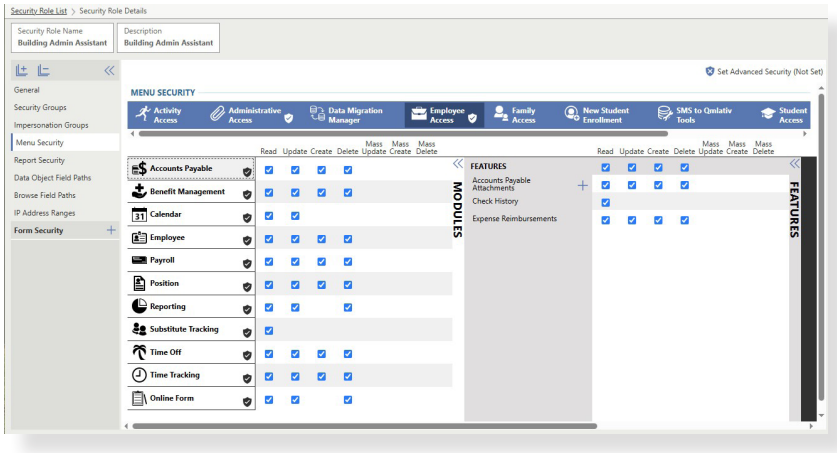
SYSTEM ADMINISTRATION TECH

SECURITY ADMINISTRATION

STREAMLINED SECURITY MAKES ADDING AND CHANGING PERMISSIONS A BREEZE.



- Flexible permission setup helps define the unique roles held at your district
- Security will streamline access, connecting users to screens, reports, attachments, accounts, and access groups
- Users can retrieve forgotten usernames and passwords at their convenience
- System profile tracks login history, screen usage, and impersonations

TAILORED SECURITY SETTINGS

Tailor security settings to meet the needs of your district by using built-in multi-factor authentication, password requirements, session time out settings, and more, all within Qmlativ. To make logging into the system easy, single sign-on can be set up within Qmlativ, or the system can be connected to common single sign-on providers. Sensitive fields can be restricted through customization. IP address ranges can determine what areas of the system are available in-district only. An "impersonate user" option can be granted to those individuals that are setting up security to provide peace of mind on what a user has access to.

ENCOMPASS MORE WITH SECURITY GROUPS

Users will be put into security groups that encompass roles, account number access, and groups. Roles will determine what screens someone has access to and what they can do in those screens, such as viewing or interacting with the data. Attachment types and report security are built into the district-defined roles so users only see the attachments and reports relevant to their role. If a report contains an account number or employee from a supervised position, the report can read off that user's account or position access to determine the data that displays. Account groups, purchasing groups, expense reimbursement groups, and more are part of that security group. This will tell the system not only what general ledger account numbers those security group users have access to, but will define the approval process when a transaction is entered.

SECURITY AUTOMATION FOR EMPLOYEES

A security username and email can be automatically created for a new employee using a district-defined structure. Upon an employee add, access to the Employee Portal can be granted by default and a message can be sent to that new user. A forgotten username or password can easily be retrieved by the user.