Passwordstate

Enterprise Password Management

Upgrade Instructions

Table of Contents

1. Upgrade Overview

This document will detail instructions for upgrading to the latest build of Passwordstate 9. It will also detail instructions for upgrading any additional modules if you have them already installed.

Please reference the **Upgrade Dependency Matrix** section and the end of this document, to confirm if any dependant modules also need to be upgraded, when you upgrade your core Passwordstate installation.

If you are unsure if you have any additional modules installed, please see section "**Find Where any Dependant Modules are Installed**" in guide below

- If you are upgrading from a build prior to 9493, please read the section "**Build 9493 Database Considerations**" below.
- To determine where Passwordstate is installed, and what database server hosts the data, login with a **Security Administrator** account and go to the **Administration** tab -> **Passwordstate Administration** page. The build number, webserver name and database server name are all located on this page.
- Do not replace your **web.config** file after a successful upgrade. This could potentially cause errors when accessing your website.
- If you are using the **High Availability** module of Passwordstate, please see **Section 3** "**High Availability Considerations**" prior to upgrading
- Your license agreement allows you to use your production license keys on a test instance of Passwordstate. If you want to practice upgrades on a test system using a copy of your production data, see this Blog Post

1 System Requirements - General

Web Server

Your web server which will host the Passwordstate web site can be any of the following Operating System versions, with required components:

- Microsoft Windows Server 2016, 2019, 2022, 2025 or Windows 11
- .NET Framework 4.7.2. or Higher
- PowerShell 5.0 or 5.1

Database Server
The following SQL Server versions are supported. Any versions of SQL Server can be used i.e., Express, Standard, Enterprise.

- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft SQL Server 2022

2. Backups, Checksum Validation and Support for Upgrades

Prior to performing any upgrades of Passwordstate, it is strongly recommended you perform backups of your Passwordstate data, and also validate the checksum of upgrade source files you download from Click Studios' CDN network.

Backups

A complete backup of Passwordstate requires a copy of your install folder, and a backup of your SQL database. It's possible to back these up using the built-in Backups feature in Passwordstate, or you can use your own 3rd party solution to back up this data.

If you need to do a complete restore, you will need to revert your install files and database back to the exact condition they were in just prior to your upgrade.

This forum post explains in more details about the different types of backups you can take before your upgrade, and how to recover from a disaster: https://forums.clickstudios.com.au/topic/15406-backups-options-before-upgrades/

Performing Checksum Validation

Downloading the source files to perform upgrades can be done via the following page on the Click Studios web site - https://www.clickstudios.com.au/passwordstate-checksums.aspx.

On this page, the published checksums are also available, along with Powershell examples of how to validate those checksums.

Validating the checksum is a guaranteed method of ensuring the source files you download were signed and provided by Click Studios.

How to get help with a Failed Upgrade?

Understandably, in the event of a failed upgrade you may need to restore your environment quickly, so your users can resume using Passwordstate immediately.

If you need to restore your environment before Click Studios technical support can assist, first collect your **upgradelog.txt** file from your Passwordstate webserver and take any screenshots of any errors you think could help troubleshoot the issue.

By default, the upgrade log file can be found in c:\inetpub\passwordstate\upgrades\upgradelog.txt

Please log a support call through the Click Studios Support Portal and supply your upgrade log and any screenshots to help troubleshoot the issue

3. High Availability Considerations

If you are licensed for the High Availability module, this will most likely mean the you have two production Passwordstate websites replicating data in real time using some form of SQL Replication.

The more advanced and modern replication technologies such as **Always On** or **Basic Availability Groups** can handle database schema changes whilst still having replication enabled. But if you are using **Microsoft SQL Transactional Replication** this does not process schema changes automatically.

In this scenario you will need to delete your transactional **Publisher** and **Subscriber** before you upgrade your primary Passwordstate server, and re-establish replication before you attempt to upgrade your second Passwordstate web server.

You will find documentation on setting up different types of SQL Replication on the Click Studios Documentation Page.

- Occasionally an upgrade will perform a re-encryption of data in your database. This process is completely automated, but best practice is to pause or disable SQL replication whilst upgrading your primary server. You can resume replication once the primary server is completed. Check Change Log notes before each build to determine if re-encryption will occur. You will see a note in the Change Log saying "**the database upgrade screen may take some time to complete**"
- Not all Passwordstate releases have database schema changes, which means you may not have to delete your Transactional Replication as part of your upgrade process. See section **Upgrade Dependency Matrix** at the end of this document for information on which builds will make changes to the schema.
- If you are using **Transactional Replication**, and you see a notification on your database upgrade screen that replication still appears to exist when performing your upgrade, run the following SQL commands to clean up left over replication tables and data:

```
USE Master
EXEC sp_removedbreplication passwordstate
```

4. Maintenance Mode

Maintenance Mode is a feature you can optionally turn on before you start an upgrade.

