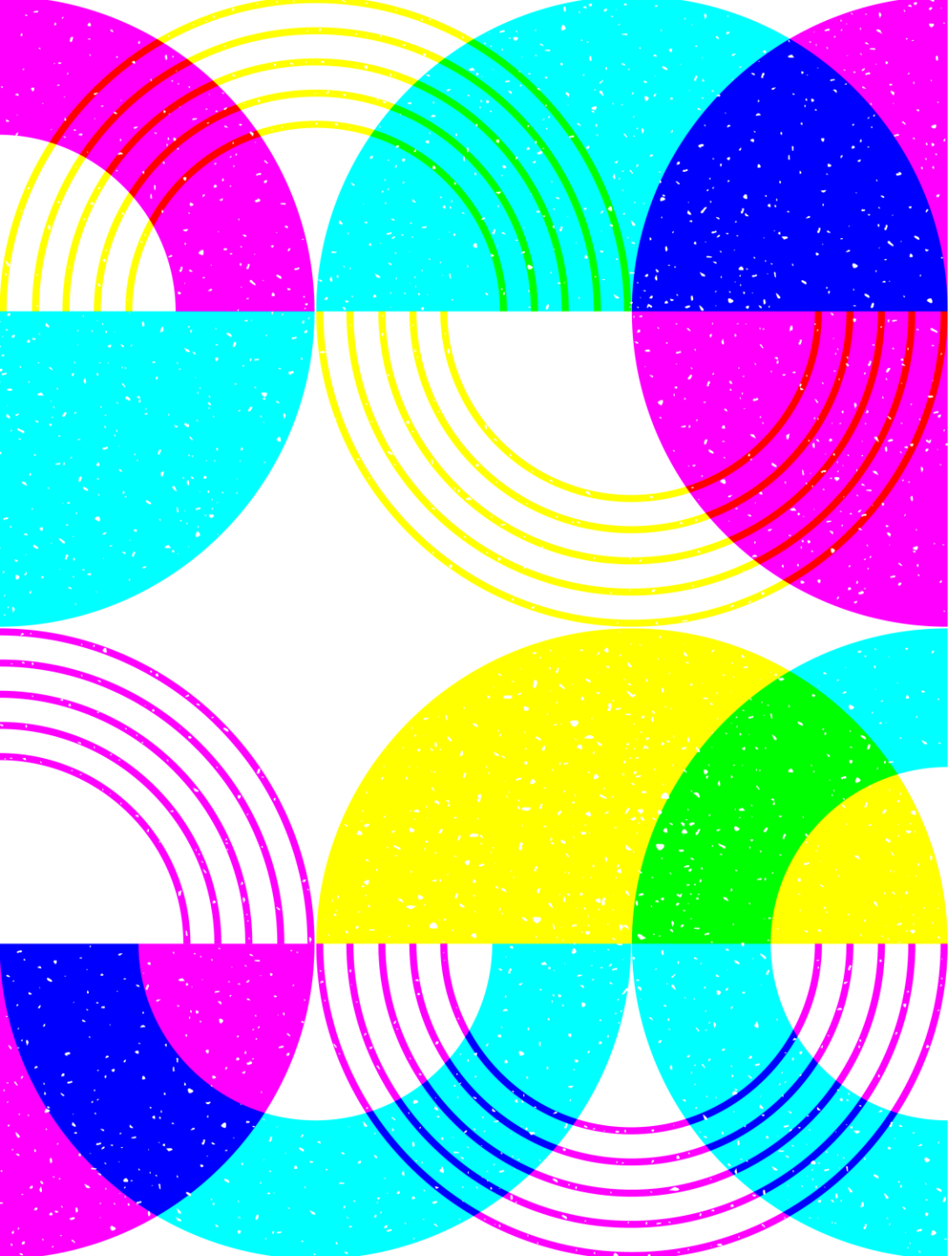


follow us on social!

#skyicon



SKYWARD®

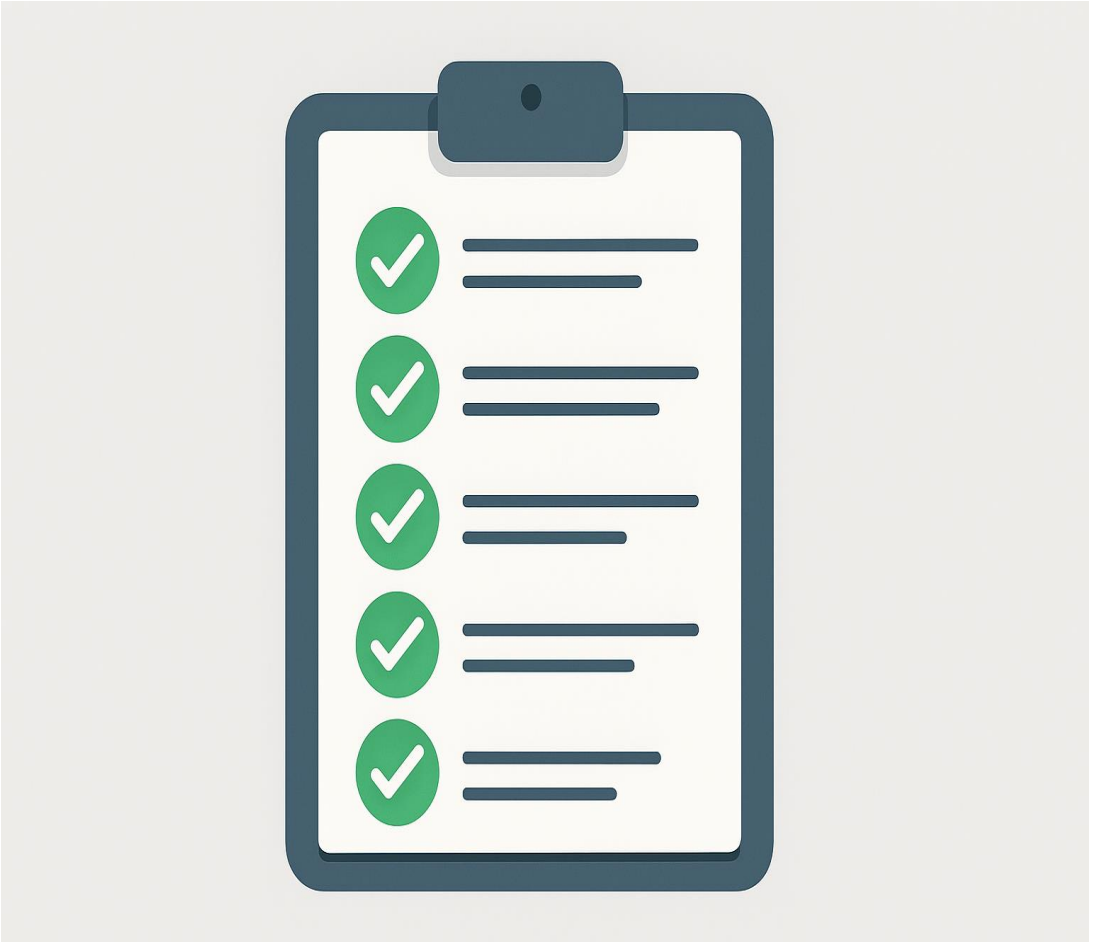
iCON

Securing the Shirt: ERP Security Setup Differences in SMS 2.0 and Qmlativ

Brad Evenson – Product Manager

Agenda

- Planning your Security
- Security Roles vs. Security Groups.
- Role Setup Options.
- Menu Security
- Security Groups
- Reports/Features
- Utilities
- Other Features
- Future Enhancements
- Q & A

