IT Glue's Security Principles and Features

Security White Paper
June 2025

ITGlue
A Kaseya COMPANY

Contents

About IT Glue and our security promise

As the industry standard for documentation, trusted by tens of thousands of managed service providers and IT professionals, we take our commitment to security seriously. IT Glue abides by strict measures to protect the security and privacy of your valued data. In addition, we understand that having reliable access to your data, with no downtime, is critical for your business. To ensure both objectives are met, we have adopted industry-leading security measures, including SOC 2 (Type II), multifactor authentication (MFA), single sign-on (SSO) and host-proof hosting.

Summary of key IT Glue security principles

- ***SOC 2 (Type II) compliance:*** IT Glue is the only IT documentation platform in the channel that has acquired Service Organization Control 2 (SOC 2) Type II, an internal controls report that captures how well data is safeguarded and the degree to which those controls are operating at industry best practices. This report ensures we are meeting stringent requirements set by the American Institute of Certified Public Accountants (AICPA). The result is a platform that has been developed under an audited process to guarantee the highest level of trust and security.
- ***Secure platform:*** Using Amazon's hosting platform, AWS, we ensure the most flexible, reliable and secure computing environment with the best global network performance available today. AWS is designed and built for redundancy, and through their denial-of-service protection, a Web Application Firewall (WAF) and PCI-level security measures, we can monitor your data on a 24/7/365 basis.
- ***Password encryption:*** Rely on the highest standard of encryption in the industry today. Passwords are encrypted with AES-256-bit encryption, including 2048-bit RSA public key, with unique keys for each customer and secure random keys unique to each password, which are kept separate from each other. If a breach was to occur in one system, this will not allow decryption of any passwords.
- ***Host-proof hosting:*** IT Glue Vault is designed to allow a user to only decrypt exclusively at the endpoint level on the user's browser with a user-specific passphrase rather than syncing it to the IT Glue system. Only the user has access to the passphrase to the password; once lost, the password cannot be retrieved by IT Glue.
- ***Enforced multifactor authentication (MFA):*** MFA is enforced on all user accounts. With enforced MFA, all users are prompted for their username and password plus a temporary one-time password generated by an authenticator application. This mitigates the risk of the user's login being compromised.
- ***SSO Access Control:*** With SSO Access Control, you have the option to make SSO login the only authentication channel into your IT Glue instance. This is achieved by enforcing SSO authentication, thereby preventing unauthorized access to IT Glue.
- ***Permissions and audit trail:*** IT Glue allows administrators and managers to add layers of control to establish security permissions where needed. Password changes are version-controlled, and access is easily restricted to specific groups and users of your choosing. Passwords that are viewed are then automatically tracked in an audit trail entry within the activity logs. IT Glue administrators can also generate an At-Risk Password Report that details which passwords a user had access to and needs to be changed during offboarding.

For more information, please visit our online resources:

- Privacy Policy — https://www.itglue.com/privacy-policy/
- Terms of Service — https://www.itglue.com/terms-of-use/

Platform security

SOC 2 (Type II) compliance

We have always operated by a comprehensive set of security systems based on industry best practices, including ISO 27001 and PCI-DSS. Since March 2017, we have been officially SOC 2 (Service Organization Control 2) compliant, and we are also audited on an annual basis. This is one of the many ways that we demonstrate our commitment to security and follow industry best practices to secure your valued data. Type II requires the implementation of the controls over a minimum six-month period in addition to the ongoing attestation of the operating effectiveness of the controls. However, acceptable security processes only need to be verified at a specific point in time. Our security infrastructure and procedures are tested and audited by third parties on a regular basis in accordance with the Trust Services Principles and Criteria for security, availability, processing integrity, confidentiality and privacy of a system.

IT Glue staff data accessibility

IT Glue treats your information with the utmost confidentiality.

In compliance with SOC 2 (Type II), when you need assistance and support, we might ask that you share your screen via a live session, leaving you to present and show us only minimum information.