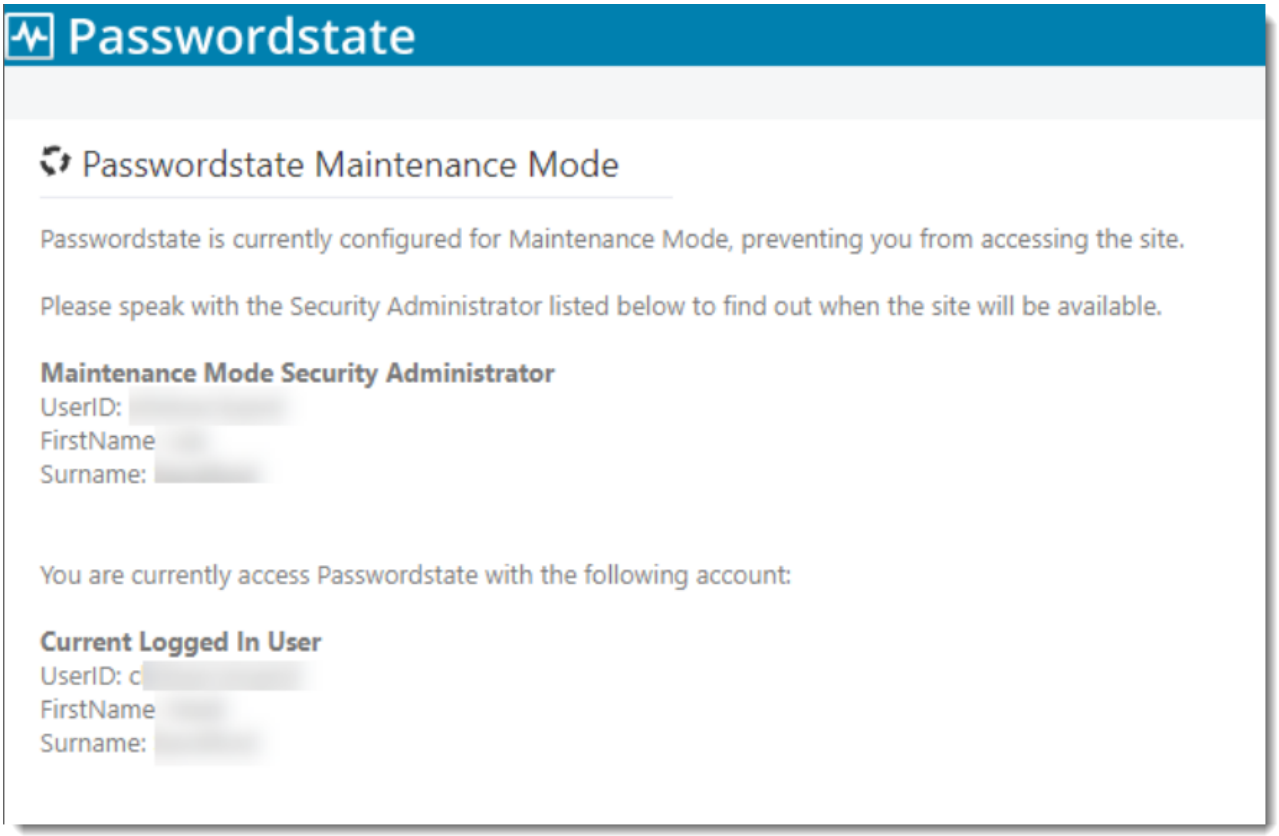
This feature will trigger a pop-up notification for any active user in their browser, and advise them to save their work and log out of Passwordstate. The default time for users to log out is 5 minutes, but this is configurable when turning on this feature.

Once the system is in Maintenance Mode, the website will not be accessible by anyone apart from the user who turned on Maintenance Mode. The Passwordstate Windows Service and APIs will also be unavailable whilst the system is in this state.

When the Upgrade is complete, Passwordstate will automatically be taken out of Maintenance Mode and all services will resume as normal.

You can also manually turn off Maintenance Mode if required. This blog post explains more about this feature: https://blog.clickstudios.com.au/what-is-maintenance-mode/

Below is a screenshot of what your users will see, when the system is in Maintenance Mode, with usernames redacted:



5. Upgrading Passwordstate Core Installation

This section shows how to upgrade your core Passwordstate website.

- Do not replace your **web.config** file after a successful upgrade. This could potentially cause errors when accessing your website.
- If your core Passwordstate software is version 8995 or above, this process will upgrade directly to the latest version. If you are running any build less than 8995, you will be required to perform a double upgrade
- If you are upgrading from a build prior to 9493, please also read the section "**Build 9493 Database Considerations**" section below.

