



Security

RMS security features designed to keep your business safe

Take Control of Your Password Management

With RMS password management, you can create unique password requirements, like character rules, password length, number of password attempts allowed, and expiration frequency. You can even choose how long a user can be inactive in the database until they're automatically logged out.

Double Up Your Security with Two-Factor Authentication

Prevent unauthorized access by adding a second layer of security to your staff's login process. Setting up two-factor authentication provides extra protection by requiring a second method of confirmation, such as a code sent to your mobile device, keeping unauthorized users at bay even if they've gained access to login credentials.

Protect Your Database with Network Controls

With the Restricted IP Addresses tool, you can grant database access only to users with static IP addresses on specific networks. Want to confine database access to just your property? Simply select "Use Current IP" from the front desk.

Authenticate & Reduce Logins with SSO

Single Sign-On uses an Identify Provider to authenticate database access. Easily set this up for extra security and the ease of using just one login for multiple applications.

Security is a Core Feature of RMS

RMS regularly conducts extensive third-party examination and compliance certification to keep your business secure, including PCI compliance, Microsoft Azure security policy based on ISO 27001, SOC2, military-grade certifications, and more.

