HARRIS School Solutions

Nextgen Security

Nextgen Best Practices & Hosting
February 2021

It All Begins with your Password!

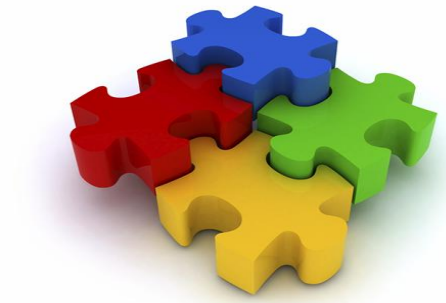
- Make it unique (not 12345) and complex
- Don’t share it with your co-workers
- Don’t write it down and keep it in your drawer
- Your Nextgen password not stored in the database only in Active Directory on your server
- ESS – Uses Two-Factor Authentication when registering
  - Some Demographic changes require additional authentication

Security Features in Nextgen

Menu Security/Transaction (User or Group)

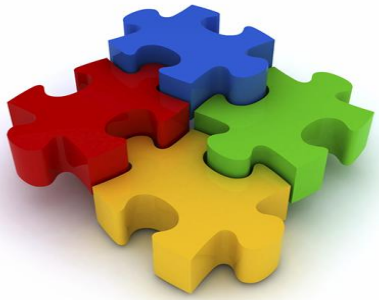
- The menu can be initialized with only those applications/transactions the user is allowed to process thus if an application/transaction is not on a user's menu, they cannot access that application/transaction. Menus can be customized per User or Group.
- Transaction Security is set within menu maintenance on specific transactions for a user and/or group.
  - Example – Inquire Only on Journal Entry Query to prevent reversing journal entries.

Component Level Security



- Component security in the Nextgen system can be set at the component level. Any value of any component can be designated as valid for each user. Component level security is enabled in the GL Parameter Maintenance transaction. This is a global On/Off switch. Once component level security is turned 'On', it must be set for each user that should not access all components and their values.
- If a user or group has access to ALL components, then Component Level Security SHOULD NOT be set for that user/group.
- Component Level Security can be turned On/Off for Input and for Reporting.

Component Level Security



- Component Level Security Maintenance is by default located in the General Ledger application in the GL Table Maintenance folder. Component Level Security can be set per application for users and/or user groups.

- Component Level Security can be set per application for users and/or user groups. If a user or group has access to ALL components, then Component Level Security SHOULD NOT be set for that user/group.

- Since all users have to access Balance Sheet Accounts due to automatic postings, then ALL users must be assigned access to the Component Value zero for all components with that value.
  - For example, when a purchase order is approved and Saved, a posting is made to the general ledger to the encumbrance account. That encumbrance account has a '000' value for the Object code as well as other components. Because of this type of posting, all users with component level security will need to be assigned the '000' Object code as well as any other components with zero values.

User Level Security

- User Parameters – user parameters are set in the User/Group ID Maintenance transaction. There are parameters that can be set for each application (see User documentation).
  - Examples
    - Can User Exceed Budget?
    - Can User Add General Ledger Accounts?
    - Can User Create Vendors?
      - Can User Modify/Delete Vendors?
    - Maximum PO Dollar Amount

Access Level Security

- Access level security is set per application NOT transaction, per user or group. Access Level Security is turned on in Installation ID Maintenance and is set for users/groups in User ID Maintenance. Access Level Security is divided into 6 levels. They are:
  - 10 - Inquiry/Print – No Financial Data
  - 20 - Inquiry/Print – Financial Data
  - 30 – Entry/Maintenance
  - 40 – Transfer/Merge, etc.
  - 80 – Support File Maintenance
  - 99 – Unlimited Package Access

Ownership Groups

- Ownership groups are created and tied to specific applications. Documents such as Receipts, Requisitions, Purchase Orders, etc., can be assigned to an ownership group. Ownership groups allow documents to be in effect ‘owned’ by a group. When a document has been assigned to an ownership group, that document can only be maintained/changed by a member of that group.

Nextgen Hosting

Nextgen / ESS in the Cloud!

- Your data resides in our state of the art datacenter, and is accessed through your web browser
- The application and database run from Harris' cloud servers

Nextgen Hosting

- Why hosting?
  - Security, Security, Security!
    - State of the art, secure datacenter
    - Encrypted traffic from client to servers
      - SSL / https:
    - No direct access to SQL server / Nextgen databases
    - Forced password restrictions
      - Length
      - Complexity
      - Periodic Changes
    - Account Lockouts
      - Prevent brute force attacks
    - Network threat mitigation
      - i.e. DDoS attacks

Nextgen Hosting

- Why hosting?
  - Access from anywhere
    - Mobile Hotspot / MiFi
    - Work from home / hotel / conference
    - Mobile Device Support
    - Windows / Mac
  - Disaster Recovery
    - Natural Disasters
    - Warmsite option for self hosted clients
  - We handle all backups
    - Automated, Managed and Monitored Backups
      - 3 levels of backup
        - 7 days local server storage
        - 14 days – datacenter backup – offsite
        - 28 days – Gemini offsite

Nextgen Hosting

- Why hosting?
  - We manage all Microsoft Licensing
    - Windows Server
    - SQL Server
    - Client access licenses
  - Minimal assistance required from district technology departments
    - Most technology departments encourage moving to cloud based solutions
  - Auditors love it!
    - Datacenter features
    - Physical Security Controls
    - Password Policies