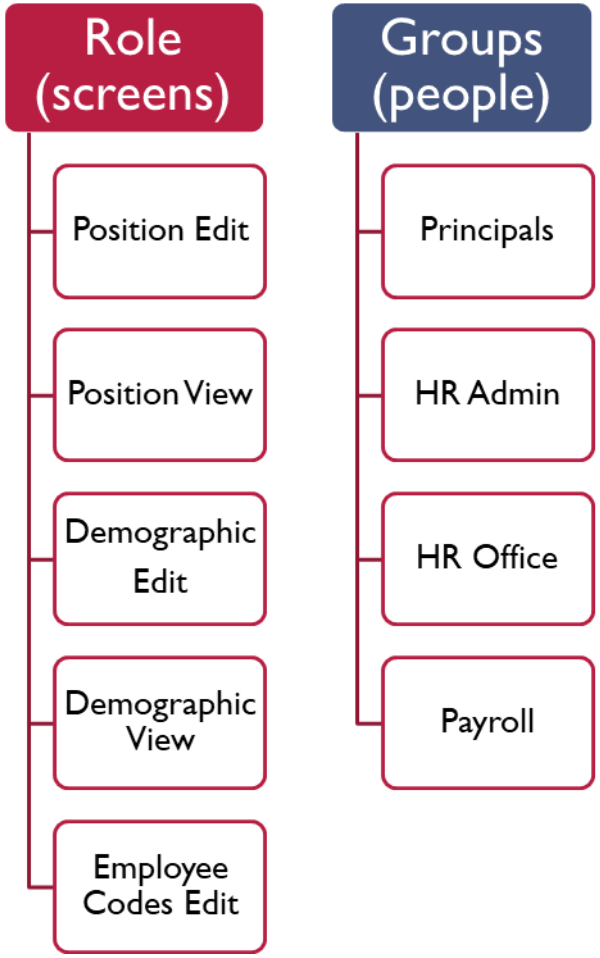


Plan Your Security

- Map out Security ahead of your migration
- Opportunity to do cleanup and review settings
- Export/Import options to transfer from Prelim to Production
- Importing from 3rd Parties.



Security Roles vs. Security Groups



Separated users and screens

Security Roles – screens and reports, with level of access (create, read, update, delete)

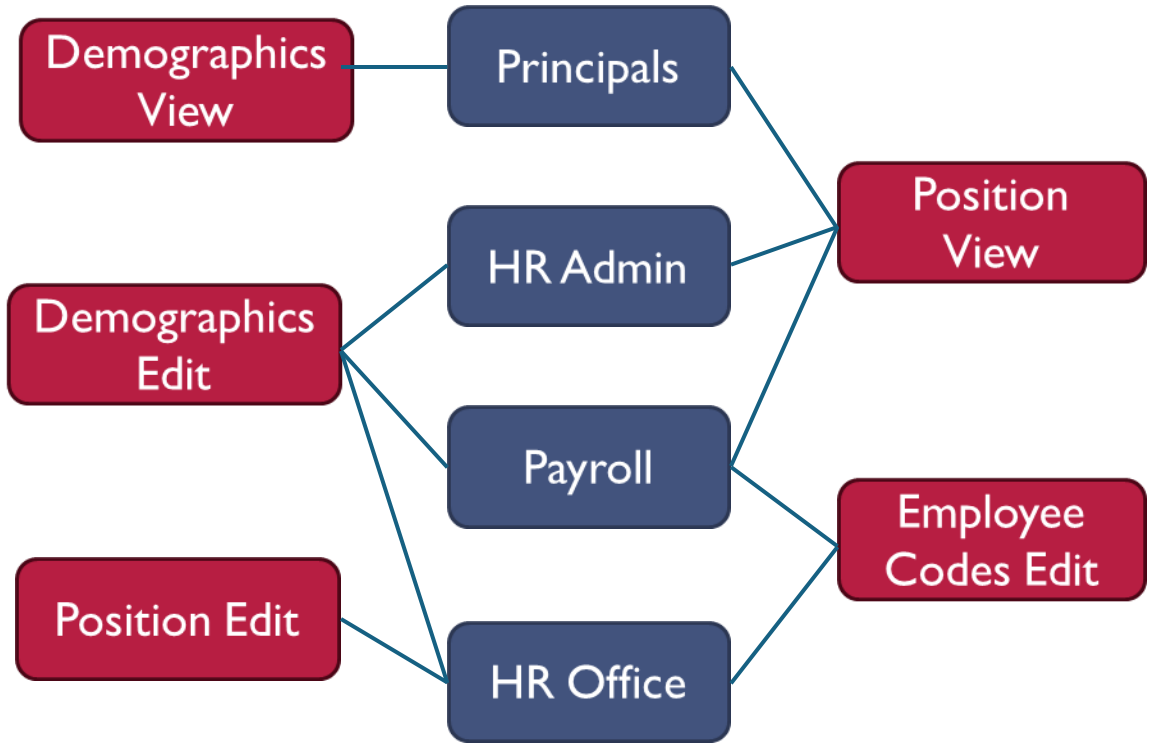
Security Groups – users that will be doing the same tasks

Entities are assigned to users, not groups

Security Group Membership – entity that applies to the user for the group

Results in few Security Groups

Role Setup Option – Task Based



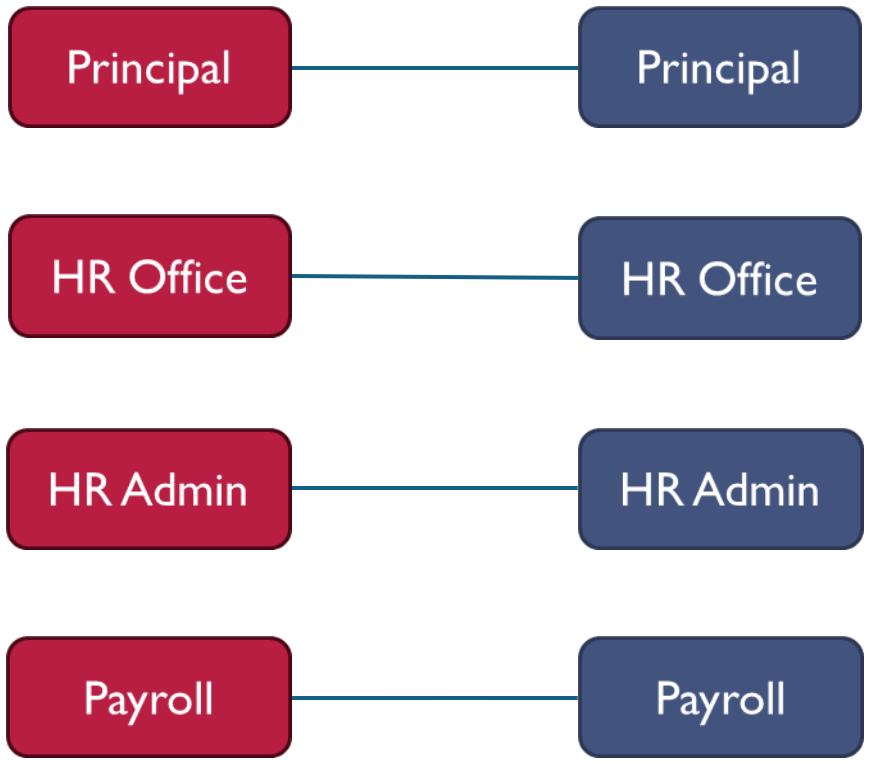
- Name of role is based on the activity is addresses.
- Assign this “task” to the groups that need to accomplish it.
- Pro: When new screens/reports/utilities become available there are a small number of roles to update.
- Con: Task roles may give broader access.

Role Setup Option – Task Based

Principal	HR Office	HR Admin
• Position View • Demographics View	• Position Edit • Demographics Edit • Employee Codes Edit	• Position View • Demographics Edit.

- Pro: With Tasks assigned to groups, it's easy to see what tasks those groups are performing.