When the only option for support is for us to access your data, a limited number of members from our senior team have the ability to impersonate your account. In this case, we make a very specific request for your permission via a support ticket. Any activity will be logged in your activity log with an added eye icon in the log to show it was our team impersonating the account. Please note, during impersonation, IT Glue staff can't decrypt the passwords stored in the IT Glue Vault.

You have the option to disable the IT Glue team impersonation during support. All you have to do is add the IT Glue IP address with the IP access control feature. Otherwise, IT Glue staff can access your data only if you invite them to your account, in which case, any views or actions are fully logged in the activity log.

Information that we have access to includes the email address and the first and last names of the POC for each account. We also have access to an account level summary of Configurations, Organizations and Contacts. We cannot access password data (because it is encrypted), customer data, Core and Flexible Assets, and MyGlue data.

Trust service principles and criteria

In compliance with SOC 2 (Type II), IT Glue has worked to meet every Trust Service Criteria by effectively operating within the controls required to meet them. Not only is this a testament to the security of our platform, but this is also our way of securing your business.

Logical access protection

IT Glue has implemented a layered security system to restrict logical access and detect potential harmful actions. This includes firewalls, network segmentation, hardened servers, IP whitelisting and encryption to ensure data is protected. Logical access rights are tested as part of our quality assurance (QA) process. Logical access controls and change management tools restrict the ability to migrate between development, test and production to change deployment personnel. Firewalls are in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks. We have also established firewall rules and the online system limits the types of activities and service requests that can be permitted from external connections.

Production security architecture

IT Glue's production systems leverage AWS security systems in a layered security model. Each layer provides role-based controls to limit access to systems and users. Systems are hardened, changed-controlled and monitored 24/7 by IT Glue. System logs are sent to the AWS CloudTrail for monitoring and review.

Security controls are monitored using several methods:

- Vulnerability scanning — Vulnerability scans are performed internally and at least quarterly. Independent vulnerability scans are performed by a third-party vendor at least quarterly.
- Penetration testing — External penetration testing is performed by an independent third party at least annually.
- Internal reviews — IT Glue performs a review of the hardening standards and their implementation at least annually. Firewall rules are reviewed at least semiannually.
- Internal audit — Independent internal auditing is performed on the controls at least annually.
- System monitoring — IT Glue's Development Operations team monitors the availability of production systems through automated systems. Logs and events are then centrally managed and analyzed by the team.

Change management

We have implemented a change management process within our production teams, including segregated development, integration, test and production environments. Our software change control process requires all changes to code to be documented and several processes to be completed like risk assessment, a code review by multiple engineers (at least two) and quality assurance (QA). These measures ensure that all changes were approved before production per SOC 2 requirements. Change management is also implemented on our production servers, including documentation of changes, risk assessments and approval processes. All incidents are documented, including steps to contain the issue, root cause analysis, long-term solutions, and related evidence and communications. High-severity incidents require an analyst to determine the root cause and changes are recommended to eliminate the incident from reoccurring.

Availability

To manage the demand for processing capacity and to enable the implementation of additional capacity commitments, we ensure that systematic network and monitoring is in place. Daily and monthly tasks and event logging are maintained. Automatic backup systems are utilized to perform scheduled system backups of target data while backup jobs are monitored with notification alerts sent out in the event of backup failure. IT Glue has a backup schedule in place to automatically initiate production backup jobs. Finally, restore operations from backup media are performed as a component of disaster recovery operations to verify that our system components can be recovered.

Secure platform by Amazon Web Services

IT Glue uses Amazon Web Services Inc. (AWS), a third-party data center provider, to host and maintain its production computing systems. Currently, AWS is responsible for the physical security of our environmental protection, networking, database platform and hosting infrastructure. We utilize the AWS security group and load balancer functionality as the primary firewall. Data within IT Glue is stored using several AWS data storage solutions. We provide an integration engine called Sync, which automates data synchronization with several sources. Sync runs within IT Glue's production infrastructure. To adhere to legislated/regulatory compliance concerning data sovereignty, data centers in North America, the European Union and Australia are used.

