Search for the account name and select the matching result to set the account:

ailed below are the	settings required to allow Passwordstate to backup its own folder, and a copy of the database if required.
backup settings	
Backups Accou	nt
Please search for a	ind select either roomain, or local Windows account below, which will be used for performing backups of Passwordstate.
Account * : pa	sswordstate
	Privileged Domain Accounts -> pback (Passwordstate Backup Account)
Backup Sche	
Backup Sche Specify setting	
Backup Sche Specify setting Enable Backup	
Backup Sche Specify setting: Enable Backup Backups To Kee	2

Next, select the option to **Enable Backups** and choose a schedule of your choice. Add in the **Network Share** path for both web files, and database backup paths, and configure any other settings as appropriate on this screen. Please note the option for **Database Location** is enabled because in this example, SQL is installed on a different server to the Passwordstate website.

	instructions	test permission results
Backups Account		
Please search for and	l select either a d	omain, or local Windows account below, which will be used for performing backups of Passwordstate.
Account * : \Priv	ileged Domain /	Accounts -> \pback -> Passwordstate Backup Account Q
Backup Start Time Backup Every Web Files Backup Pa	th :	18 V Hour 00 V Minute 24 Hours V \\StorageServer01\Backups
Database Backup Pat	th :	* To backup to a network share location, specify the path in the format of \\ <servername>\<sharename> \\StorageServer01\Backups \\backup up a network share to ation, specify the path in the format of \\<servername>\<sharename></sharename></servername></sharename></servername>
Backup Database		Vou should only deselect this option if you have your own established SQL Database backup process.
Database Location		Check If your Database is hosted on a different Server compared to where Passwordstate is installed.
SQL DINS LOOKUP	:	Check this option if you want FQDN connectivity to SQL Server i.e. SQL Server Aliases.
Backup Split Secrets		Check this option if you would like your encryption keys (split into secrets) backed up into a separate zip file.
Password Protect Ba	ckup Zip Files :	Select this option if you want to password protect your zip files with the password from the selected Backup

You should now be able to press the **Test Permissions** button on this page and if all configured correctly, you will get a successful result and your configuration of backups is complete.

[®] Backup Setting	IS			
etailed below are the s	settings required to	allow Passwordstate to backup its own folder, and a copy of the database if required.		
backup settings	instructions	test permission results		
lease click the Test Pe	ermissions button b	pelow in order to confirm correct permissions for your backup account.		
est Permission Resu	lts			
Testing SQL Server of Testing SQL Server of est Completed Succe	ersion of PowerShe Jatabase server pre Jatabase backup	n on web server		
atus:		Test Permission:	s Save	Cance

4. FAQ

4.1 Manual Backups

You can run a manual backup at any time if you have configured your settings correctly by clicking the **Backup Now** button:

Passwordstate v9.0 (Build 9000)			
 Passwordstate Administration Account and Host Discovery Active Directory Domains Auditing Auditing Graphs 	Backups and Upgrad Below is a history of all web and From this screen you can specif	d database backups for Passwordstate. I database packups for Passwordstate.	kups and upgrades, as well as initiate backups or upgrades.
Authorized Web Servers	Backup Date	Backup Detail	
Backups and Upgrades Bad Passwords	T	T	
Browser Extension Settings	No records to display.		
Brute Force Blocked IPs	Settings Send Outage N	Jotification Backup Now Up	grade Now Purge Logs Verbose Logging Grid Layout Actions 🔻
🗹 Email Notification Groups			
🗠 Email Templates			
Emergency Access			

4.2 Session Recording Files

If using the Browser Based version of the Remote Session Launcher, Session Recordings will not be included in the standard Passwordstate backup functionality, due to the potential size of the files. If you have left the recording folder in the default path, then you need to organize your own backups of these files

4.3 Password Protecting the Backup Files

One of the options on the backups page is to Password Protect your zip files. If you have selected this option, then it is imperative you know the password. We'd recommend storing this in a safe place outside of Passwordstate. Without knowing this password, you will not be able to access your backup files.

4.4 Automatic Reset of Backup Account

If you select the option '**Enable for Resets**' for your account on your Password Record, and you have the option to password protect your zip files on the backups page, then it is imperative you know the password after it is reset. We'd recommend storing this in a safe place outside of Passwordstate. Without knowing this password, you will not be able to access your backup files.

4.5 Backup Split Secrets

Backup Split Secrets is another option on the backup **Settings** page you can choose to ensure you have a copy of your encryption keys, half of which reside in your web.config file, and the other half are located in your database. These encryption keys are critical when restoring your environment. By enabling this option, these keys will get backed up to the **Web Files Backup Path**.