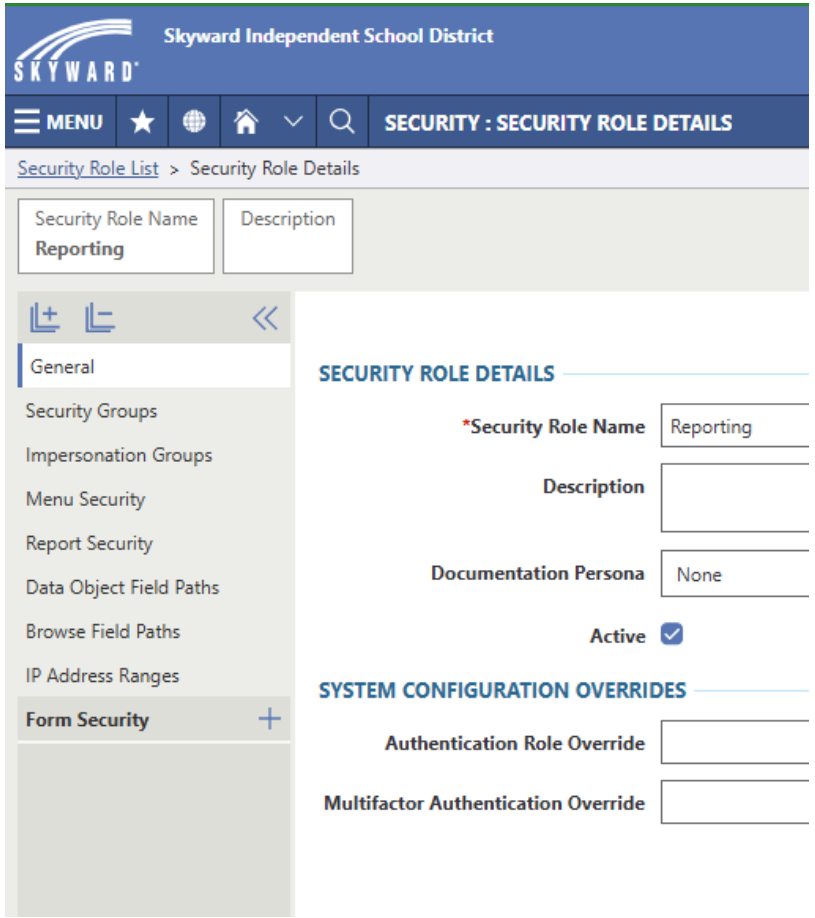
Role Setup Option – Position-Based



- Name of the role matches a position in your organization.
- Assign this role to the matching security group – usually 1:1 correlation.
- Pro: Access is tailored exactly to what that group needs.
- Cons:
  - When new screens/reports/utilities become available it is more work to figure out which roles need to be updated.
  - Hard to know what rights the group has access to by looking at roles.

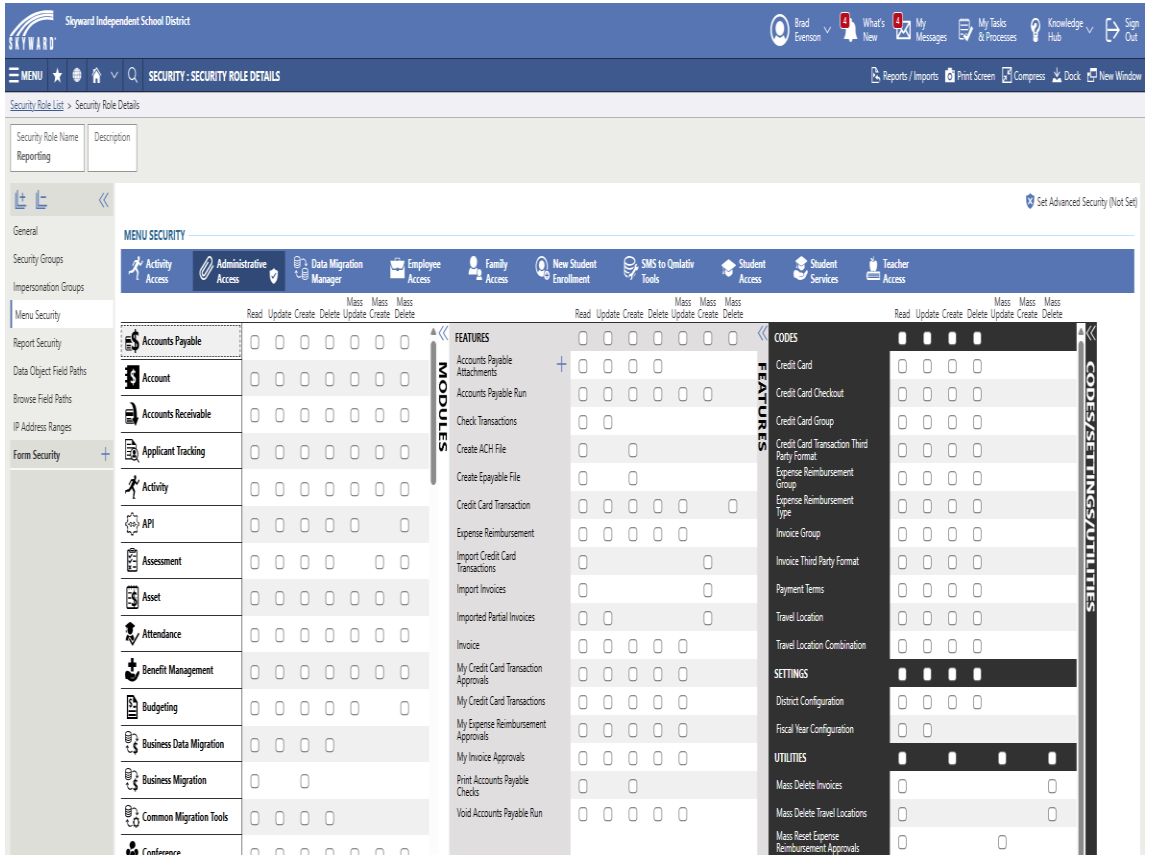
Security Roles

- **Security Group** – groups of users attached to this role.
- **Impersonation Group** – used to limit which security groups can be impersonated, if impersonation is also granted in menu security.
- **Menu Security** – screens, utilities and access level for each that will be applied.
- **Report Security** – reports that will be accessible.
- **Data Object Field Paths** – if you want to provide access to a field(s) that this group would not normally be able to access (ex: Social Security Number), add it here and it becomes available throughout the system.
- **Browse Field Paths** – similar to Data Object Field Path, but when adding a field here, you specify which browse screen the field is available on for more targeted access.
- **IP Address Ranges** – limits the IP addresses that the user must be connected to in order to access the items set in this role.
- **Form Security** – forms that will be accessible to this group.

