Clickstudios PASSWORDSTATE

Secure by Design!

Security designed to protect your data

Table of Contents

Click Studios prides itself on providing the best support possible. If you are having issues with Passwordstate contact us at support@clickstudios.com.au, or alternatively you can reference:

Community Forum : https://forums.clickstudios.com.au/
Documentation : https://www.clickstudios.com.au/documentation/default.aspx

Our Credentials

370,000+	29,000+	98.8 %	97.9%
SECURITY & IT PROFESSIONALS GLOBALLY	CUSTOMERS GLOBALLY	CUSTOMER RETENTION RATE	CUSTOMER SATISFACTION RATE

Why do we start this security document with what looks like marketing hype?

Quite simply because these figures are a testament to what Click Studios has achieved since it started in 2004. We're proud of our achievements and value our customer base, from the largest Enterprise to the smallest Not-for-Profit, every single day. It's what drives us to continually focus on improving our responsiveness, the calibre of our technical support and the innovation in our products, for you our customers. We genuinely believe that Password Management should be affordable for everyone. Because it is important!

That's why we state that only Click Studios Passwordstate, based on a consistent security architecture and utilising 256bit AES data encryption, code obfuscation, Hashing and Data Salting with true enterprise scalability can provide you with the answers and assurance you need.

Secure by Design!

Passwordstate allows Teams of people to access and share sensitive password credentials without the need for additional complex security and auditing tools. Through role based administration and end-to-end event auditing it provides customers with a trusted and secure platform for password storage and collaboration.

Any unauthorised access to password credentials could expose your organization to serious risk including the potential for data theft, irreparable reputational loss and financial damage.

To minimise this risk, we've ensured that Passwordstate uses a consistent Security design, including code obfuscation, to protect access to your credentials from user authentication and access, through transmission, to your encrypted storage. It's what we call **Secure by Design!**

The following is a brief outline of the security features and approaches used in our product.

Passwordstate Vault

Key Points

- Industry standard .NET Framework & AES-256 Encryption is utilised to ensure the privacy and protection of your credentials. AES-256 is to all intent unbreakable by brute force with current computing power making it the strongest encryption.
- Unique Initialization Vectors for every encrypted field and record ensures that each field and record is unique in its encryption and decryption. This prevents any inference of the relationships between segments of the encrypted fields and records.
- Use of HMAC-SHA512 Hashing Algorithm ensures data is unable to be intentionally manipulated directly within the database. Data that is attempted to be directly manipulated will result in a data integrity error and prevent Passwordstate from being accessed.

Click Studios is proud of its support for small business, non-profit and education organisations.

Passwordstate is free for up to 5 users. Registered Charities and Education Providers receive a 30% license discount in support of the positive impact they have in our communities.

Additional

- Encryption is performed at application and database level.
- Encrypted fields are Salted & Hashed using random and known bits.
- Encryption key and encrypted data cannot reside together.

Base Authentication

Key Points

- Microsoft Active Directory integration allows the reuse of existing AD accounts, attributes, security groups and policies within Passwordstate. Accounts and security groups can be imported for consistent security administration and the status of accounts can be synchronised.
- Single Sign-On using Active Directory credentials is possible when the AD Integrated Base Authentication is selected at installation time. This allows passthrough of AD credentials for login to Passwordstate.
- LDAP and LDAP over SSL for Active Directory communications. Whilst LDAP is supported the credentials are passed over the network unencrypted. LDAPS encrypts the connection between the respective parties using the SSL certificate before exchanging the required credentials.

Additional

- Forms-based Authentication is provided as an alternative.
- RBAC (Role Based Access Control) to password credentials.
- SAML 2.0 integration with all SAML 2.0 Compliant providers.

Application Integrity

Key Points

- ASP.NET pages and obfuscated .NET Assemblies ensure application integrity by preventing decompliation to view critical areas of code such as methods, functions and classes.
- DBA's cannot change records in the database and grant themselves, or others, access to passwords they are not authorized to have access to. Any attempt to directly manipulate records in the database will result in data integrity errors.
- Encrypting the Web.config for the Passwordstate web site ensures an additional level of protection. Through encryption of the database connection string, and split secrets sections in the web.config file you further secure access to the database and encryption keys used in Passwordstate.

Additional

- Admins cannot write ASP.NET pages to extract data from DB.
- Authorize webservers that can host Passwordstate.
- Two unique encryption keys, 4 secrets, independently stored.
- Encryption key rotation with full auditing.
- Export encryption keys (in split secret format) for DR.
- Developed using OWASP Methodology.