Amazon's hosting platform is one of the most secure and highly tested systems in existence. Their entire infrastructure is PCI-DSS certified. AWS services maintain PCI-DSS Level 1, SSAE16 SOC 1, SOC 2 and SOC 3, ISO 27001, 27017 and 27018. These certifications cover selected AWS services, including their security governance, physical security, network infrastructure, change management and administration practices. Leveraging these established services, IT Glue delivers a secure and reliable application that you can trust with your operational documentation.

Reliability and disaster recovery

Our goal is 100% uptime. To meet this goal, we have architected our infrastructure and applications to be both robust and scalable. We monitor security, uptime and performance 24/7/365, and have a dedicated team proactively managing the environment at all times. Our service is protected from external attacks through Amazon's denial-of-service protection, a Web Application Firewall (WAF) and PCI-level endpoint security measures. Leveraging this low-latency, high-availability cloud infrastructure enables IT Glue to maintain almost five nines of uptime with a 200 ms average response time.

AWS has built its data centers in multiple geographic regions, with multiple availability zones within each region. AWS regions are completely isolated from one another for maximum fault tolerance and stability. Even though regions are isolated, they are connected to the rest of the AWS network through low-latency links to offer maximum resilience against disruptions.

IT Glue's concept of a "Datacenter" (e.g., our "North America Datacenter" or our "European Union Datacenter") refers primarily to a continental grouping of resources. For instance, in each continent, IT Glue operates its primary infrastructure within a specific AWS region, leveraging real-time data replication to a secondary region within the same continent (e.g., us-west-1 and us-east-1).

We also have two backup and disaster recovery strategies: daily backups and replications between AWS zones. In the case of a disaster, we can operate on a secondary AWS region. Currently, IT Glue replicates its databases between two North American AWS regions. If a catastrophic failure occurs, we have implemented failover capabilities, allowing regional failover. The database is also backed up daily to protect against data corruption. IT Glue ensures that our Disaster Recovery Plan (DRP) is tested at least annually.

In the event of a region failure, data that is already replicated to another region in real time, can be made "primary," with roughly only a 1,500 ms lag in the cutover of workloads. In addition to that, IT Glue performs nightly snapshots of critical database infrastructure to be able to recover data in the event of a disaster recovery scenario.

Account data protection

Password encryption

All data transfer to and from the IT Glue application is through TLS encryption, reducing any opportunity for attacks through active connections.

Passwords are encrypted with AES-256-bit encryption and a unique AES key is generated for each encrypted password. RSA encryption is then used to encrypt the AES key used in the AES-256 password encryption with a 2048-bit RSA key pair. The RSA key pair is then encrypted with a secure RSA key passphrase and stored in an isolated key management system that is locked down to only allow access from our application servers as required for decryption.

To decrypt the data, an attacker would need to effectively access each element of our encryption process. In addition, the web servers for our application are also locked down with multiple firewalls, whitelisting incoming and outgoing traffic, key-based access and many other measures.

When a user needs to access a password, the decryption key that is stored in the isolated key management system and the encrypted password that is stored in the database are both sent to the IT Glue application to be processed. Then, it is sent to the user's browser securely through HTTPS for consumption (see Figure 1).