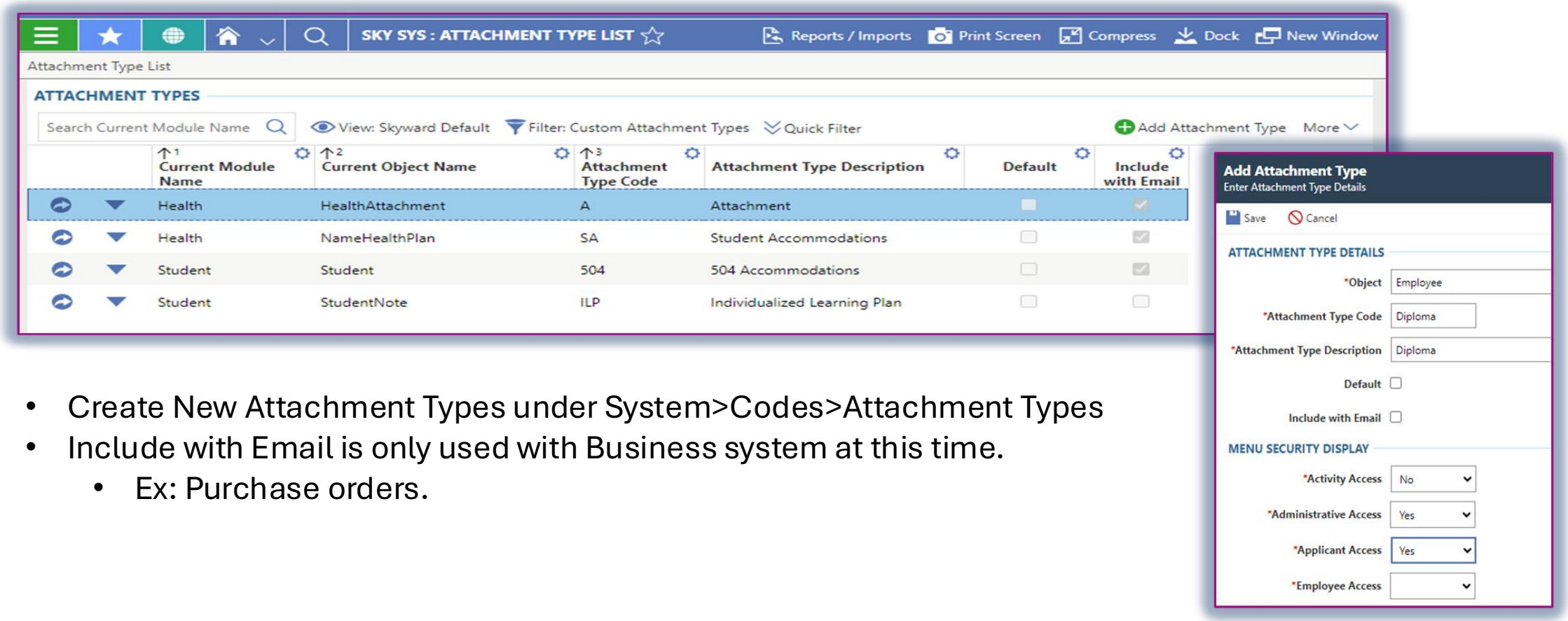


Security Roles – Menu Security

- **Security Group** – groups of users attached to this role.
- **Impersonation Group** – used to limit which security groups can be impersonated, if impersonation is also granted in menu security.
- **Menu Security** – screens, utilities and access level for each that will be applied.
- **Report Security** – reports that will be accessible.
- **Data Object Field Paths** – if you want to provide access to a field(s) that this group would not normally be able to access (ex: Social Security Number), add it here and it becomes available throughout the system.
- **Browse Field Paths** – similar to Data Object Field Path, but when adding a field here, you specify which browse screen the field is available on for more targeted access.
- **IP Address Ranges** – limits the IP addresses that the user must be connected to in order to access the items set in this role.
- **Form Security** – forms that will be accessible to this group.

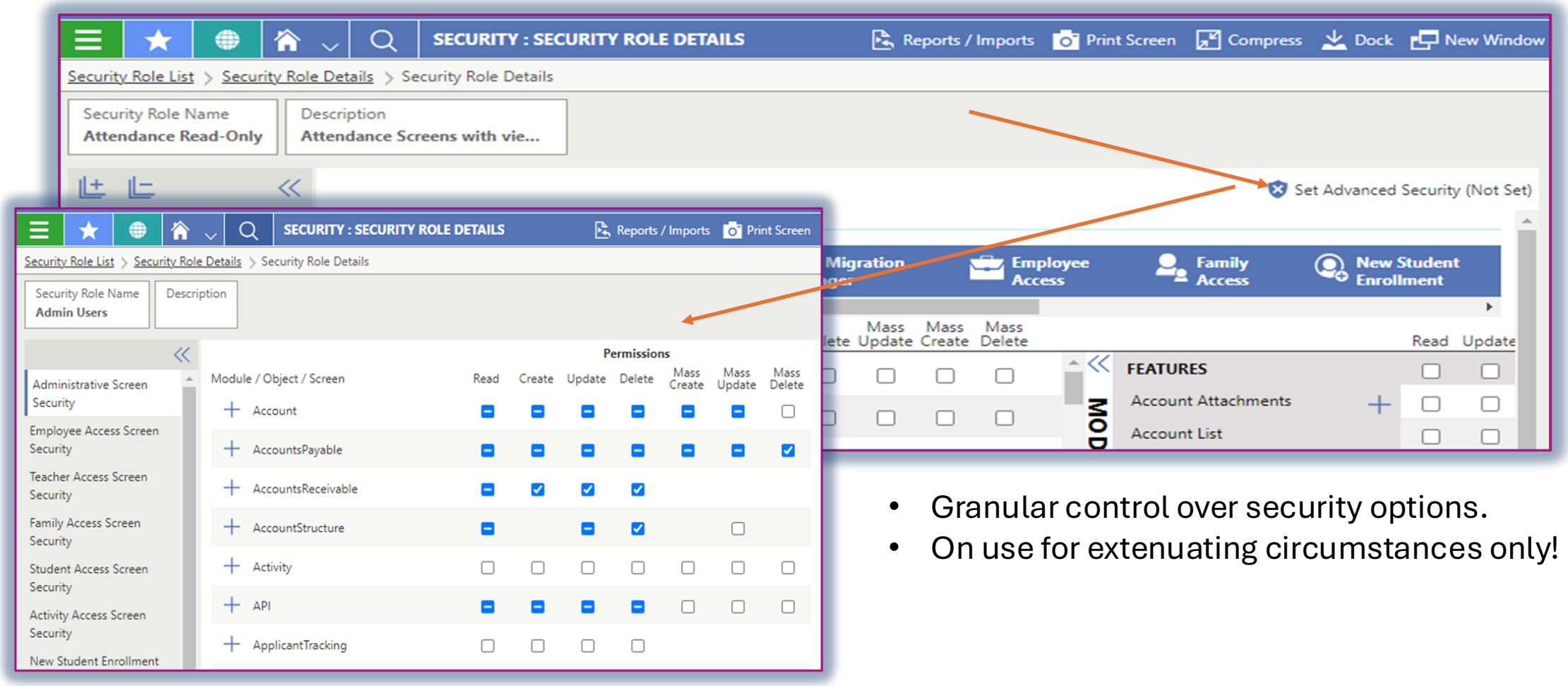


Security Roles – Attachment Type



- Create New Attachment Types under System>Codes>Attachment Types
- Include with Email is only used with Business system at this time.
  - Ex: Purchase orders.

Security Roles – Advanced Security



- Granular control over security options.
- On use for extenuating circumstances only!

Security Groups

Group Memberships – user and entity combination that is assigned to this group.

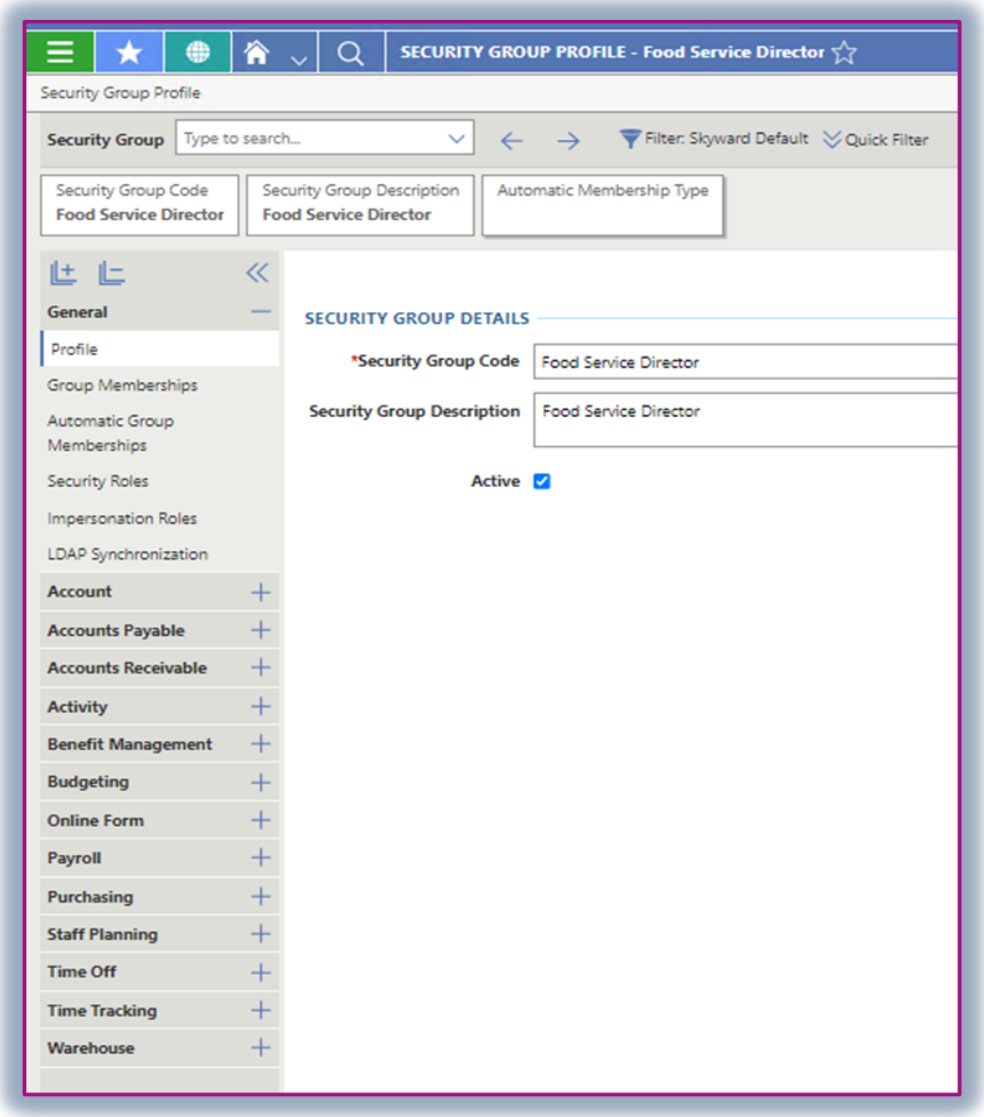
Automatic Group Memberships – can be used to auto-assign a user type (students, families, teachers) to this Security Group.

