VSA™ SECURITY

Kaseya®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Information security is an essential consideration for all MSPs and IT departments globally, regardless of their size or location. Security is always the top priority for Kaseya, and our engineering teams ensure our products are constantly improving through the use of up-to-date technologies and security policies that are enforced for both staff and end users. Security is designed into our products and is complemented by best-in-class Kaseya security practices.

The key factors for controlling the security of a RMM platform include:

Product features

- ✓ Ensuring that all agent/platform and console/platform communications are secure.
- ✓ Built-in protection against brute-force attacks.
- ✓ Ensuring the integrity of runtime code through code signing.
- ✓ Limiting access to the platform and restricting the scope within the platform via role-based access controls (RBAC) and strictly enforcing best practice security hygiene.
- ✓ Ensuring credentials protection through multifactor authentication to prevent lost/stolen passwords from allowing unauthorized access.
- ✓ Enabling secure API integrations (via API tokens) that restrict access and scope for integrations with Security, IT Service Management (Service Desk/IT Documentation), Backup, Compliance, Accounting/Finance and Project Management applications.
- ✓ Providing an immutable audit trail of all activity performed by the platform.

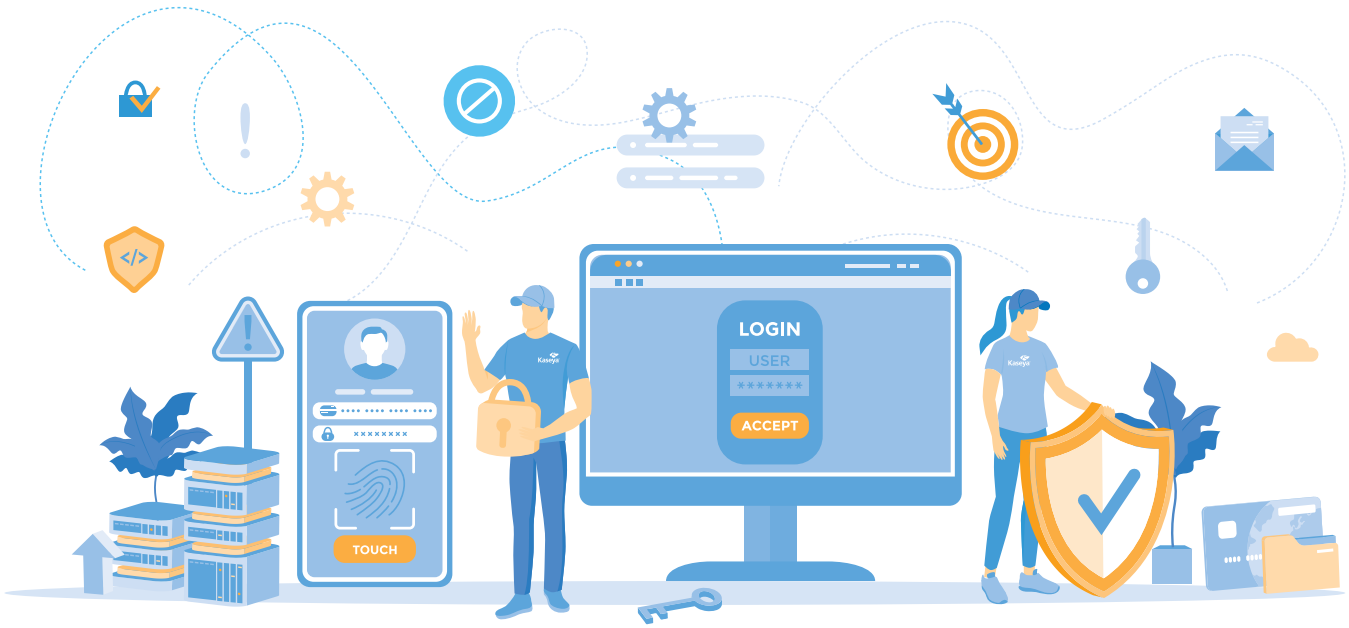
Best-in-class security practices are documented in the Kaseya Trust Center

- ✓ Earning Your Trust covers Kaseya's adherence to compliance standards, security validation practices and our information security strategy.
- ✓ Information Security details Kaseya's commitment to supporting all aspects of the security life cycle.
- ✓ Privacy and Legal demonstrates Kaseya's commitment to privacy standards and practices.
- ✓ Security Advisories brings relevant industry-wide threat insights to your attention.
- ✓ Engage With Kaseya enables our customers and partners to report incidents and vulnerabilities directly to Kaseya.

