Set up security roles

Updated: June 2018

To access the Banking module, users must be assigned with the proper security roles. The Banking module includes independent security roles, which grant users access to different facilities and functionalities within the Banking module.

Security roles are configured and assigned in standard AX/D365 and is already well described elsewhere. This guide will instead focus on describing the Banking security roles and how these roles can be assigned and combined

Assigning security roles

For more info on role-based security and assignment of security roles, please see:

https://technet.microsoft.com/en-us/library/gg731787.aspx

https://docs.microsoft.com/en-us/dynamics365/unified-operations/dev-itpro/sysadmin/role-based-security

Security roles in Banking

All security roles in Banking have been constructed as stand-alone roles. This means, that assigning a single security role, is sufficient to complete the tasks related to that specific security role. E.g. the payment approvers can enter payment journals, in need of approval, without having additional payment clerk privileges.

The security roles in Banking are:

- AMC Banking demo supervisor: Assigned to users responsible for creating and importing demo return files, thereby allowing simulation of live bank responses.
  !!! This role is solely designed for demo purposes and should therefore never be assigned in live production environments

- **AMC Banking payment approver:** Assigned to users responsible for approving payment journals/batches prior to transferring payments to the bank.

- **AMC Banking payment clerk:** Assigned to users responsible for creating and executing payments. The payment clerk has full access rights to payment journal related data

- **AMC Banking posting clerk:** Assigned to users responsible for posting and settling imported customer and vendor payment notifications and handling of recurring bank transactions like fees and interests. The posting clerk has full access rights to posting journal related data

- **AMC Banking reconcile clerk:** Assigned to users responsible for reconciling imported bank account statements against ledger and bank accounts in the system.

- **AMC Banking manager:** Assigned to users responsible for maintaining customer and vendor bank accounts. This role also grants view access throughout the module, allowing the manager to supervise the daily tasks, that are maintained by the clerks.

- **AMC Banking setup manager:** Assigned to users responsible for maintaining the core setup in the Banking module, which is often static and not very likely to change, once it has been configured during the initial project phases.

- **AMC Banking workflow approver:** Assigned to users responsible for approving pending payee bank accounts. This role is only used in environments, where the payee bank account approval workflow is enabled and is in use.

Please note, that the security roles in Banking solely grants privileges within the Banking module. In most cases, Banking users must therefore also be assigned one or more standard AX/D365 security roles, to access standard AX data. An **AMC Banking payment clerk** might require an additional **Accounts payable payments clerk** role, an **AMC Banking posting clerk** might require an additional **Accounts receivable payments clerk** role, the **AMC Banking manager** an additional **Accountant Supervisor** role etc.

Please also note, that due to the AX/D365 system architecture, printing of reports requires additional external rights. Relevant users, must be assigned proper rights on the external Reporting Server, which is done externally on the Reporting Server itself.

Security role assignment examples

The role assignment examples below are meant as inspiration, and is therefore provided "AS-IS". User role assignments should always be carefully tailored to the individual organizations and the individual user responsibilities.

- The "Superuser":
  Bundle the three AMC Banking clerk roles with the **AMC Banking manager** security roles, and you will end up with a role assignment, that is very similar to the **AMC Banking user** role, known from earlier versions of Banking. This user can both view and maintain most data throughout the Banking module.

  This role assignment offers a very seamless daily use of the Banking module, as restrictions are almost non-existent, but since this role assignment offers both access to maintaining bank accounts, as well as payment execution, it also increases the risk of fraud.

  To counter the increased fraud risk, this role assignment should be combined with usage of the included payee bank account approval workflow. This workflow ensures that a supervisor, which has been granted workflow approval privileges, must approve payee bank account changes, which prevents the super user from singlehandedly creating or changing bank accounts. For more info, see separate **Activate bank account approval workflow** document

- The Controller and the Accountant – "Segregation of duties":
  In this scenario, one or more accountants maintain the daily tasks via the relevant clerk roles, while the controller via the manager role, less frequently maintains payee bank accounts. In addition, having the proper view privileges throughout the module, allows the controller to supervise and assist the daily clerk tasks

The clerk and manager security roles have been carefully designed to offer segregation of duties. This is very important, especially in relation to the payment clerk role, where segregation of duties is crucial to preventing fraud.

The **AMC Banking payment clerk** role can successfully be bundled with the standard role **Accounts payable payments clerk**. This allows the payment clerk to maintain the daily payment processes and view bank accounts and other vendor payment related information in both standard AX and the Banking module, but at the same time it restricts the payment clerk from creating and modifying payment information.