Security Roles – roles assigned to this group.

Impersonation Roles – used to limit which roles can be accessed when in impersonation mode, if impersonation is also granted in menu security..

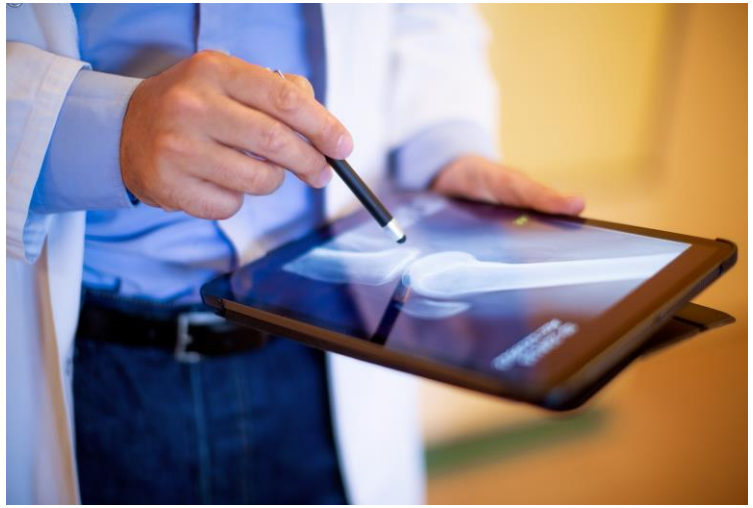
LDAP Synchronization – used to link an organization's LDAP group(s) to a Qmlativ security group so that as users are added or deleted from the LDAP group, those changes are made here also.

Specialty Access Groups – used to limit access to select records within each area.

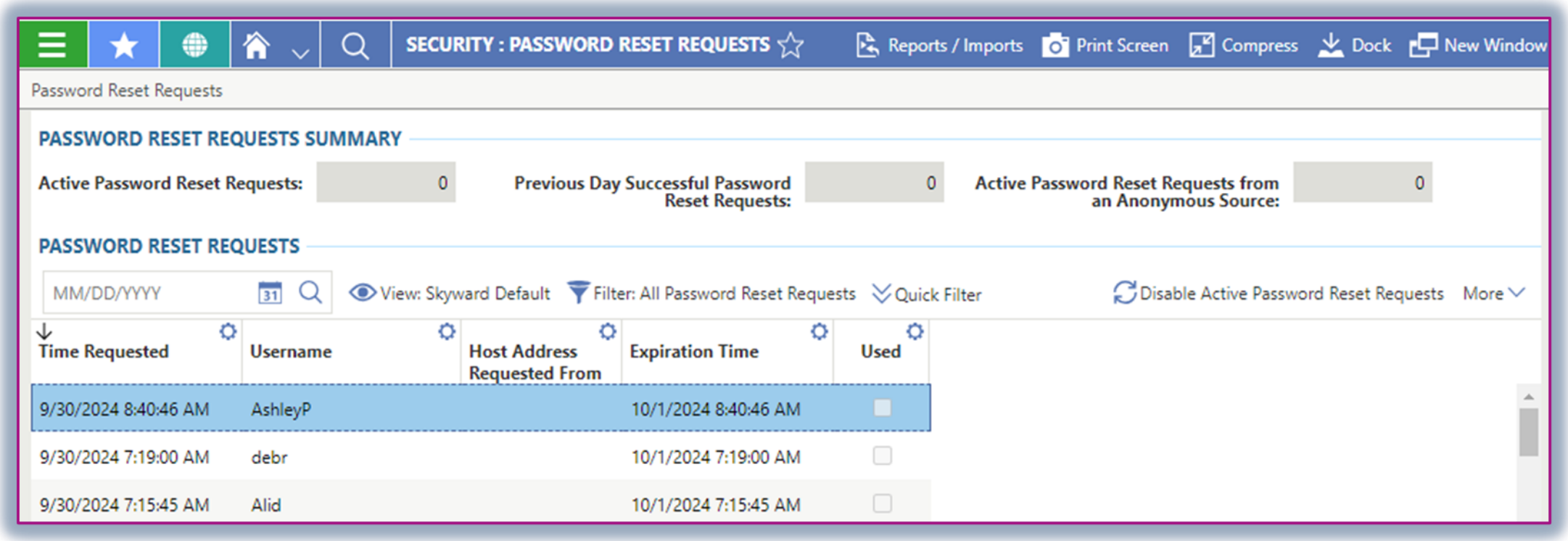


Security Reports

- Login and Usage History
  - List of users' login activities to help identify bad actor access attempts.
- Users without Security Groups
  - Identifies users that could potentially be activated due to not being a part of a Security Group anymore.
- Workflow and Report Activity
  - List of what was accessed by a select user within a date range.



Password Reset Request Summary



- Lists users that have requested the “Reset my Password” link.
- Helps in identifying potential bad actor access attemps.

Utilities

- **Security Audit**
  - Gives a report of the current system settings.
  - Items that do not align with Skyward's best practices will be highlighted in Yellow or Red.
- **Security Import/Export**
  - Utilities used to transfer Security Groups and Roles from one environment to another.
  - Import completely overwrites any setup in the target environment.
  - Can include the Security Group Membership records.



Utilities



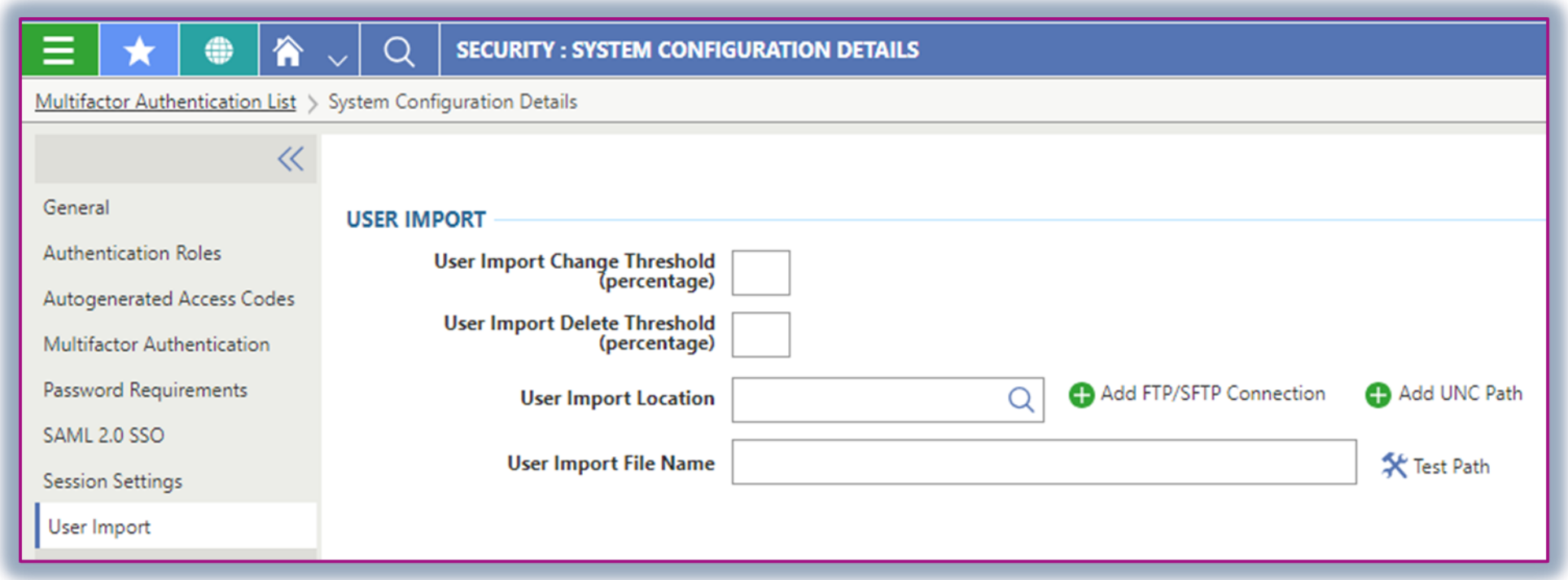
- **Staff External Sync**
  - Update staff records that are exported from an external Human Resources or other third-party source.
  - Auto-assigns/unassigns security groups.
  - Uses External Unique Identifier (EUI) field on the Name record to match records.
  - Source file is a complete list of staff regardless of whether changes are needed.

