

Access Control

Last Modified on 12/11/2020 3:14 pm AEDT

Overview

Access Control is the security system that determines which users have permission to:

- view, modify, and delete existing existing records
- create new records
- access screens, reports, and other content

Access control rules that automatically grant per-record permission based on the metadata of those records, or based on how the records relate back to individual users, can be easily achieved by creating an Access Rule report.

See also: [Access Control Security whitepaper](#).

Access Control Terminology

- **User** - Each person typically has one user account. All interactions with the ReadNow server are done in the context of a user account.
- **User Roles** - Users are members of security roles. A user can be in multiple roles. Role can be members of other roles.
- **Permission** - A permission is something that is required to perform an activity, such as View, Modify, Delete, Create. For example, you need the **View** permission to see a record.
- **Access Rules** - An access rule (or simply Rule) grants some permissions for users in a role to interact with records of a particular type.
- **Access Rule Reports** - Access rules typically include a report which acts as a record filter to determine which records are included by the rule. Whether or not an access rule grants access to a report is determined by whether or not the access rule report, and its analyser filter, includes the record as a row.
- **Navigation Access** - Simply makes app content, such as screens and reports, visible to a role
- **Security Relationships** - Allows a relationship to be configured so that permissions for one record flow to related records.

Other Elements of Security

The ReadNow platform supports other security features such as [SSO](#) (single-sign), configurable [Password Policy](#), [IP whitelisting](#), configurable [Record Audit Log](#) and [Security Audit Log](#). These work in tandem with access control, but are not part of access control.