1. Determine the version of Passwordstate you are running. If you are running a build **less than 8995**, then go **to Step 2**. If you are running a build **8995 or higher**, go straight to **Step 5**
2. Download the **"Passwordstate 8 (Build 8995)"** upgrade file from the checksums page and extract the zip file to a temporary location
3. Run the **passwordstate.exe** as an Administrator (right click and **Run as Administrator**) on your Passwordstate web server – simply follow the on-screen instructions for the upgrade wizard
4. Browse to your Passwordstate URL. When you log in, you'll be presented with a database upgrade screen. Click the **Start Upgrade** button to initiate the database upgrade phase and this process is completely automated
5. Download the **"Passwordstate 9 (Build 9xxx)"** upgrade file from the checksums page and extract the zip file to a temporary location. (The version will change depending on what build we have released)
6. Run the **passwordstate.exe** as an Administrator (right click and **Run as Administrator**) on your Passwordstate web server – simply follow the on-screen instructions for the upgrade wizard
7. Browse to your Passwordstate URL. When you log in, you'll be presented with a database upgrade screen. Click the **Start Upgrade** button to initiate the database upgrade phase and this process is completely automated

Your upgrade is complete. You should now be able to log in and you will be running the latest version of Passwordstate 9.

6. Upgrading High Availability Instance of Passwordstate

Once your primary site has been upgraded to the latest build of version 9, follow these instructions to upgrade your High Availability instance of Passwordstate if you have purchased this additional module.

1. Ensure you have established SQL replication if you have multiple databases in your High Availability environment. Your databases should be an exact mirror or each other before you attempt to upgrade your High Availability website. To confirm both databases are running the latest build, run this SQL query below:

   USE Passwordstate
   SELECT BuildNo
   FROM SystemSettings

2. Determine the version of Passwordstate you are running. If you are running a build **less than 8995**, then go **to Step 3**. If you are running a build **8995 or higher**, go straight to **Step 6**
3. Download the **"Passwordstate 8 (Build 8995)"** upgrade file from the checksums page and extract the zip file to a temporary location
4. Run the **passwordstate.exe** as an Administrator (right click and **Run as Administrator**) on your Passwordstate web server – simply follow the on-screen instructions for the upgrade wizard
5. Manually delete the file c:\inetpub\passwordstate\App_JScript**cs_library-8537.min.js**
6. Download the **"Passwordstate 9 (Build 9xxx)"** upgrade file from the checksums page and extract the zip file to a temporary location. (The version will change depending on what build we have released)
7. Run the **passwordstate.exe** as an Administrator (right click and **Run as Administrator**) on your Passwordstate web server – simply follow the on-screen instructions for the upgrade wizard
8. If upgrading from a build of Passwordstate **earlier than 9947**, and only if using a load balancer in front of your Passwordstate web servers, static machinekey settings are required in IIS for seamless failover between web servers when required. To generate static machinekey value, you will need to generate new **Validation** and **Decryption** machine keys in **IIS**. Below are the steps for this:
   a. On your primary web server, open **Internet Information Services (IIS) Manager**
   b. Browse to the Passwordstate website, and click on **Machine Key** icon
   c. Click the **Generate Keys** button on the right-hand side of the page, and then click the **Apply** button
   d. Copy the "C:\inetpub\Passwordstate**web-machineKey.config**" file across to your second Passwordstate webserver, replacing the existing file
9. The upgrade of the High Availability instance is complete

- When upgrading your High Availability webserver, you should never be prompted to upgrade the database. If you are prompted to upgrade your database, there is something wrong with your SQL replication and you should investigate this before proceeding any further.
- Both Passwordstate installs and databases must be running the same version in order for your websites to function correctly. This guide explains how you can determine this: https://forums.clickstudios.com.au/topic/1664-how-to-tell-what-version-of-passwordstate-i-am-using/