This Photo by Unknown Author is licensed under CC BY-SA

Utilities

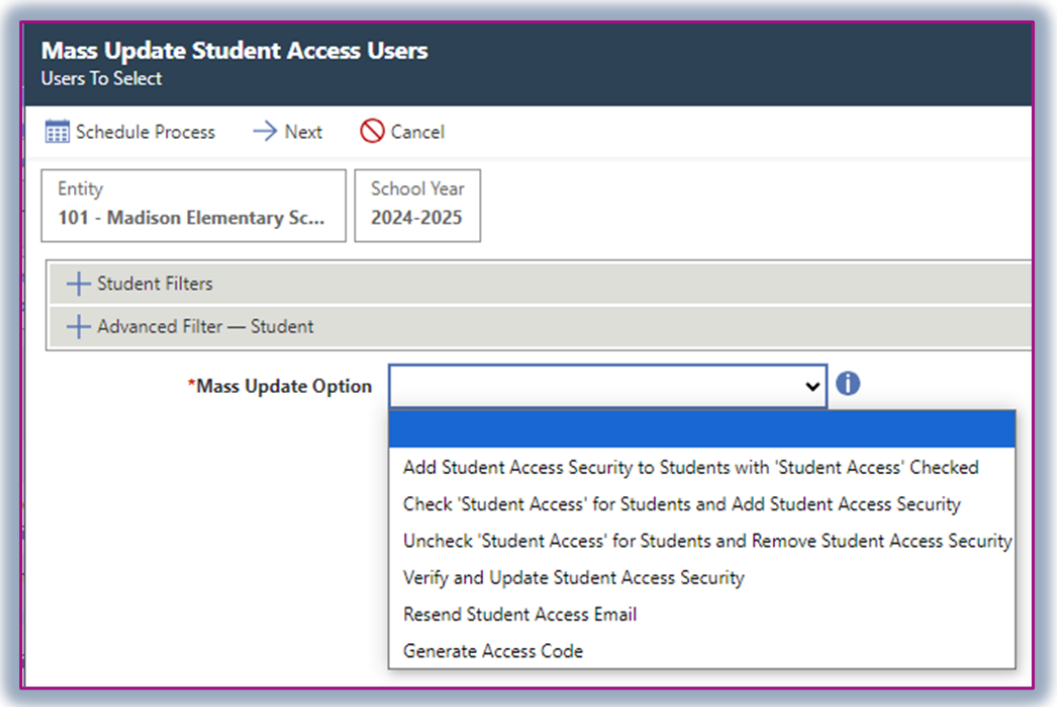


- **User Import**
  - Utility to mass create or update secured user information
  - May also be used to mass create staff and staff entity records.



This Photo by Unknown Author is licensed under CC BY-SA

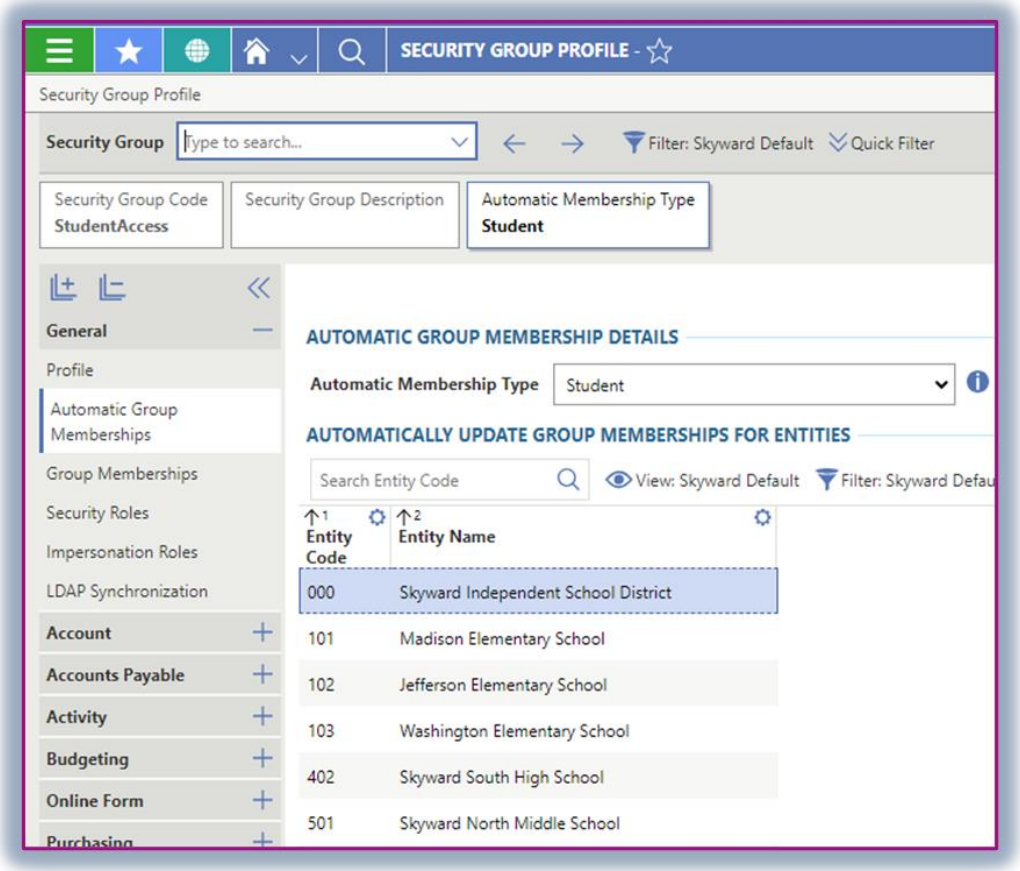
Mass Update Utilities



- Activity, Employee, Family, Staff, and Student user types.
- Used in conjunction with the User Type on a Security Group to auto-assign users of the selected type to the security group.
- Typically set up as a scheduled task so it is updated regularly.