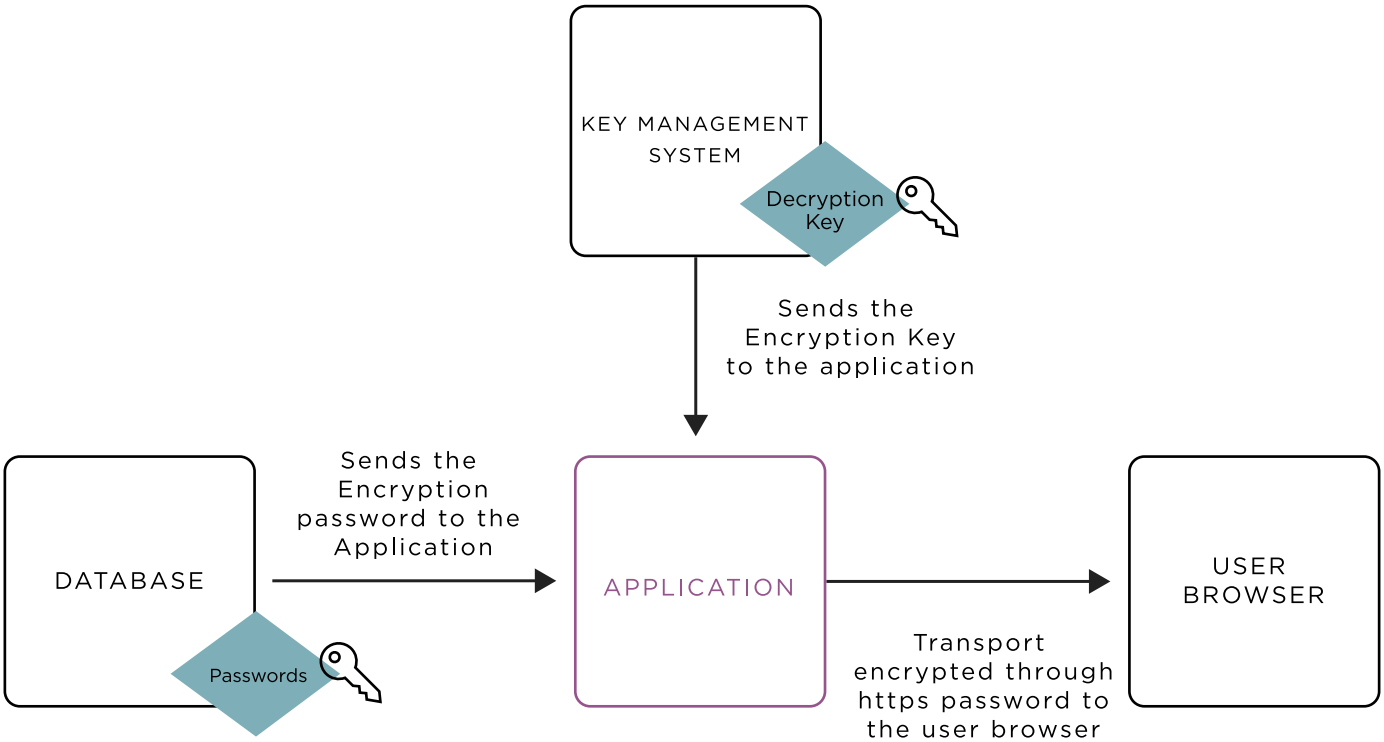

Figure 1. A user accessing a password stored in IT Glue.

Host-Proof Hosting — IT Glue Vault

Users also have the option to add an additional security layer to their most sensitive passwords and quick notes.

With IT Glue Vault, host-proof hosting or client-side-only encryption and decryption are designed to allow a user to only decrypt exclusively at the endpoint level on the user's browser with a user-specific passphrase rather than syncing it to the IT Glue system.

User-based passphrase

IT Glue Vault is encrypted using AES-256-GCM and a unique AES key is generated for the Vault. An IT Glue administrator may choose to grant Vault access to other users by giving them a copy of the Vault AES key. RSA encryption is then used to encrypt the user-based AES key with a 2048-bit RSA key pair. This unique RSA key pair is then protected by the user-based Vault passphrase, which only the user has access to. Each IT Glue user that's granted access can only access the passwords and quick notes within the Vault based on their security permissions.

A number of encrypted keys are sent to IT Glue but they cannot be decrypted without the user-based Vault passphrase. IT Glue servers do not have access to the user-based Vault phrase at any point, so it is not possible for us to decrypt the data (see Figure 2).