4.6 Access Denied Errors when Performing Backup Tests

If you have configured everything as per this documentation, but are still getting errors performing the Permission Tests, please check the following:

Troubleshooting Step #1:

Confirm that the account you set up for backups, has a correct password set within Passwordstate. You can confirm this by opening the Password Record you created, and click on the Heartbeat icon.

Troubleshooting Step #2:

Ensure the account is not locked out in Active Directory

Troubleshooting Step #3:

Investigate if you have a policy applying to your server that is denying the Backup Account from logging on. To check this, run the command "**secpol.msc**" on your Passwordstate server, and the server where you have your network share located, and investigate these options:

a Local Security Policy							
File Action View Help							
🗢 🄿 🙍 💼 🗟 🖬							
here a security Settings	Policy	Security Setting					
> 📴 Account Policies	Access Credential Manager as a trusted caller						
 Local Policies 	Access this computer from the network	Everyone Administrators Users Backup Operators					
> 📴 Audit Policy	Act as part of the operating system						
> 📴 User Rights Assignment	Add workstations to domain						
Security Options	Adjust memory quotas for a process	I OCAL SERVICE NETWORK SERVICE Administrators					
> Windows Defender Firewall with Advar	Allow log on locally	Curet Administratory Lieur Backup Operatory					
Network List Manager Policies	Allow log on through Remote Deskton Services	Administrators Personal Deskton Llear					
> Public Key Policies	Administrators Rankur Operators Administrators Rankur Operators						
Software Restriction Policies	Bupace traverse checking	Partimistation power of the second seco					
Application Control Policies	ug sypass traverse enecking Everyone,LIOCAL SERVICE,Administrators,Users,Backup Operators						
Security Policies on Local Computer	des on Local Computer Grant the system time LOCAL SERVICE Administrators						
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration						
	Create a pageme	Partitistators					
	Create a loken object	LOCAL SEDURCE NETWORK SEDURCE Administratory SEDURCE					
	Create global objects	LOCAL SERVICE/VETWORK SERVICE/Administrators/SERVICE					
	Create permanent shared objects	Administration					
	Debug programs	Administrators					
	Debug programs	Administrators					
	Deny access to this computer from the network	oust					
	Deny log on as a batch job						
	Deny log on as a service	Cont.					
Deny log on locally		Guer					
Enable computer and user accounts to be trusted for delegati							
Enable computer and user accounts to be trusted for delegat		Administrators					
	Generate segurity audite						
Imperconate a client after authentication		LOCAL SERVICE, VELWORK SERVICE					
	Inspector a process working set	Local Service INFORM SERVICE Administrators, SERVICE					
	Increase a process working set	users Administratory Window Managor/Window Managor Group					
Increase scheduling priority		Administrators, window Manager (Window Manager Group					
	Lock pages in memory	Administrators					
	Lock pages in memory	Administrator Radium Operator: Performance Los Uror					
	log on as a patient	NIT SERVICES ALL SERVICES					
	Manage auditing and security log	IVI JERVICE VILL JERVICES					
	Modify an object label	Mutuitistatois					
	Modify firmware environment values	Administrators					
	Contain an impersonation token for another user in the same	Administrators					
	Deform volume maintenance tasks	Administrators					
	Profile single process	Administrators					
	Profile system performance	Administrators NT SERVICE/WdiSanicaHost					
	Remove computer from docking station	Administratore licere					
	Replace a process level token	I OCAL SERVICE NETWORK SERVICE					
	Restore files and directories	Administrators Backup Operators					
	Shut down the system	Administrators Users Backup Operators					
	Synchronize directory service data						
	Take ownership of files or other objects	Administrators					

Troubleshooting Step #4:

Another reason this error may happen is due to the way we impersonate the backup account. As the Passwordstate website runs under the identity of Network Service by default, which is a built in IIS account, we need to impersonate the backup account when performing tests, so it's the backup account you have configured that effectively performs the backup.

There are three Microsoft values for this impersonation, and the default value is 2. You can change this impersonation type to either 4, or 9 using SQL Management Studio Tools, when connected to your Passwordstate database server.

To change the Impersonation value to 4, run the following SQL Script: (change values to 9 if 4 does not work)

Use Passwordstate Update BackupSettings Set BackupDatabaseImpersonation = 4 Update BackupSettings Set BackupEncryptionKeysImpersonation = 4 Update BackupSettings Set BackupFilesImpersonation = 4 Update BackupSettings Set BackupTest1Impersonation = 4 Update BackupSettings Set BackupTest2Impersonation = 4 Update BackupSettings Set BackupTest3Impersonation = 4 Update BackupSettings Set BackupTest4Impersonation = 4 Update BackupSettings Set BackupTest4Impersonation = 4 Update BackupSettings Set UlImpersonation = 4 Update BackupSettings Set ServiceImpersonation = 4

If neither of these impersonation values work, please revert the values back to the default values of 2.