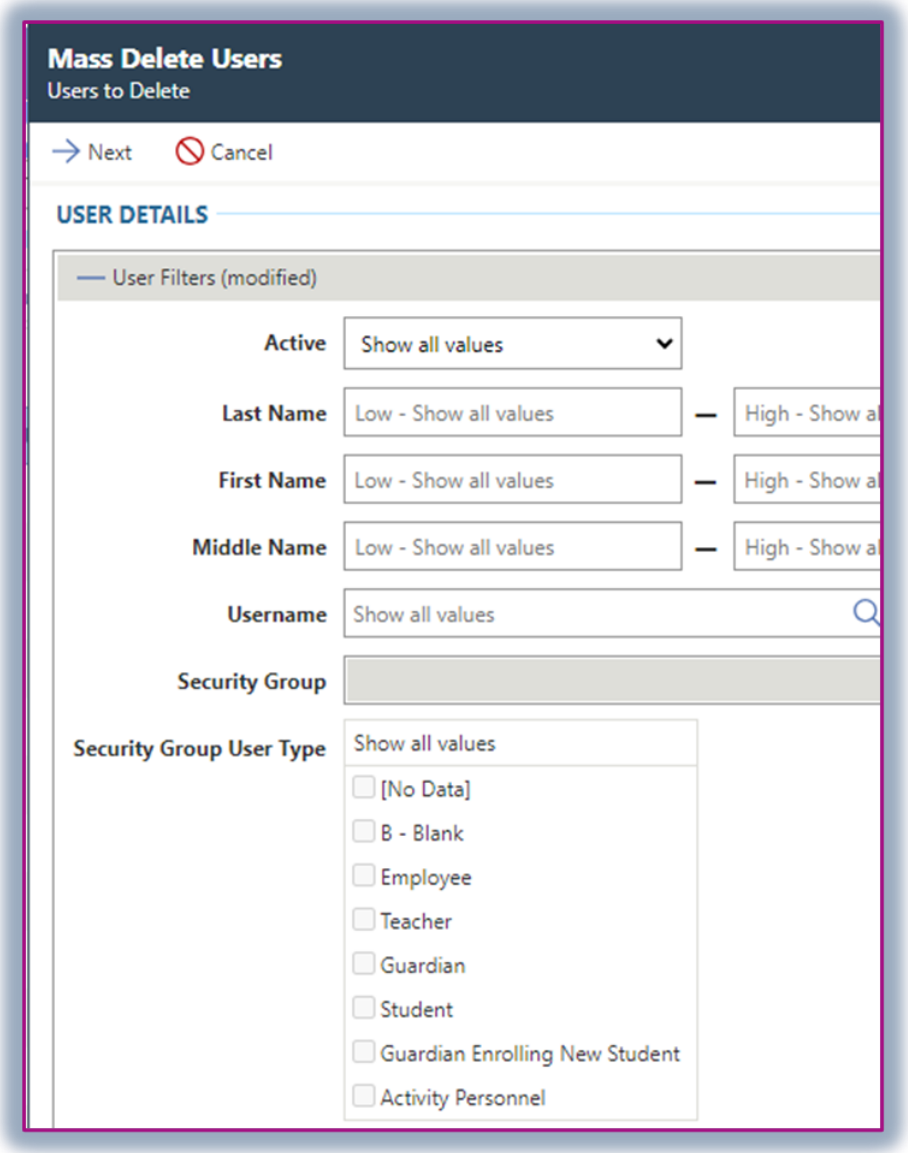
Automatic Group Memberships

- Auto-Assign users of the selected types to the Security Group.
- Used best in conjustion with the Mass Update Utilities in the Security Module.

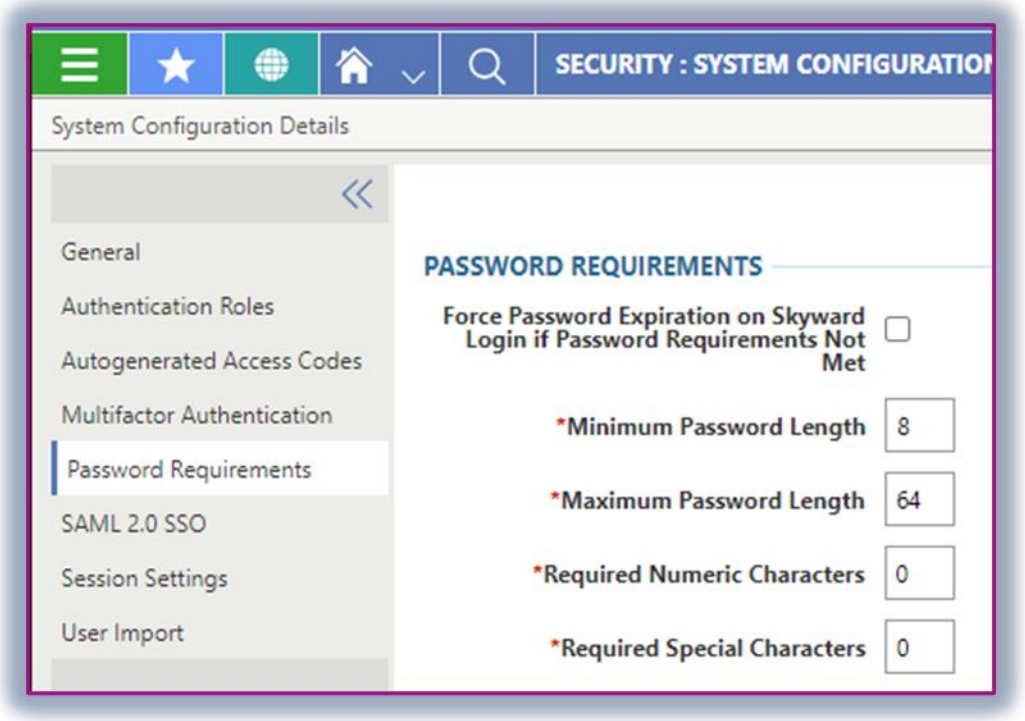


Mass Delete Users

- Clean-up utility to remove user records when the user is no longer assigned to a security group.