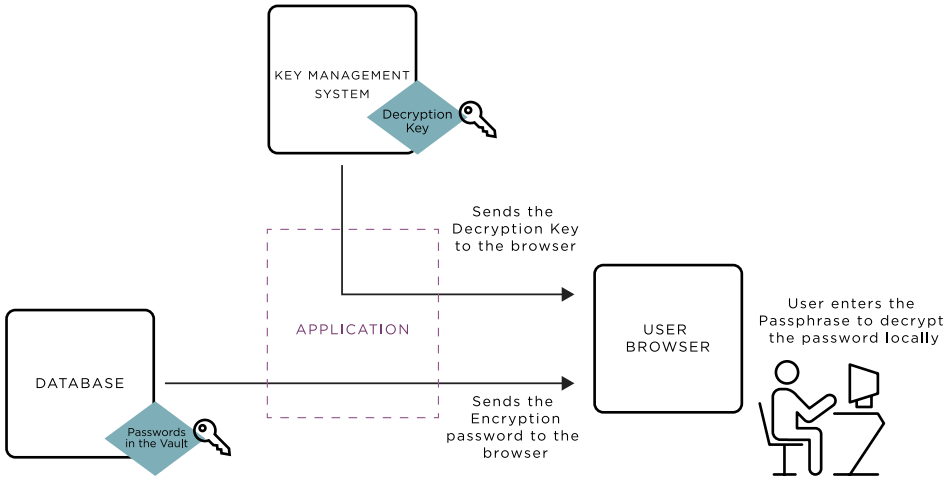

Figure 2. A user accessing a password stored in the Vault within IT Glue.

We have consulted many security and software experts and incorporated industry-leading security practices while developing the Vault. The Vault gives each user total control with a user-based passphrase, not an organization-based passphrase that every employee shares. Having a user-based passphrase means that only the user has the decryption key to the Vault and that the encrypted Vault passwords and quick notes are meaningless to IT Glue or anyone else without the decryption key. Having a user-based passphrase also means an IT Glue administrator doesn't have to change the passphrase every time an employee leaves.

Security permissions and activity logs

IT Glue also offers additional layers of control and protection via security permissions and activity logs. Access to passwords can be controlled at a granular level by limiting access to any combination of users and groups. Revealed passwords only remain visible for a short time with each reveal resulting in an audit trail entry. In addition, all password changes are version controlled and immutable with full rollback capabilities.

User login protection

Malicious and suspicious traffic blocking

IT Glue utilizes AWS's WAF firewall to block malicious and suspicious traffic. Rate-limiting is enforced to help us identify and block suspicious traffic and prevent brute-force attacks.

Enforced multifactor authentication

IT Glue enforces MFA to all accounts for an additional layer of protection on top of your username and password. With MFA, the user will be prompted for their credentials, as well as an authentication code generated by an authenticator application when signing into IT Glue.

IT Glue currently supports most one-time password (OTP) compliant applications that can be used as an additional factor for MFA logins to IT Glue.

SSO Access Control

With the SSO Access Control feature, you can choose whether to make SSO login the only authentication channel into your IT Glue instance. Enforced SSO Access Control provides a secure way of accessing systems and applications, which helps to reduce the risk of security breaches. Thanks to this feature, you are in complete control of your IT Glue user login experience when you set up SSO.

In some cases, organizations may need to grant access to specific users who do not have SSO credentials. As part of this feature, you can select a limited list of users who can log in via SSO or via MFA directly on the IT Glue web app. With SSO user overrides, an administrator can grant access to a specific user, even if they do not have SSO credentials.

This feature is currently available for SAML SSO (both 1.0 and 2.0 protocols), KaseyaOne, as well as JWT SSO.

IP Access Control

IP Access Control allows you to limit IT Glue access to a specified list of IP addresses or a range of IP addresses. Any requests from an IP address list outside the allowed list or range will be denied.

By restricting access from suspicious sources, you can have better control over who can access your sensitive data. Administrators and managers can configure this from the Account tab. This is an optional feature, so you have the option to allow access to all IP addresses too. Moreover, you can deny API access and mandate users to whitelist vendors for active integrations to work as usual.

Conclusion

One of IT Glue's core values is trust. We champion complete vigilance for the privacy and security of information. We take our internal processes and compliance with industry-level security standards seriously.

IT Glue offers you a way to effortlessly maintain the integrity and safety of your data and documents. By embedding security features into our software and maintaining rigorous adherence to our third-party audits, we continue to provide you documentation services you can securely use in your business daily.