Click Studios prides itself on providing the best support possible. If you are having issues with Passwordstate contact us at support@clickstudios.com.au, or alternatively you can reference:

Community Forum : https://forums.clickstudios.com.au/
Documentation : https://www.clickstudios.com.au/documentation/default.aspx

- Mitigation against SQL injections, cross-site scripting, broken access control and other attacks.
- Regular Penetration Testing of Click Studios Passwordstate.
- Encryption at application and database level.
- FIPS 140-2 compliant mode (application).

Network Transmission

Key Points

- Passwordstate is fully compliant with Transport Layer Security protocol 1.2 being enabled on your web server. It allows communication over the internet securely without the transmission being vulnerable to a 3rd party listening.
- All Passwordstate traffic between the Client web browser and the Passwordstate web site is encrypted and transmitted over HTTPS. This ensures any data packets that are intercepted will effectively contain nonsensical characters.
- Login credentials are retrieved from Passwordstate, encrypted and sent to the Remote Session Launcher gateway, where they are decrypted and passed on to the remote client for execution. This ensures the authentication credentials remain secure.

Additional

- Password Resets through PowerShell Remoting and SSH.
- RDP and SSH sessions from any compatible browser.
- RDP, SSH, Telnet, VNC, SQL and Teamviewer Sessions from Clients.
- Remote connections tunnelled through Passwordstate.
- Passwords for remote sessions can be hidden from user.
- No direct connectivity between user device and host for Browser based sessions.
- No plugins or agents required on remote hosts.

Two-Factor Authentication

Key Points

Passwordstate offer two base forms of authentication - Active Directory Integrated, and Forms-Based Authentication. Many two-factor authentication options are available, and when used in different combinations, 24 different authentication options are available:

- Google Authenticator is a free two-factor authentication solution that implements two-step verification using the Time-based One-time Password Algorithm and HMAC-based One-time Password algorithm. Software is available for most mobile clients.
- RSA SecurID is a leading two-factor authentication solution. It requires users to authenticate using tokensSecurID Authentication which uses a 64-bit current time and 128-bit seed record hashed down to produce 6 or 8-digit PIN.
- Duo two-factor authentication is a leading cloud-based two-factor authentication solution. It uses asymmetric cryptography with a public key stored in their cloud with a private key on your device. You can choose Duo Security's Authentication via Push, SMS or Phone Call.

Additional

- ScramblePad Authentication.
- Email Temporary Pin Code.
- AuthAnvil Authentication.
- SafeNet Authentication.
- One-Time Password.
- SAML 2.0 Authentication.
- RADIUS Authentication.
- YubiKey Authentication.

Role Based Access Control

Key Points

- Role Based Access Control (RBAC) ensures only authorized users have access to sensitive data. It enables granular governance of Passwordstate through the assignment of multiple roles and permissions. You can grant separate roles for users and Security Administrators using Local Security Groups, or synchronize Active Directory Security group memberships.
- There are multiple Security Administrator roles within Passwordstate. This allows segregation of internal Passwordstate management duties amongst System and Security Administrators across the core product, Remote Site Locations and Password Reset Portal.
- Assignment via Security Groups simplifies the process of organizing access for multiple user accounts. Security groups can be local to Passwordstate, or synchronized with Active Directory Security Groups.

Additional

- Permissions granted to Password Lists and individual Passwords.
- 41 Security Administrator roles assignable to users and security groups.

Auditing and Compliance

Key Points

- Real-time event monitoring keeps System and Security Administrators informed as different events take place. This is achieved through a combination of audit records and real-time email notifications. Security Administrators can enable or disable real-time notifications for all users of Passwordstate. Individual users can elect to disable or enable email categories as required. Real-Time Notification Groups are available, so different sets of users can receive different categories of email alerts.
- Security Information & Event Management (SIEM) integration with Passwordstate further enhances the comprehensive auditing capabilities provided. Integration is via supply of data to a nominated SysLog server. Two services check for new events, if events have been successfully sent and queuing of new events to be sent.

- Remote Session auditing and session recording can be specified based on Users and Security Groups. This can be used to review and investigate activities performed during privileged sessions and comply with regional or corporate regulations and policies. All Remote Sessions are audited with information captured including who launched a Remote Session, to which Host, from what IP Address, and using which specific authentication credentials.

Additional

- 110+ auditable events for reporting.
- Real-time Email notifications using predefined templates.
- Password length & complexity indicators.
- Enforced Password Rotation.
- Password Reset Recommendations on removal of user access.
- 35 pre-defined reports covering Users, Passwords, Permissions, Activity & documents.
- One-time & Scheduled reports.