7. Build 9493 Database Considerations

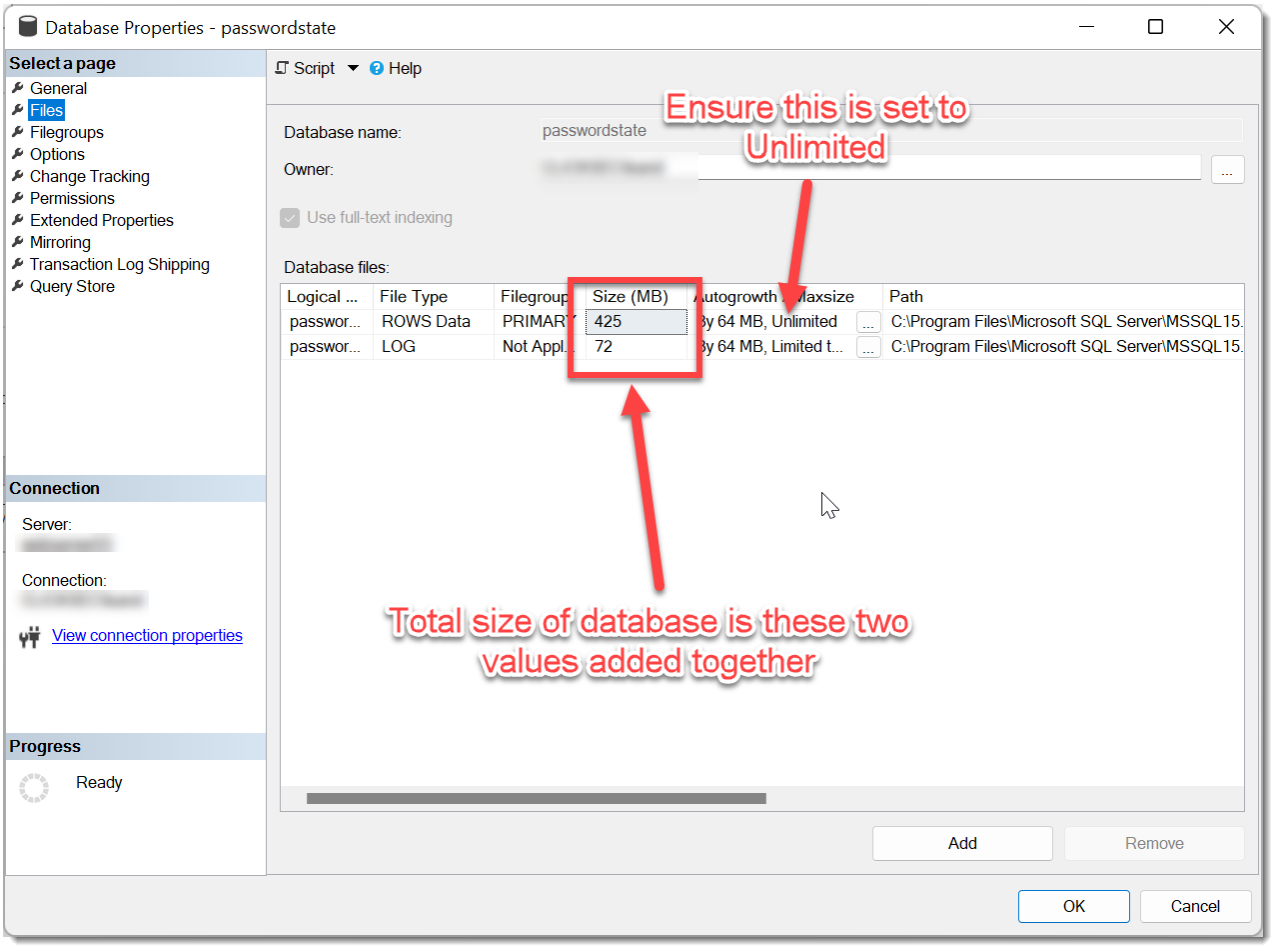
In Build 9493 of Passwordstate, Click Studios introduced support for Unicode characters for our international customers. This change requires many fields in the database to be changed to a datatype of **NVARCHAR**.

This change will result in approximately 300% to 400% database growth, possibly even more in some cases, and the upgrade will take longer than normal. Some customers have seen the upgrade take up to 20 minutes. The more data you have stored in your database will result in a longer upgrade through build 9493.

If you are upgrading from an earlier build than 9493, then please consider the following recommendations, to ensure a seamless upgrade experience.

Pre-Upgrade Considerations – Check Available Space

It is important that you have not only adequate free disk space for the upgrade, but also that you have not limited database growth within SQL Server for your Passwordstate database. To find the size of your database, right click it in SQL Management Studio Tools and select Properties:



In the example above, the database is just under 500mb in size, so the SQL server will need at very minimum 2GB of free disk space. The more space you have free, the better.

Pre-Upgrade Considerations – Reduce Space within Database

There are a couple of methods to reduce the size of your database, prior to upgrading:

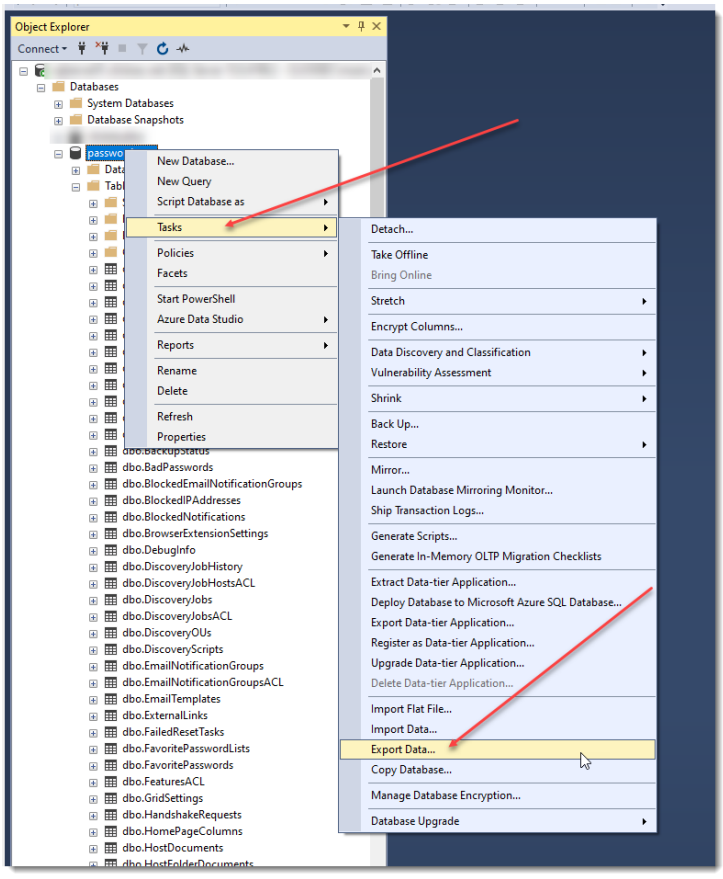
Option #1: Reduce Auditing Records

Passwordstate has two tables for auditing, and these are called **Auditing**, and **AuditingArchive**. Older data will automatically be moved from the **Auditing** table into the **AuditingArchive** table, and this archived data is generally not referenced by Passwordstate. The purpose of this **AuditingArchive** table is to increase website performance but also retain data for compliance reasons.

To check the number of rows you can run the following queries in SQL Server Management Studio. If you have millions of rows, you should consider cleaning up this table"

```
USE Passwordstate
SELECT COUNT(*) FROM Auditing
SELECT COUNT(*) FROM AuditingArchive
```

If needed, below is a screenshot of how you can export your **AuditingArchive** table (if required for compliance reasons), or This Forum Post explains this in more detail.

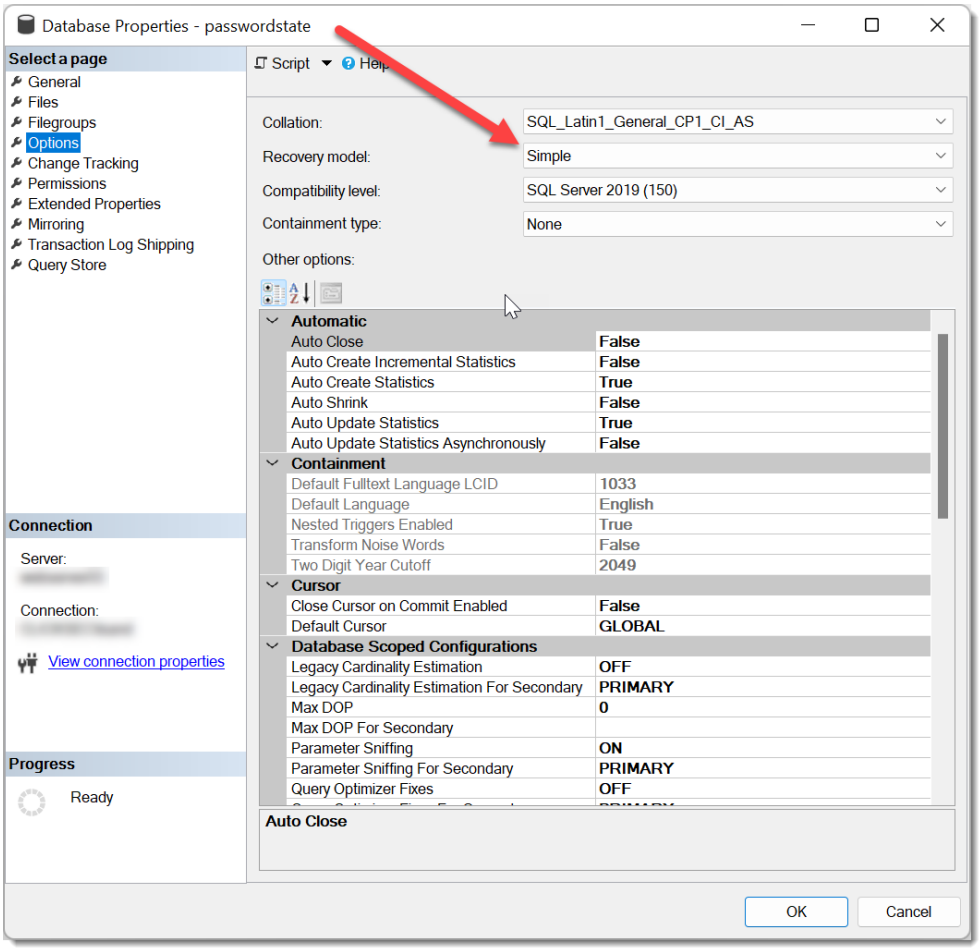


Once you have exported your data, you can remove all data in the **AuditingArchive** table by running this SQL script:

```
USE Passwordstate
TRUNCATE TABLE AuditingArchive
```

Option #2: Shrinking the Database

If you are not using any form of SQL Server replication, you can change the recovery mode of the database to **Simple** as per the screenshot below. Check with your database administrator prior to changing this, as this can prevent transaction log restores throughout the day, but does not prevent normal full backups and restores:



Alternatively, you can run the following command in SQL Server Management Studio – this will try and shrink both the database file, and transaction log file, if possible:

DBCC SHRINKDATABASE (Passwordstate)

Post-Upgrade Considerations – Shrink Database Again

As the conversion to NVARCHAR will increase the size of your database transaction log, it is recommended you shrink the Passwordstate database again after you upgrade, by following one of the options mentioned above.

