How LogMeIn Rescue Supports PCI Compliance

LogMeIn understands that organizations that store, process, or transmit cardholder data must meet strict requirements to be PCI compliant. Although no PCI evaluation or certification process exists for third party applications such as LogMeIn Rescue, security is an integral part of our service offering, software, and policies. This document indicates some of the ways in which we help organizations using LogMeIn Rescue to comply with PCI requirements.

According to the PCI Security Standards Council:

- The PCI Data Security Standard applies to all organizations that store, transmit or process cardholder data.
- If you are using a third party product, the product should support the compliance of your organization.
- It is the merchant or service provider's responsibility to ensure that they are using only products that support compliance. However, the PCI Security Standards Council does not offer certification for most of these [third-party] products at this time.

REQUIREMENT: BUILD AND MAINTAIN A SECURE NETWORK

1. **Install and maintain a firewall to protect data**.
   LogMeIn servers are hosted at a leading, carrier-grade data center with restricted, secured access, redundant power, dual HVAC, fire detection systems, and 24/7 network monitoring. See the LogMeIn Rescue Architecture whitepaper for details.
2. **Do not use vendor-supplied defaults for system passwords and other security parameters.**
   LogMeIn Rescue customers define their own passwords when creating an account. These passwords are not generated by LogMeIn. Furthermore, additional settings in the LogMeIn Rescue Administration Center allow organizations to adhere to strict password policies:
   a. *Minimum password strength.* To help ensure that LogMeIn Rescue users choose a good password, we've created a "password strength meter" that visually displays how strong your password is while you are creating it.
   b. *Maximum password age.* LogMeIn Rescue Administrators are able to define a maximum password age. Specify the maximum age allowable (in days) according to your policies. Users must re-set their password after the time allotted expires.
   c. *Force password change.* Force users to change their password when they change their Windows password.

REQUIREMENT: PROTECT CARDHOLDER DATA

1. **Protect stored data.**
   No data from remote computers is stored on LogMeIn servers (only session and chat data is stored, and Rescue allows organizations to store text chat exclusively on their own servers, in the event that text chat contains credit card data). All data in transit is protected by end-to-end 256-bit SSL encryption. Furthermore, technicians can be denied permission to use the file transfer feature, thereby eliminating their ability to take a file from a remote computer. For those technicians with file transfer rights, MD5 Hash provides enhanced security and traceability of any file transfers.

For details regarding the physical security of our datacenters, see the LogMeIn Rescue Architecture whitepaper.

2. **Encrypt transmission of cardholder data and sensitive information across public networks.**
   All LogMeIn Rescue support sessions are protected with end-to-end 256-bit SSL encryption, the de-facto standard for secure communications over the Internet. This encryption method has been endorsed by Visa, MasterCard and American Express—the same coalition that came together to create the PCI compliance standards. The SSL implementation used by LogMeIn Rescue is OpenSSL.

REQUIREMENT: MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

1. **Use and regularly update antivirus software.**
   LogMeIn cannot be responsible to the antivirus practices of its user base, but does actively protect and secure its own systems and servers.
2. **Develop and maintain secure systems and applications.**
   LogMeIn deploys systems with hardened operating systems and maintains current security patch levels on exposed systems. See the LogMeIn Rescue Architecture whitepaper for details.

REQUIREMENT: IMPLEMENT STRONG ACCESS CONTROL MEASURES

1. **Restrict access to data by business need-to-know.**
   LogMeIn Rescue has a number of features in place that restrict access to data, including:

   a. The technician management model makes it possible to limit specific support sessions to certain technicians. For example, support requests from certain users having critical data on their devices could be offered only to senior support technicians.

   b. Unless a technician has permission to use the Unattended Access or Connect on LAN feature, a remote user must be in attendance at the remote PC to accept and authorize support. (With both of these features the technician must authenticate using Windows Administrator credentials, with access according to rights granted outside of LogMeIn Rescue.) The remote user has override rights, and can end the support session at any time.

   c. Once a remote support session has concluded, the LogMeIn Rescue Applet is automatically removed, and all access rights revoked. Future support sessions must be permitted by the end user every time except when a technician has permission to use the Unattended Access or Connect on LAN feature. With both of these features the technician must authenticate using Windows Administrator credentials, with access according to rights granted outside of LogMeIn Rescue.

   d. Administrators can set granular permissions for its technicians, authorizing technician groups to perform only specified functions. This includes setting permissions to allow (or deny) remote control, remote view, file send, file receive, file management, URL send, system info viewing, rebooting, session screen recording, private session starting, unattended access, and single prompt for all permissions.

   e. LogMeIn Rescue can be set so that the end user being supported is required to permit each support act individually: view system information; remote view; remote control; file transfer, etc.

2. **Assign a unique ID to each person with computer access.**
   Each administrator and technician has a unique password for logging in to LogMeIn Rescue, and

specific permissions are attached to that user. Technicians cannot view, access, or modify settings established by administrators. Technicians are assigned unique login IDs and corresponding passwords by their administrators (who can force users to change those passwords). These credentials are entered into the login form on the LogMeIn Rescue website.

