SUMMIT SERIES

Frequently Asked Questions

Q: What abilities does the solution have to log/store data and for what devices?

A: All transactions performed at the safe are logged to the cloud. Device firmware level metrics and usage data are extracted from the device and are made available to the reporting and maintenance modules. All information is transferred to the cloud and configurable alerts are generated in near real time.

Q: What user activities are logged?

A: All user activity is logged through the application level software and reported up to the cloud backend.

Q: What network connectivity details are logged?

A: Connect, Disconnect, IP, GW, Netmask, MAC, MTU.

Q: What other events are captured and stored?

A: VPN, data synchronization, content and firmware updates, system level metrics.

Q: What is the retention length of logs stored?

A: 30 days for application logs, 1 year for server logs, 3 months for safe level transaction records, 6 months on the server (database). Data may be archived for longer periods based on customer requirements but is not retained in the production databases beyond these periods.

Q: What is the process for Application software patching and configuration (e.g. User management, device configuration)?

A: Remote update process – the safe or other cash handling device checks into the server(s) periodically for updates. As currently deployed this happens every 5 minutes or less – the interval is configurable.

Q: What is the process for OS patching (e.g. Network setup, patches)?

A: The operating system is remotely updatable including the ability to apply patches and upgrade packages. Adjustments to network setup can also be configured remotely.

Q: What is the process for Firmware patching (e.g. Tracking and updating, acceptance of bill denomination changes)?

A: Remote update process is currently managed on an as-needed basis but may be automated based on business need.

Q: What other remote capabilities are there?

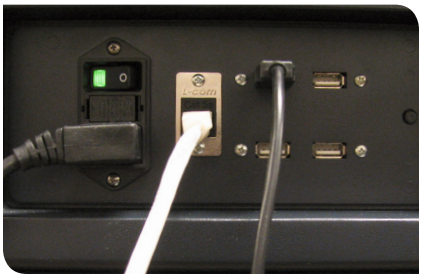
A: Software restart, note device initialization, full safe configuration and management, and touchscreen recalibration.

Q: Does the solution offer the ability to create device location specific (or grouped) messaging to display immediate notification/bulletin for end user messaging? If so, please explain the functionality.

A: Yes, the safe level software includes a scrolling message center that is used for status, event notifications and messaging. This is located at the bottom of the touchscreen and is available at all times.

Q: How do back office users access the software solution?

A: Full remote management via a web browser using a secure connection and login credentials. Capabilities include configuration changes, software revision and a robust business intelligence reporting platform (cash and activity level reporting).



Q: What data is accessible to display to the customer?

A: All transaction and configuration based information is available, accessibility will be determined by role and entitlement based on user credentials.

Q: What level of encryption capabilities are used for data storage, data transmission and user access (internal and remote)?

A: All data from the safes to the servers is encrypted by Blowfish encryption during its entire route. Triple DES and other ciphers also available. Access to the web services is encrypted via SSL.

Q: How is physical hardware/software maintenance performed (at device)?

A: Software maintenance is performed remotely via web services. Hardware maintenance can be accomplished through the dispatch of our Field Service Technicians. Reliability is enhanced by our ability to perform predictive maintenance based on metrics kept by the system.

Q: What is the process for a sync after an offline condition?

A: Once connection is re-established all locally stored information is pushed to the cloud, and all configuration data is pulled down. The safe synchronizes at configurable intervals – typically less than 5 minutes. The sync process has 4 steps: check for updates and commands; gather and report health and status metrics; report transactional events that the server(s) have not received yet; check and update configuration.

Powered by APUnix