High Availability

Key Points

- The High Availability Module is an optional product to enable either Active/Passive or Active/Active High Availability. This module is required if you intend to use Virtual Server Replication technologies for Disaster Recover or Business Continuity.
- By default, the HA module provides a read-only replica of your production installation in an Active/Passive configuration. Users are able to perform all normal operations within Passwordstate except those which modify data in the database.
- Full auditing of Passwordstate access for Active/Passive configuration is provided. Whilst users cannot update data on the HA server logging of all events is recorded locally on the passive instance with replication back to the Primary Instance once it becomes available again.
- Can be configured in Active/Active mode for true High Availability. This allows users to update data in both website instances of Passwordstate. This requires Basic Availability Groups, or Always On Availability Groups using SQL Server Standard and above.

Backup and Recovery

Key Points

- Live website and database backups to a network share using Passwordstate's own in-built feature for performing backups. This provides a backup of your entire website folder, and SQL Server database with the output stored within a ZIP compressed file. Sensitive data within the SQL Backup file is encrypted.
- Can restore database and/or Passwordstate web server depending on the nature of the event you are recovering from. Full documentation is provided for both web server and database restores.

- In the event your entire Active Directory domain is unavailable it is possible to restore your Passwordstate Instance and access all data with the use of the Emergency Access login. This has no reliance on Active Directory.

Additional

- Optional exclusion of database to cater for in-house backups.
- Backup automatically invoked as part of In-Place Upgrade.

Policy Driven

Key Points

- Strength Policies are a set of rules for enforcing the strength of a password and are applied to one or more Password Lists. Specification of minimum number of Lowercase, Uppercase, Numeric and Symbols characters, as well as mixed Upper and Lowercase characters and minimum/maximum length of passwords can be set.
- Generator Policies are used as a set of rules for generating random passwords. Once a policy is created, it can be assigned to one or more Password Lists, or users can simply select the policy when they need to generate random passwords on mass. These policies can also be called via the API to generate passwords.
- Templates can be used to apply consistency to settings for your Password Lists. Accessing Templates from within the administration area allows you to see all Templates created by all users. Password Lists can be linked to the Template for management and permission setting.

Additional

- 31 user account policies applicable to users and Security Groups.
- Email Notification policies to control which emails users receive.

Browser Extensions

Key Points

- Automatic saving of website credentials to Password Lists. On first login to a new website you are prompted to save your credentials back to Passwordstate. You can elect to save your credentials, close the dialog without saving them this time or ignore saving them and never prompt for that URL again.
- Generate strong random passwords using Password Generators and Policies. These are random passwords generated based on the Password Generator policies that apply to you. This allows you to generate long and secure passwords that you never need to remember.
- Choose to save credentials to Private or Shared Password Lists. This allows you to share work related password credentials for websites whilst keeping access to personal website logins confidential in your own Private Password Lists.

Password Reset Portal

Key Points

- The Password Reset Portal is a subscription based, optional module, that allows your users to unlock or reset the password for their Active Directory Domain. This can be used via mobile devices in addition to standard Windows PCs.
- Provides tracking of where User Account lockouts are occurring through integration with Event Log monitoring. This can be used for monitoring for Account Lockouts and Bad Login Attempts.
- Enforce Password Strength policies, matching your AD password length and complexity requirements, through the use of Passwordstate's core Password Strength Policies. Users are guided through the reset process and provided with on screen instructions informing them of the password requirements.
- Prevent 'Bad Passwords' from being used in your organization. Passwordstate provides 2 options. Either add prohibited words as a 'Bad Password' into the Passwordstate database, or use the online 'Have I been Pwned' database. Both solutions ensure users will no longer be able to save 'Bad Passwords' and will result in them being informed the password value they have entered is not allowed.

Additional

- Can be installed in a DMZ.
- 10 Verification Policies to securely "identify" users.
- Verification policies used for enrolment, unlocking & resets.

Remote Site Locations

Key Points

- Remote Site Locations is a subscription based, optional module, that extends the Passwordstate PAM solution to disconnected networks, either firewalled on your internal network or over the Internet. Using one agent per remote site it enables account discoveries, password resets and remote site management from within the Passwordstate UI. Security is assured via independent In-Transit encryption between the agent and the Passwordstate instance.
- Communication is restricted to a single open port on the remote firewall, locked down to the IP addresses for the Passwordstate Instance and the agent. All activities are performed by the agent and results returned to the Primary Passwordstate Instance.
- In large complex environments you can easily specify which assets in Passwordstate belong to each of the Remote Site Locations by tagging them against the correct Site. This includes AD Domains, Accounts, Security Groups, Hosts, Password Lists & Folders and all discovery jobs and auditing data.