When combined with your organization's Windows logon procedures, you gain two-factor authentication (users log onto their PCs, and then log into LogMeIn Rescue using a password only they know).

Additionally, Administrators can immediately revoke access for any terminated users; block out users after multiple unsuccessful login attempts; and define timeframe by which an inactive user/session will timeout.

End users being supported by technicians enter a unique PIN code or click a unique link to initiate a support session. Authentication procedures in LogMeIn Rescue ensure that a technician or administrator logging into the Rescue system is in fact who he claims to be.

3. **Restrict physical access to cardholder data.**
   Administrators can set IP address restrictions, ensuring that LogMeIn Rescue Technicians/Administrators are using Rescue only within accepted physical confines.

   Though no cardholder data is held in our datacenters, see the LogMeIn Rescue Architecture whitepaper for details regarding the physical security of our datacenters.

REQUIREMENT: REGULARLY MONITOR AND TEST NETWORKS

1. **Track and monitor all access to network resources and cardholder data.**
   Any remote support solution must place strong emphasis on accountability. LogMeIn Rescue provides several auditing and monitoring features.

   a. The "Chat log" is saved in the Rescue database. The "Chat log" is transmitted to the Rescue servers by the technician console in real time, and contains events as well as chat messages that pertain to a particular support session (although organizations have the option to house chat text exclusively on their own servers).

      For example, a log file would display when a remote control session is started or ended, or when a file is sent by the technician to the end user. Accompanying metadata, such as the name of a transmitted file, is also included in the log when applicable. The "Chat log" database can be queried from the Administration Center.

   b. Master Administrators can force recording of remote control and desktop viewing sessions to provide a trail of a technician's actions. Once set, technicians cannot cancel this function. Administrators can also specify a central location to which the recordings are written.

   c. File transfer traceability: MD5 hash is calculated and recorded for each file transfer. The hash is shown in the Chat Area on the Technician Console and on the customer's PC. It is also included in the session log. Generating an MD5 hash makes it possible to easily check whether a file sent to a customer's PC has been altered. Reports that help audit technician and session activity can be generated with details of:

      i. Technician or Administrator login details: the start time, end time and duration of each technician or Administrator login period, together with the WAN IP address from which they logged in.

      ii. Session details: the start time, end time and duration of each support session; which technician handled the session; the session ID assigned automatically to the session; the customer's WAN IP address (if known); the tools used by the technician to resolve the incident; whether a file was exchanged with the customer; whether the customer's PC was rebooted during the session; and whether the session was recorded.

iii. The Chat log. On screen, this gives an overview of sessions, together with a button which can be used to retrieve the contents of the chat during a session.

2. **Regularly test security systems and processes.**
   LogMeIn is committed to ongoing security, and continually reviews its software, policies and data centers for security.

REQUIREMENT: MAINTAIN AN INFORMATION SECURITY POLICY

1. **Maintain a policy that addresses information security.**
   LogMeIn Rescue has been designed to help support organizations maintain strict information security policies.

   a. Access Controls

      i. Define permission-based access on a granular level (for example, allow technicians to use desktop viewing only, but not remote control).
      ii. No data from remote devices is stored on LogMeIn servers (only session and chat data is stored; chat text can be stored separately). Additionally, permissions can be set so that technicians do not have file transfer rights, eliminating their ability to take files from remote devices.
      iii. Unless a technician has special permission to use the Unattended Access or Connect on LAN feature, the end user must be present at the remote machine, and permit remote access. (With both of these features the technician must authenticate using Windows Administrator credentials, with access according to rights granted outside of LogMeIn Rescue.)
      iv. Unless a technician has permission to use the Unattended Access or Connect on LAN feature, the end user maintains control and can terminate the session at any time (With both of these features the technician must authenticate using Windows Administrator credentials, with access according to rights granted outside of LogMeIn Rescue.)
      v. Permissions can be set so that the end user must explicitly allow a technician to use specific functions (remote control, desktop view, file transfer, system information, and reboot & reconnect)
      vi. Access rights are automatically revoked when session is terminated except when a technician has permission to use the Unattended Access or Connect on LAN feature. (With both of these features the technician must authenticate using Windows Administrator credentials, with access according to rights granted outside of LogMeIn Rescue.)
      vii. IP address restrictions limit use by physical location
      viii. Forced password expiry and change
      ix. Predetermined time of inactivity forces automatic logoff
      x. Hosted at redundant leading, carrier-grade data centers with restricted, secured access

   b. Audit Controls

i. Option for forced session recording, with ability to store audit files on a secure network share
ii. Technician sessions and remote session activity is logged on the host computer to ensure security and maintain quality control (successful logins, unsuccessful logins, remote control started, remote control ended, reboot initiated, logout)
iii. Person or entity authentication; Technicians identity is defined by a unique email address, and technician must be authenticated
iv. Excessive number of unsuccessful login attempts (three unsuccessful attempts) will lock the Rescue account

c. Transmission Security

i. End-to-end 256-bit SSL encryption of all data
ii. MD5 Hash for enhanced traceability of file transfers