RUNMYJOBS® SECURITY

FLEXIBLE, RELIABLE AND SAFE

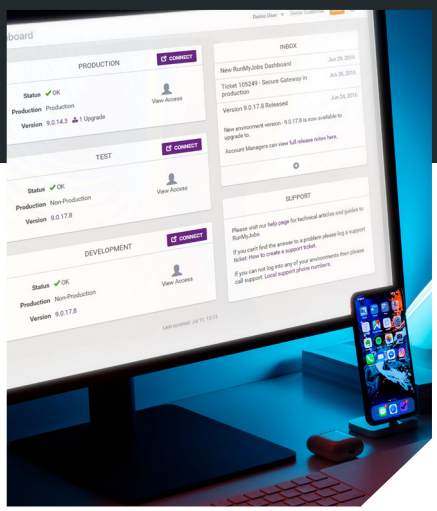
Redwood has been a leader in automation technology for more than 25 years and is now the only global provider with this single focus. As such, our approach to automation security is unparalleled in the industry.

RunMyJobs® (RMJ) is the only workload automation and scheduling solution available as Software-as-a-Service (SaaS). It's designed to integrate easily with your existing security framework. RMJ also includes its own state-of-the art security technology and standards that uphold the highest possible availability and security with end-user simplicity.

Our cloud infrastructure is delivered through industry leader, Amazon Web Services (AWS), which provides world-class support for complete resource flexibility, redundancy, high availability and security. In fact, our cloud-based service comes with an availability guarantee with ISAE 3402 (SSAE 18) type II external certification. ISO 27001 certification is currently in progress.

RMJ uses our unique Secure Gateway technology to connect your system landscape, which employs strong encryption to support our high security standards.

The security section of the RunMyJobs admin dashboard features an overview of all users, including their user type and access rights within your RMJ environments. Here you can see, define and manage user roles and permissions. Administrators can use this dashboard to adjust specific user relationships to suit your organization's own security standards and requirements. RMJ also integrates with Active Directory, LDAP-managed security environments, and supports the SAML protocol for single sign-on deployment.



USER ACCESS AND TWO-WAY BROWSER AUTHENTICATION

Customers can only log in with a named account. A specific user at the customer location is designated as the account administrator during customer account creation. This user can create, modify and delete additional users for the customer account.

Whenever a user logs in from a browser that they haven't used to access the scheduling environment before, they are emailed a link to authorize that browser. Clicking on the link sets a special browser cookie with the user. Users cannot access the service without this cookie. The only way to access this cookie is via a link in the email. The link itself times out after a short time. Separate authorization is required for each browser and for each system. If the authentication cookie is deleted, browser authorization will be required again.

RunMyJobs scheduling includes a standard set of typical user roles, each with their own set of privileges:

- **ADMINISTRATOR** - create objects, schedule tasks, run processes and monitor activities
- **OPERATOR** - schedule tasks, run processes and monitor activities
- **VIEW** - monitor activities
- **LOGIN** - can connect but can only perform tasks granted via custom roles
- **NO ACCESS** - cannot access the environment

SINGLE SIGN-ON SUPPORT

RMJ supports single sign-on technologies. You can configure it to authenticate against an external security provider that supports the Security Assertion Markup Language (SAML) standard as defined by RFC 7522. You can also use SAML to directly integrate with your active directory domain controller using active directory federation services, or through online middleware providers such as OneLogin, Ping Identity and Okta. When using SAML authentication, you enable single sign-on, which means machines that are part of the domain can transparently log in to the solution.

CLOUD SECURITY

RMJ is both ISAE 3402 and SSAE 18 certified to support end-to-end service control. All communication is encrypted and authenticated using military-grade TLS 1.2 technology. Communications with the user interface and connections to the remote servers and applications on which processes are automated are secured with HTTPS (also with TLS 1.2 encryption).

Redwood's infrastructure within AWS includes firewalls between the internet and the service where the provisioning and automation infrastructure for customers' environments are hosted. The account management system and the customer environments are hosted on different AWS instances. Only operational scheduling staff have access to this area. Multiple security layers are in place to prevent unauthorized access.

Multiple security layers are in place to prevent unauthorized access at any time.

The RunMyJobs scheduling website is protected by an Extended Validation SSL certificate (EV-SSL). This provides a deep level of encryption, including in-depth identity checks and additional visual indicators to reduce risks from phishing and other attacks. RMJ implements an ongoing policy of holistic security improvements to stay ahead of new dangers.

Our security implementation around scheduling adopts a defense in depth philosophy that has proven to be strong and successful for decades. For more information about our security, contact your Redwood representative.

TALK TO A REDWOOD REPRESENTATIVE NOW TO LEARN MORE, DISCOVER MORE AT WWW.REDWOOD.COM