AccountMate®
SOFTWARE THAT FITS

Article # 1213

Technical Note: Effectively Utilizing the AccountMate Security Features

Difficulty Level: Beginner Level AccountMate User

Version(s) Affected: AccountMate 12 for SQL and Express
AccountMate 11 for SQL and Express
AccountMate 10 for SQL, Express, and LAN
AccountMate 9 for SQL, Express, and LAN
AccountMate 8 for LAN

Module(s) Affected: SM

Posting Date: 04/07/2021

DESCRIPTION

AccountMate provides tight security features to address growing concerns of fraud. Understanding these security features enables you to effectively utilize them. This document discusses the security features available in AccountMate. Once you become familiar with these features, you can then design your own security procedures by mixing and matching the available features for improved security and privacy.

SOLUTION

Below is a list of the AccountMate security features:

- **Group/User Access Rights**

  It is always prudent to set up the appropriate Group and User access rights to ensure that sensitive information does not fall in the wrong hands. Information leakage may cost the company thousands of dollars; it could even cost the company its very existence.

  For greater administrative control over sensitive data, you can do the following:

  - Set up Group and User access rights to functions and features
  - Restrict user logins by day and time
  - Track User access
  - Require password change at next login
  - Disallow changing of passwords
  - Disallow multiple logins per User
  - Lock out a User account(s)
  - Disable a User account(s)

You can use any of the following functions to view the security settings you have set up:

- **View Function Access Rights**
- **View Extended Rights**
- **Function Access Rights Listing**
- **Extended Rights Listing**
- **Locked-out User Listing**

You will find these features in the AccountMate Administrator Program > **Setup** menu > **Security** option.

- **Password Policy**

  After you have set up the appropriate access rights, it is equally important to assure that these access rights are not violated. This is where the password comes into play. It is important to develop a strict password policy so that passwords cannot be easily deciphered. AccountMate supports secure password policy for Sarbanes-Oxley compliance.

  - Password complexity

    AccountMate provides a number of options that you can use to set up the parameters for your password structure. You can set up the following parameters to facilitate complex user passwords:

    - Minimum password length
    - Minimum number of letters
    - Minimum number of lower-case letters
    - Minimum number of upper-case letters
    - Minimum number of digits
    - Minimum number of punctuation and other characters
    - Cannot be the same as the User Name
    - Cannot contain the User Name
    - Cannot be the same as the User Full Name

  - Password expiration
  - Disallow reuse of old password
  - Lock out a user after a specific number of failed login attempts
  - Require password change at next login
  - Disallow changing of passwords

  You can set up the above parameters in the AccountMate Administrator program > **Setup** menu **> Security > Password Policy** function.

- **Other Security Features**

  Aside from administrative control over Group and User access rights and password policy, additional security features are available at both the transaction and maintenance levels. These security features include the following:

- Credit card encryption

  The customers' credit card numbers are encrypted before they are saved in the database and decrypted before they are displayed on the AccountMate screen. This helps to protect your customers from unauthorized and fraudulent use of their credit card information.

- User-defined mask and/or user access right for printing vendor's Federal Employer Identification Number (FEIN) or vendors'/employees' Social Security Number (SSN)

  You can grant access rights to users in order to view the vendor's complete federal employer identification number and the vendors' or employees' complete SSN on check stubs and other reports; otherwise, only the last four (4) digits of the SSN will be shown and the rest will be encrypted. This helps to protect your employees from unauthorized and fraudulent use of their FEIN and SSN information.

- Positive Pay file generation for fraud protection

  You can transmit to banks a positive pay file and arrange with your bank to honor only those checks listed in the positive pay file. This feature helps to protect your company against check fraud and improves cash management due to a security-enhanced environment.

- User Access Log

  If you want AccountMate to automatically keep a log of the date and time when the user accesses and exits a company and function in AccountMate, mark the **User Access Log** checkbox in the **Group/User Setup > Add User/Edit User** window. Click the **View** button in the **Add User/Edit User** window to view the **User Access Log.**

- Company Access Lock *(available only in AM for SQL/Express versions)*

  This feature allows you to lock the company to prevent other users from accessing or logging into it. This may be necessary when performing functions that require exclusive company access including period-end closing, year-end closing, the addition or editing of custom fields, installation of product updates, etc.

- Audit Trail *(available only in AM for SQL/Express versions)*

  Using the **Audit Trail** function, you can set up the parameters to track data changes entered in the main AccountMate program. This feature is configurable to give you the flexibility to select the critical data that must be tracked. You can review the audit trail settings and transactions for each company by generating the **Audit Trail Setup Listing** and **Audit Trail Transaction Log**. This feature helps strengthen the company's internal controls and facilitates compliance with the Sarbanes-Oxley Act.

- System Audit Trail *(available only in AM for SQL/Express versions)*

  Using the **System Audit Trail Setup** function, you can set up the parameters to track each user who accesses certain functions in the AccountMate Administrator program and to track the date when each function was last accessed. This feature provides the flexibility to select the functions, tables, and fields from which you choose the records that must be tracked. You can review the system audit trail settings and records for each Administrator function by generating the **System Audit Trail Setup Listing** and **System Audit Log**. If necessary, you can also delete the audit trail settings for a particular Administrator function using the **Purge System Audit Log** function. Similar to the Audit Trail feature, the System Audit Trail feature helps strengthen the company's internal controls and facilitates compliance with the Sarbanes-Oxley Act.

- Customizable Database Connection Password *(available in AM11.2 for SQL/Express and higher versions)*

  AccountMate provides the flexibility of customizing the AMLOGIN password. The **Database Connection** function requires the System Administrator login and password for added security.

AccountMate has powerful security settings. These security features are ready for your use; thus, we highly recommend that you examine each of these features and find ways to make use of these features in ways that can be of the best benefit to your organization.

This information is provided "AS IS" without warranty of any kind. AccountMate Software Corporation disclaims all warranties, either express or implied. In no event shall AccountMate Software Corporation be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits, or special damages, even if AccountMate Software Corporation has been advised of the possibility of such damages.