8. Find Where any Dependant Modules are Installed

This section will explain how you can locate if and where any additional modules are installed, so you can determine if they need to be upgraded after you upgrade your main Passwordstate website.

Module Name	**Additional License Required**?	**Description**	**Location**
High Availability Node	Yes	Second Passwordstate website that is effectively a mirror of your Primary Passwordstate website. Can be running in Read/Write or Read Only mode. Used to ensure instant access to data in the event of an outage of your Primary server, or for Load balancing purposes. Can be connected to same SQL database as primary server but typically connected to a second SQL database, that is replicating data in real time from and/or to the Primary SQL database.	In Passwordstate go to **Administration** -> **Authorized Web Servers** and look for a server on that page with the "**High Availability**" server role.
App Server	No	Separate website that is primarily used for the Mobile iOS or Android Apps to connect to, but can also act as a proxy for other features to connect through such as Self Destruct Messages, Browser Extensions, or API requests.	In Passwordstate go to **Administration** -> **Authorized Web Servers** and look for a server on that page with the "**App Server**" server role.
Self Destruct Push/Pull website	No	Separate website that can be used to access self-destruct messages.	In Passwordstate go to **Administration** -> **System Settings** -> **Self Destruct Messages** tab. Look for a "**Separate Site URL**" field and if populated, a DNS lookup on that URL will advise where the server is located

Browser Based Launcher	No	Used to remote into servers and hosts on the network within a new tab in your browser (RDP and SSH).	In Passwordstate, go to **Administration** -> **Remote Session Management** -> **Browser Based Gateway Settings** and look for a URL on that page, and if populated, a DNS lookup on that URL will advise where the server is located
Password Reset portal	Yes	Additional website you can install on any server of your choice, where standard users can log in and reset or unlock their own Active Directory account password.	In Passwordstate, go to **Administration** -> **Password Reset Portal Administration** -> **System Settings** -> **Miscellaneous** tab. Look for a URL field and if populated, a DNS lookup on that URL will advise where the server is located
Remote Site Locations	Yes	Windows Service/Agent that can be installed on remote air gapped networks, for the purpose of privileged account management on those networks. These agents are self-updating, so typically should not require any sort of manual upgrade to be performed.	In Passwordstate, go to **Administration** -> **Remote Site Administration** -> **Remote Site Locations**. If you have any remote sites added on this screen, it will list which server they are installed on. It will also show the version number, and they should all be running the same version, if the self-updating feature is working.

9. App Server Upgrade Instructions

Please refer to the section '**Upgrades Dependency Matrix**' below to determine if you need to follow the instructions below to upgrade the Passwordstate App Server install.

In this upgrade Matrix, if there are any builds which indicate the App Server, Self-Destruct or Browser Extensions require an upgrade from the build you are currently using, then follow these instructions:

1. In your Passwordstate folder (typically **c:\inetpub\passwordstate**), you will see a sub-folder called **Downloads**.
2. Take a copy of the file **PasswordstateAppServer.exe**, and copy it across to the server where you have your App Server installed
3. Run **PasswordstateAppServer.exe** as an Administrator (right click and Run as Administrator), and follow the on-screen instructions for the upgrade wizard

10. Password Reset Portal Upgrade Instructions

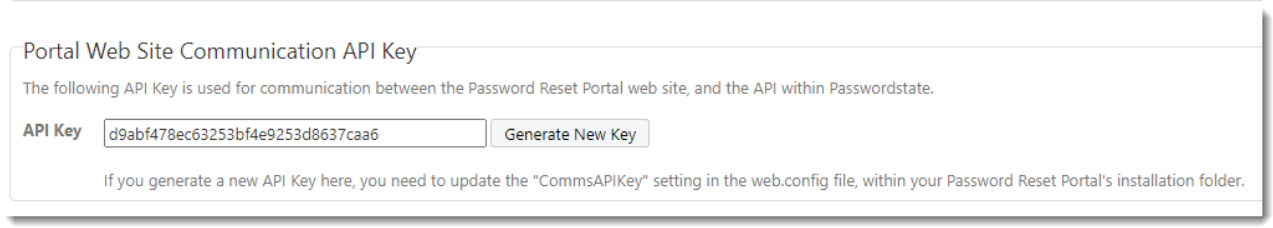
Please refer to the section '**Upgrades Dependency Matrix**' below to determine if you need to follow the instructions below to upgrade the Password Reset Portal install. If needed, follow these instructions:

1. In your Passwordstate folder (typically **c:\inetpub\passwordstate**), you will see a sub-folder called **Downloads**.
2. Take a copy of the file **PasswordstateResetPortal.exe**, and copy it across to the server where you have your Password Reset Portal installed
3. Run **PasswordstateResetPortal.exe** as an Administrator (right click and Run as Administrator), and follow the on-screen instructions for the upgrade wizard

Important Upgrade Instructions

If upgrading your core Passwordstate installation from a version earlier than build **9611**, then there is a once off manual step required when upgrading your Password Reset Portal Installation. Please follow the instructions below for this:

1. In Passwordstate, go to the screen **Administration** -> **Password Reset Portal Administration** -> **System Settings** -> **API** tab
2. Copy the "**Portal Web Site Communication API Key**" value you see below in the screenshot



3. In your Password Reset Portal folder, typically in the path of c:\inetpub\PasswordstateResetPortal, edit the **web.config** file and add the line you see in the screenshot below – with your API Key value. Save the file after making this change.

   <add key="CommsAPIKey" value="d9abf478ec63253bf4e9253d8637caa6" />

Note: If you tried to access your Password Reset Portal site before following the instructions above, you will need to restart Internet Information Services (IIS), or reboot your server, to avoid an error message about the APIKey not being found.

11. Remote Site Locations Agent Upgrade Instructions

With any deployed Remote Site Location Agents, these will automatically upgrade themselves within 10 to 15 minutes after you have upgraded your main Passwordstate server.

As of build 9300, the upgrade process has been changed to download upgrades from your Passwordstate web server itself, instead of from Click Studios' CDN network.

Because of this change in architecture, if you are upgrading Passwordstate from a build earlier than build 9300, you need to follow the instructions below to perform a manual upgrade – all subsequent upgrades will be automatic:

1. In your Passwordstate folder (typically **c:\inetpub\passwordstate**), you will see a sub-folder called Downloads.
2. Take a copy of the file **PasswordstateAgent.exe**, and copy it across to the server where you have your Agent installed
3. Open a DOS prompt as Administrator, and browse to the directory where you copied the file, and run the following command:

   PasswordstateAgent.exe /s

- To check the versions of each agent, visit the **Administration** -> **Remote Site Administration** -> **Remote Site Locations** and each site along with the version will be displayed on this screen

12. Self Destruct Message Web Site Upgrade Instructions

There are three versions of the Self Destruct Message Web sites available, and each have different upgrade processes.

Standard Self Destruct

This site is embedded by default with your main Passwordstate install, and will get upgraded automatically when you upgrade the core Passwordstate website.

App Server

It can also be used as part of the Passwordstate App Server, and section "**App Server Upgrade Instructions**" above describes upgrading this feature, if you have deployed this separately from your Passwordstate install.

Push/Pull Self Destruct

Another version of Self Destruct is available called "**Push/Pull**", in which the site uses a local SQLite database, and your core Passwordstate installation pushes and pulls all data to this SQLite database. This Self Destruct web site implementation does not require any access back to your Passwordstate SQL database.

To upgrade the Push/Pull version of the Self Destruct Message web site, follow these instructions:

1. In your Passwordstate folder (typically **c:\inetpub\passwordstate**), you will see a sub-folder called Downloads.
2. Take a copy of the file **PasswordstateSelfDestruct.exe**, and copy it across to the server where you have your Self Destruct Web Site installed
3. Run **PasswordstateSelfDestruct.exe** as an Administrator (right click and Run as Administrator), and follow the on-screen instructions for the upgrade wizard

13. Browser Based Remote Session Launcher Gateway

By default, the Browser Based Remote Session Launcher Gateway is embedded with your Passwordstate web site. This will get upgraded automatically when you upgrade the core Passwordstate website.

This Gateway can also be installed on a separate server to where you have Passwordstate installed if desired. If you have deployed the Gateway separately to your main Passwordstate web site, you will need to follow the instructions below to manually upgrade your Gateway.

1. Log into the server where the Gateway has been installed, stop the '**Passwordstate Gateway Maintenance**' and '**Passwordstate-Gateway**' Windows Services
2. From your core Passwordstate installation, copy the "html" folder across from the folder **C:\inetpub\Passwordstate\hosts\gateway** to where you have the Gateway installed (default path is C:\Program Files (x86)\Passwordstate Remote Session Gateway\gateway), and overwrite existing files
3. From your core Passwordstate installation, copy the following 4 files across from the folder **C:\inetpub\Passwordstate\hosts\gateway** to where you have the Gateway installed, and overwrite existing files:
    a. License
    b. Passwordstate-Gatewayw.exe
    c. SparkGateway.exe
    d. SparkGateway.jar
4. Restart the '**Passwordstate Gateway Maintenance**' and '**Passwordstate-Gateway**' Windows Services