In a world full of cyberthreats, Kaseya keeps IT and MSPs safe, protected and secure through our industry-leading cybersecurity products, processes and people. The entire team at Kaseya, and especially our Security Operations Center, continuously monitors for any information pertaining to attacks in the industry and will continuously review, adjust and improve our own security practices to ensure you are protected.

Fred Voccola, CEO of Kaseya, summarized our organizational-wide focus on cybersecurity when he said "The Kaseya Community is based on trust. Our commitment to privacy and cybersecurity revolves around you and your data." Kaseya's commitment to transparency and open communication regarding cybersecurity and privacy policies is documented at Kaseya.com/trust-center/.

As always, our team is here for you should you have questions or concerns at security@kaseya.com.



PRODUCT LEVEL PROTECTION

Transport & message encryption

VSA 10 uses end-to-end encryption, which ensures that your private infrastructure information stays private and unauthorized access is prevented. All connections to VSA services are done with fully encrypted communication based on RSA public/private key exchange and AES (256-bit) session encoding. This is a current industry standard encryption algorithm used worldwide.

All communication messages are encrypted with AES (256-bit) symmetric keys, which utilize the RSA public/private key exchange mechanism to guarantee that in the unlikely event of transport encryption failure, privacy is not compromised. Keys are automatically rotated on a controlled interval to prevent brute-force attacks, also adding an extra layer of security against man-in-the-middle attacks.

BRUTE FORCE PROTECTION

A brute-force attack is a trial-and-error method commonly used to gain unauthorized access to accounts. With the growing computing power of standard computers, the time needed for guessing long passwords has increasingly reduced. Kaseya defends against brute-force attacks by blocking multiple failed requests to VSA 10 and by increasing the timeout between failed requests.

CODE SIGNING

All the VSA 10 Windows and MacOS agents and applications are signed using a code signing certificate to guarantee that the binaries were not altered or compromised by a third party.

DEVICE ACCESS CONTROL LISTS

For enhanced security on the VSA 10 mobile apps, you can set up:

- ✓ PIN code mobile authentication (and Touch ID / Face ID where supported) to prevent unauthorized access to the monitored systems.
- ✓ Centralized device access control lists with the ability to remotely disable mobile devices.
- ✓ Default device access control list for newly added systems that allows you to deny access for all systems until you explicitly approve the new device.

TWO-FACTOR AUTHENTICATION

Two factor authentication (2FA) is enforced, providing a security layer that will require an additional step to access your account or perform certain operations.

You can opt-in to receive push notifications on your mobile apps to approve authentication requests, or use a TOTP app (time-based one-time passcode) like Google Authenticator, Authy or 1Password.

When setting up 2FA, the system will also generate backup codes that can be used when all the other authentication methods are not available. Each backup code can only be used once.

SECURE INTEGRATIONS

Integration is the lifeblood of both an IT professional's day-to-day and Kaseya's IT Complete platform. VSA 10 leverages secure, token-based authentication for integrated solutions. Personal access tokens can be much more secure than a typical user password, and unlike a password, a token can be restricted to access only explicitly allowed APIs. Tokens can be given more restricted role access rights than the user it belongs to based on which specific API calls are required for the application. VSA 10 uses a least-privileged approach with limited scope and limited duration of access to ensure secure communication between integrated tools.

AUDITING AND LOGGING

All VSA 10 commands are locally logged in both the Windows Application Log and in the VSA Server database for auditing reasons. The account owner is notified via email every time a new mobile device or a web browser instance is registered on the account.

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

Kaseya®