If you still have issues running the tests, please contact Click Studio Support and send a screenshot of the test results for further analysis.

Troubleshooting Step #5:

If you find that the Passwordstate SQL database is not being backed up, either on a schedule or you notice an error when doing a test, please check the following settings:

- If your database resides on a separate server to where you have Passwordstate installed, ensure you have configured the "Database Location" setting on the backups page appropriately
- If your SQL Services are configured to run under the identity of a custom account, then that account too will
 need access to your database, and network share. Unless you have a specific reason to run your services
 under a custom account, it may be easier to change the Log On As value back to the defaults, which can be
 seen in the screenshot below:

Sql Server Configuration Manager File Action View Help									
SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration (32bit SQL Server Network Configuration (32bit) SQL Server Networ	Name SQL Server (MSS SQL Server Browser	State Running Stopped	Start Mode Automatic Other (Boot, Syste	Log On As NT Service\MSSQLSERVER NT AUTHORITY\LOCALSERVICE	Process ID 2808 0	Service Type SQL Server			
> ⇒ SQL Native Client 110 Configuration (Sci) ⇒ SQL Server Network Configuration > ➡ SQL Native Client 11.0 Configuration	SQL Server Agent	Stopped	Manual	NT Service\SQLSERVERAGENT	0	SQL Agent			

4.7 Backup File Naming Convention

The last section of the settings page gives you control of what your zip files should be called. These values can be changed to anything you like. The current date and time of the backup operation will be appended to these file names below.

The **Test Permissions** button at the bottom of the page can be used to check all your settings are valid.

Please specify the file naming conven	rention for your backup zip file	s below - the current data and time will be appended to these file names.	
Web Files Backup Name	: PasswordstateFiles		
Database File Backup Name	: PasswordstateDB		
Split Secrets File Backup Name	: PasswordstateKeys		
		· · · · · · · · · · · · · · · · · · ·	
		Test Permissions Save	Cancel

4.8 SQL Server Express Considerations

If you're using SQL Server Express on a different server to where you installed Passwordstate, please ensure the **TCP/IP Protocol** is enabled (use **SQL Server Configuration Manager** -> **Protocols for SQLEXPRESS**)

Sql Server Configuration Manager			
File Action View Help		/	
🗢 🔿 🖄 🗟 🛛			
SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration Protocols for SQLEXPRESS SQL Native Client 11.0 Configuration	Protocol Name	Status Enabled Disabled Enabled	

By default, SQL Express configures the TCP/IP Protocol to communicate on a dynamic port. If you have a firewall enabled on your database server, you may need to set a static port in the TCP/IP properties which will match your firewall rule. Restart the service again after configuring the option in the screenshot below:

	TCP Port	
	IP4	
	Active	Yes
	Enabled	No
	IP Address	127.0.0.1
	TCP Dvnamic Ports	0
	TCP Port	
Ξ	P5	
	Active	Yes
	Enabled	No
	IP Address	fe80::5efe:192.168.0.6%12
	TCP Dynamic Ports	0
	TCP Port	
Ξ	IP6	
	Active	Yes
	Enabled	No 🥒 📃
	IP Address	fe80::100:7f:fffe%13
	TCP Dynamic Ports	0
	TCP Port	
Ξ	PAII	
	TCP Dynamic Ports	
	TCP Port	1433 👻

4.9 Azure and Amazon SQL Databases

If you are using either an Azure or Amazon SQL database service to host your Passwordstate data, our backup process will not work with those services as they do not support the Powershell backup commands we use.

We'd recommend configuring those cloud services to back up your database, and then deselect the database backup option in Passwordstate.

5. Server Permission Matrix

So far, this document used an example of having your Passwordstate database hosted in SQL on a separate server to where you have Passwordstate installed. It also assumed you had your backup share on a third, separate server. Below is a matrix to consider if you have a slightly different setup to the above example.

Database on Passwordstate Web Server	Share Permissions	Share Folder NTFS Permissions	Database Permissions
Local Share on Passwordstate Web Server	Change for Backup Account Change for SQL Server Service - Log On As Account	Modify for Backup Account	db_backupoperator Permissions in SQL Server for Backup Account
Local Folder on Passwordstate Web Server		Modify for Backup Account	db_backupoperator Permissions in SQL Server for Backup Account
Remote Network Share	Change for Backup Account Change for SQL Server Host Name	Modify for Backup Account	db_backupoperator Permissions in SQL Server for Backup Account

	NTFS Permissions	Permissions
ange for Backup Account ange for SQL Server Host me	Modify for Backup Account	db_backupoperator Permissions in SQL Server for Backup Account Backup Account in Remote Management Users Security Group PowerShell Remoting on SQL Server Host
ar ar m	nge for Backup Account nge for SQL Server Host ne	nge for Backup Account nge for SQL Server Host ne Backup Account