

Kaseya® Cryptography

At the center of the Kaseya architecture is a strong conviction to security. In fact, many government agencies utilize Kaseya to manage local and remote systems.

The Kaseya VSA uses encryption to secure communications between its client and server components, which are the Agent and the KServer. The cryptography is implemented completely in software in a FIPS 140-2 Level 1 certified crypto library (certification currently in progress as of September 2011) that is linked into the KServer and Agent applications.

The Kaseya VSA uses 256-bit AES for its encryption algorithm to protect communications between the Agent and KServer applications. The key length is set at the time that the VSA software product is built (i.e. compiled and linked). The cryptographic software library includes the Secure Hash Algorithm–256 (SHA-256) implementation.

The communications, protected with AES-256, is processed as follows:

- 1) Agents are deployed with a username and password with a maximum of 32 hex characters (256 bits).
- 2) An Agent initiates communications to the KServer by sending its name/GUID as identification.
- 3) The KServer responds by sending a random number challenge back to the Agent. The use of a different random number with each checkin session prevents playback/man-in-the-middle vulnerabilities.
- 4) The Agent computes a SHA-256 value over a combination of the current password and random number.
- 5) The Agent sends the resultant hash value to the KServer.
- 6) The KServer computes the SHA-256 hash of the same combination its copy of the random number with its copy of the current password for the particular Agent.
- 7) The hash values are compared and if they match, then the Agent session has been authenticated.
- 8) All subsequent messages, containing commands and responses, between the KServer and Agent are encrypted using AES-256, where the SHA-256 result is used to derive the session encryption key.

The encryption key is discarded after each session between the Agent and KServer. The user password is updated independently both at the Agent and KServer applications after each session. An identical procedure is used both by the Agent and KServer independently to prepare for the next communication session.

The Kaseya VSA uses encryption to secure communications between its client and server components, which are the Agent and the KServer.