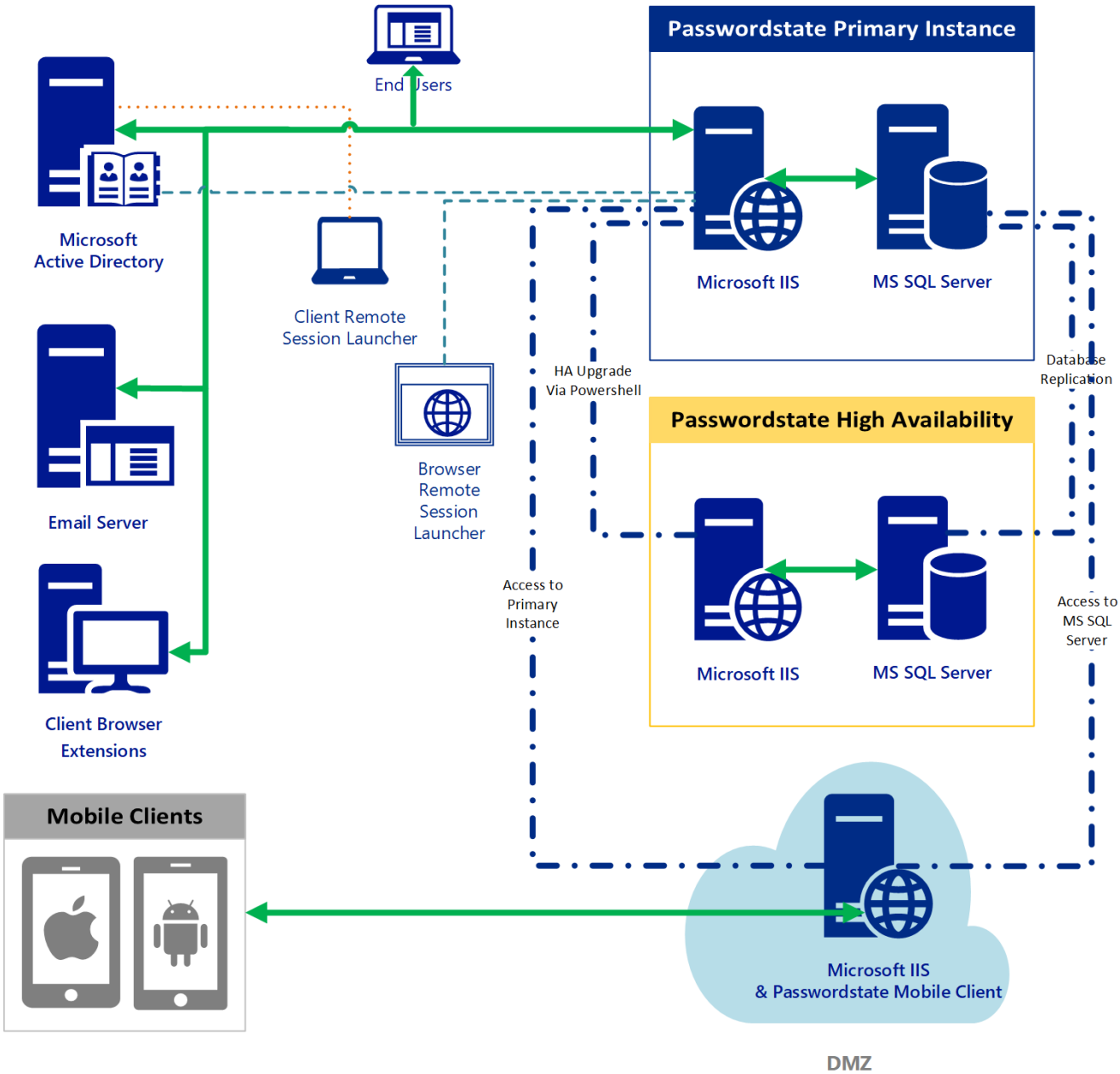
Logical Architecture

The diagram below represents a logical view of a typical Passwordstate Instance. Each instance consists of a Microsoft IIS installation coupled with a SQL Server installation. These can be hosted on the same physical or virtual server infrastructure, depending on the number of user accounts and hosts being managed, and the discovery and password reset workloads. Larger installations are recommended to be hosted on separate infrastructure.

In a High Availability configuration, the Passwordstate Instance is 'mirrored' like for like. The HA instance can be configured as either Active/Passive or, with an appropriate SQL Server version, configuration and the use of Load Balancers, in an Active/Active configuration.

The Mobile client gateway is installed by default on your Primary Instance, but for access from the internet can be installed on a separate hardened server located within your DMZ.

All open port requirements for Passwordstate and its various modules can be obtained from https://www.clickstudios.com.au/documentation/



Click Studios prides itself on providing the best support possible. If you are having issues with Passwordstate contact us at support@clickstudios.com.au, or alternatively you can reference:

Community Forum : https://forums.clickstudios.com.au/
Documentation : https://www.clickstudios.com.au/documentation/default.aspx