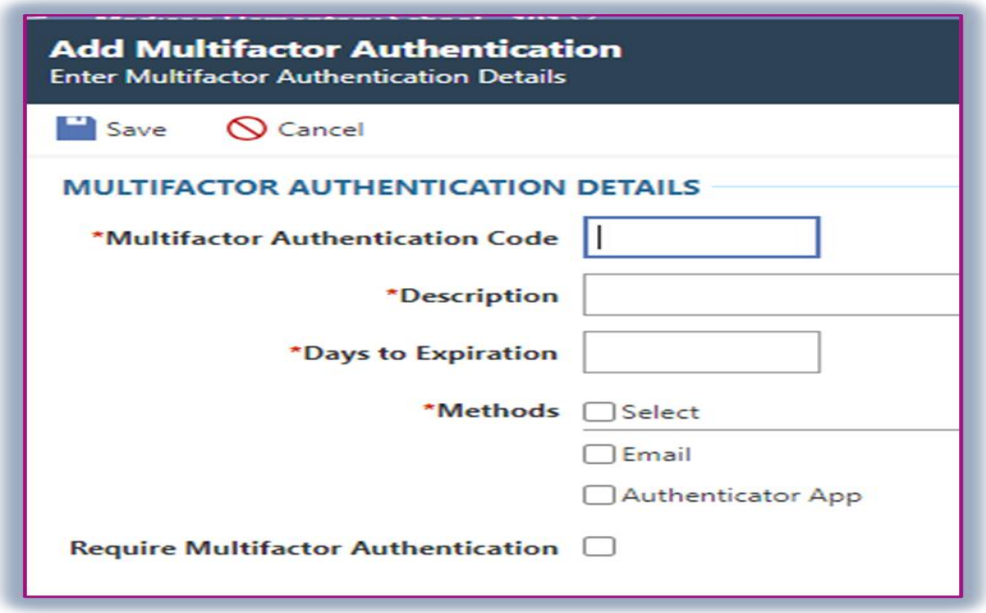


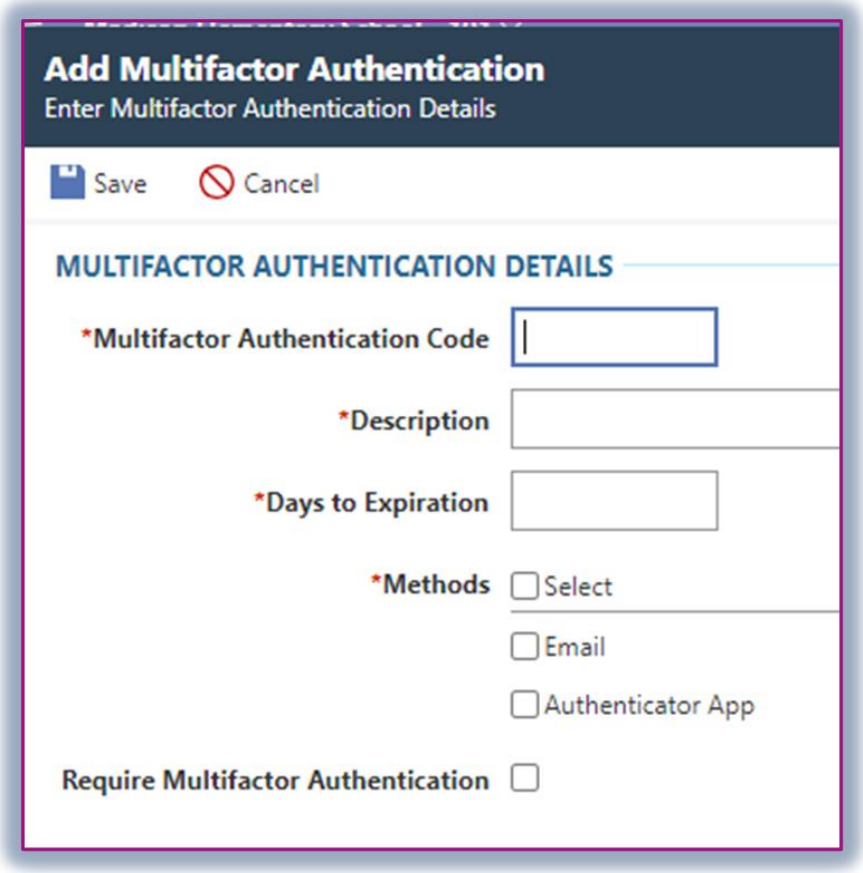
Password Requirements



- Recent NIST Proposal Highlights
  - Min of 8 Characters, but 15 ideal.
  - Max of 64 Characters
  - NO requirement for periodic changes unless compromise is suspected
  - NO requirement to have a mixture of character types
  - Hints and security questions are no longer acceptable
  - Find Proposal here.

Native Multi-Factor Authentication (MFA)

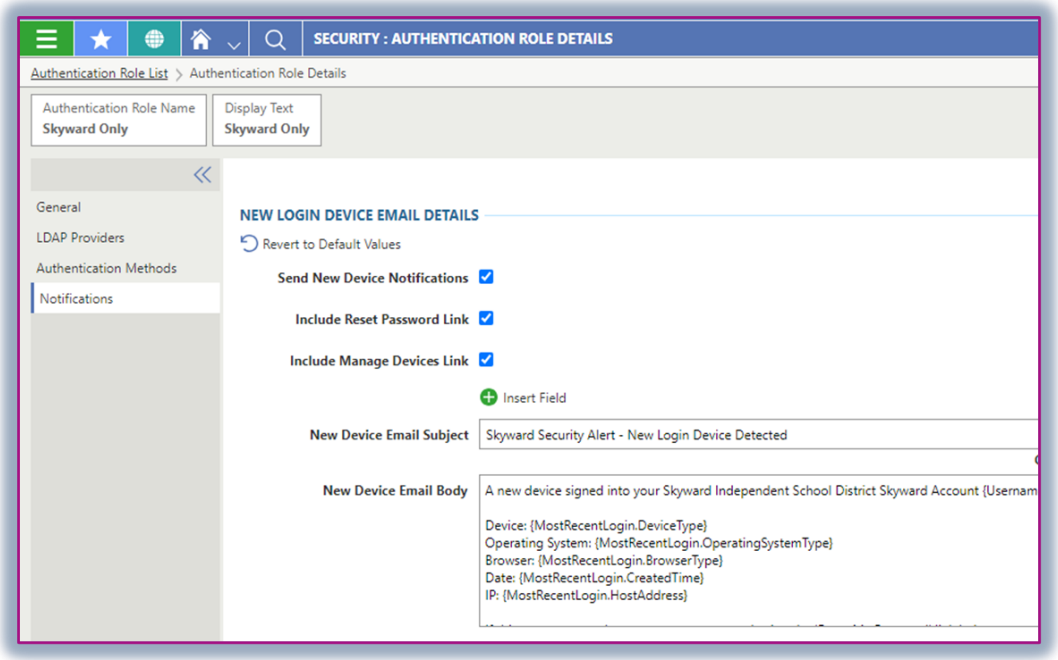




- **Set MFA by User Type**
  - Most restrictive takes precedence
  - Email or Authenticator app options.
  - Override at the role or user level.

Security Notifications

- **Set on select Authetication Types**
  - New Device Login
  - Password Change
  - Account Locked



Impersonation

- **Known in SMS 2.0 as “Super User Access”**
  - Allows a user with these rights to log in as another user.
  - Can be limited to designated Entities, Security Groups, And Roles.
  - Does NOT log the impersonated user out of the system.

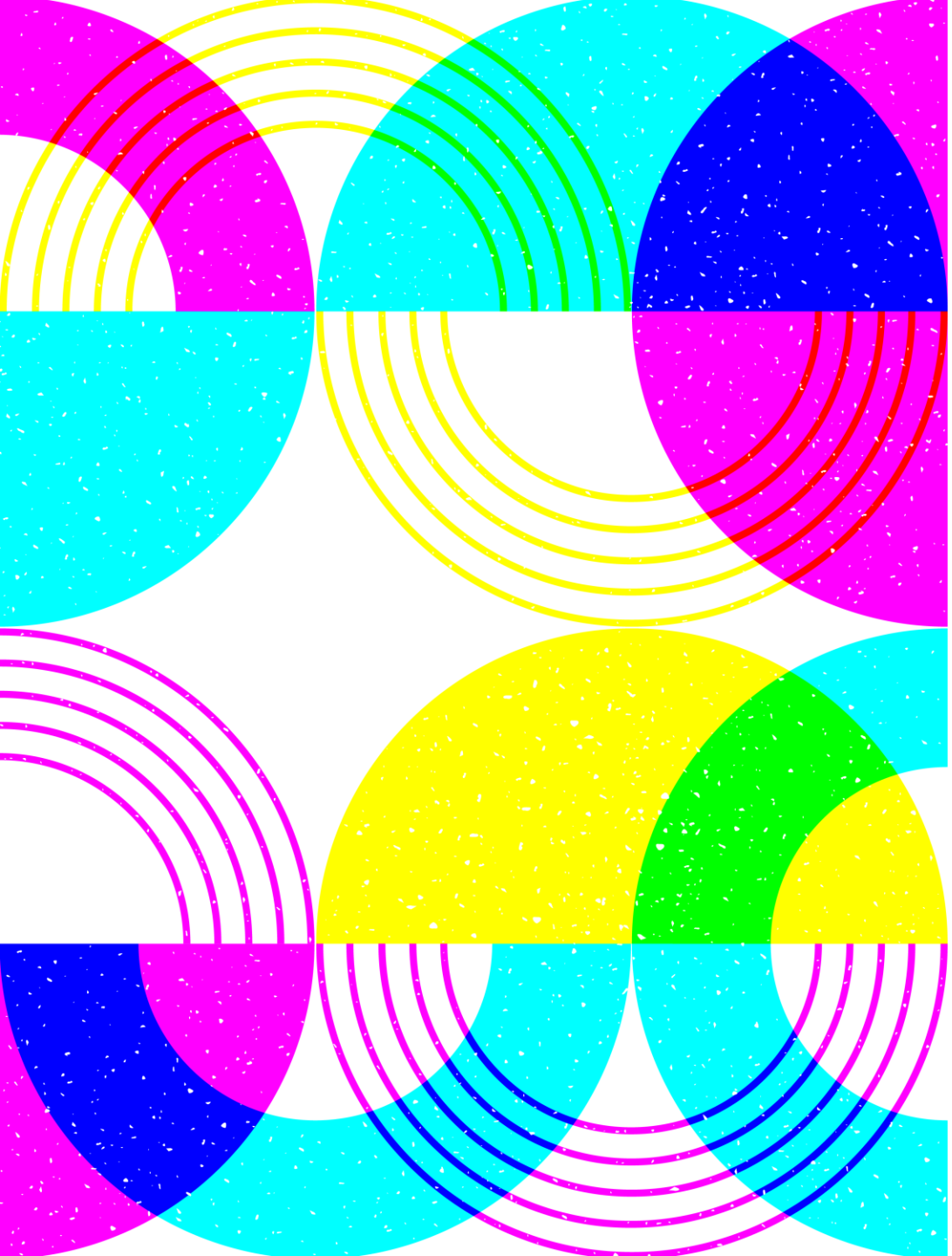


Future Enhancements



- Guardian Password Reset outside of Security (recently started).
- Support for Hardware Tokens for MFA.
- Require MFA for Superusers and users with access to Sensitive Data.
- Impersonating users while maintaining own session.

Q & A



SKYWARD®

iCON

thank you!