Tenant Configurable Security Tools

Last Modified on 12/03/2024 1:09 pm AEDT

In this article:

Overview

The ReadiNow platform offers a rich set of tools to allow customers to configure and monitor their own security within the platform tenant.

Configurable security policy and tools include:

1. Access control configuration
2. Single Sign-On (SSO)
3. IP Address Range White-listing
4. Configurable password policy
5. Configurable Record change audit log
6. Security audit log
7. Configuration change audit

Access Control Configuration

ReadiNow allows for rich record access control policy to be defined that can be automatically driven by the relationships that interconnect your data records.

For example, with a single access rule, it is possible to define a policy that would allow Employees to have access to documents that are attached to projects, where the project is marked as active and assigned to the same region as the employee. Record access changes are automatically reflected as any of the relevant record relationships are updated. Rich policy conditions involving relationship connections such as this can be defined over any relationships.

Please refer to the “ReadiNow Access Control Security” whitepaper to learn more about the relationship based access control policy, as well as other access control features (including as nestable user roles, security relationships, and navigation access).

Single Sign-On

ReadiNow supports Single Sign-On via both SAML and OpenID Connect identity providers. This allows for integration with Microsoft Azure single-sign on, and other popular identity providers.

Multi-factor authentication is supported when using an identity provider that supports it, such as Microsoft Azure.

IP Address Range White-listing

Customers may self-serve to configure a white-list of acceptable IP-address ranges. This allows, for example, the platform to be configured so that access will only be provided to computers and devices if that are originating from within a company office network, or via a company VPN.

Attempts to log in or use the system from an IP address outside of this range are denied and logged.

Configurable Password Policy

Customers may define their own password policy restrictions to meet their own security policy standards.

Configurable options include:

- Minimum length
- Whether it must contain upper-case, lower-case, digits, characters (individually)
- Maximum password age
- Number of incorrect password attempts before lockout
- Lockout duration

Record Change Audit Logging

Customers may log record-changes for auditing by configuring audit policies.

An audit policy specifies the type of record (the object), and the fields and relationships on that object, that will be monitored for changes.

The record change audit log include the type of change, old and new values, time of change, and the user account that made the change.

Security Audit Log

Security-sensitive events are logged and available to the tenant administrator. The tenant administrator can configure the log sensitivity and retention.

Event Type	Events

Event Type	Events
User accounts	• Creation • Deletion • Rename • Expiry • Password change • Change user account expiration • Change of user account status
Login sessions	• Logon • Logoff • Locked user account
User role configuration	• Creation • Deletion • Rename • Membership change
Access rule configuration	• Creation • Enabling • Condition structure change • Permission change • Deletion
Password policy	• Change
Application	• Creation • Deletion • Deployment • Publish

Configuration Change Log

In addition to the security audit log, the platform maintains a log of changes made to the structure of the ReadiNow platform applications (the 'metadata'). This includes, but is not limited to:

- Object/schema changes
- Forms and screens

- Workflows
- Report
- Charts
- Navigation
- Administrative settings and configurations

Configuration change log details include:

- Time of change
- User account
- Type of metadata changed
- Description of the change
- And, where available, the object that the change relates to