Build 9627 Changes

If you are upgrading from a build of Passwordstate prior to **9627**, then the following is required – there has been some architectural changes to the Remote Session Gateway:

1. As per point 2 above, you need to copy across the html folder to where you have the gateway installed separately
2. In the gateway.conf file, you need to:
    a. Add the line "recdir.play.enable = true" as you see in the screenshot below
    b. And update the "html" setting to be like the screenshot below
    c. Then restart the "Passwordstate-Gateway" Windows Service

```
#listening port
port = 7273

#directory for session recording.
recdir = rec
recdir.play.enable = true

#default folder of where the html files are stored
html = html
```

14. Upgrade Dependency Matrix

The following table below shows which Passwordstate Build Numbers require schema changes in the database, or any other dependant modules which also require upgrading at the same time - after you have upgraded your installation of Passwordstate.

Some of these modules do get updates to them over time, but you are not necessarily forced to upgrade them when you upgrade your main Passwordstate instance.

Build No	Database Schema Updates	App Server	Mobile Apps	Password Reset Portal	Remote Site Locations Agent	Browser Extensions	Self Destruct	Browser Based Gateway	Client Based Launcher
9955	No	No	No	No	No	No	No	No	No
9952	No	No	No	No	No	No	No	No	No
9950	No	No	No	No	No	No	No	No	No
9947	No	No	No	No	No	No	No	No	No
9943	Yes	No	No	No	No	No	No	No	No
9938	Yes	No	No	No	Yes	No	No	No	No
9930	No	No	No	No	No	No	No	No	Yes
9925	No	No	No	No	No	No	No	No	No
9922	No	No	No	No	No	No	No	No	No
9920	Yes	No	No	No	No	No	No	No	No
9915	No	No	No	No	No	No	No	No	No
9911	Yes	No	No	No	No	No	No	No	No
9905	Yes	No	No	No	No	No	No	No	No
9894	No	No	No	No	No	Yes	No	No	No

9890	No	No	No	No	No	No	No	No	No
9881	Yes	No	No	No	No	No	No	Yes	Yes
9873	No	No	No	No	No	No	No	Yes	No
9866	No	No	No	No	No	No	No	No	No
9858	No	No	No	No	No	No	No	No	No
9853	No	No	No	No	No	No	No	No	No
9849	No	No	No	No	Yes	No	No	No	No
9839	No	No	No	No	No	No	No	No	Yes
9835	Yes	No	No	No	Yes	No	No	Yes	No
9823	Yes	No	No	No	No	No	No	No	No
9811	Yes	Yes	No	No	Yes	No	No	No	No
9795	Yes	No	No	No	No	No	No	No	No
9786	No	No	No	No	No	Yes	No	No	No
9785	Yes	Yes	No	Yes	No	Yes	No	Yes	No
9753	No	No	No	No	No	No	No	No	Yes
9737	No	No	No	No	No	No	No	No	No
9735	No	No	No	No	No	No	No	No	No
9727	Yes	No	No	No	No	No	No	No	No
9715	No	No	No	No	No	No	No	No	No
9708	No	No	No	No	No	No	No	No	No
9700	Yes	Yes	No	No	No	No	No	No	No
9665	No	No	No	No	No	No	No	No	No
9661	Yes	No	No	No	No	No	No	No	No
9653	No	No	No	No	Yes	No	No	No	No

9630	No	No	No	No	No	No	No	No	No
9627	Yes	Yes	No	Yes	Yes	No	No	Yes	No
9611	Yes	No	No	Yes	Yes	No	No	No	No
9595	No	No	No	No	No	No	No	No	No
9593	Yes	Yes	No	No	No	No	No	No	No
9583	Yes	Yes	No	Yes	Yes	No	No	Yes	No
9535	No	Yes	No	Yes	Yes	No	Yes	No	No
9533	No	No	No	No	No	No	No	No	No
9531	No	No	No	No	Yes	No	No	No	No
9519	Yes	No	No	No	No	No	No	No	No
9512	Yes	No	No	No	No	No	No	No	No
9500	No	No	No	No	No	No	No	No	No
9493	Yes	Yes	Yes	Yes	No	No	No	No	No
9471	Yes	No	No	No	Yes	No	No	No	No
9455	Yes	No	No	No	No	No	No	No	No
9435	Yes	Yes	Yes	No	No	No	Yes	No	No
9414	No	No	No	Yes	No	No	No	No	No
9400	Yes	No	No	Yes	No	No	No	No	No
9381	Yes	No	No	No	Yes	No	No	No	No
9360	No	No	No	No	No	No	No	No	No
9350	Yes	No	No	No	Yes	No	No	No	No
9300	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
9117	Yes	No	No	No	Yes	No	No	No	No
9112	Yes	No	No	No	No	No	No	No	No

9100	No	No	No	No	No	No	No	No	No
9073	No	No	No	No	No	No	No	No	No
9065	Yes	No	No	No	No	No	No	No	No
9050	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
9000	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No