Enhanced Security Sage 300

How we protect your credentials and maintain the integrity and continuity of critical systems

Sage

acute data

Sage and Sage 300's credential security and governance work to keep your system safe and reliable.

We've written this document to explain Sage 300's enhanced security, to provide step-by-step instructions for migrating to the enhanced security version of Sage 300, and to convey in-progress and future enhancements.

All customers should follow appropriate security precautions, such as setting up a firewall, employing strong passwords, ensuring appropriate physical security, and having appropriate security policies and procedures.

Overview **5**

What's New **6**

Prerequisites **8**

Upgrading from a previous version that already has this security enhancement 8

Overview 9

Sage 300 Database Setup Screen 9

Sage 300 User Security 12

Appendix **22**

Known Issues 22

Overview

The security of our products and customers is a top priority for Sage. Historically, Sage 300 has stored encrypted user credentials on the file system in ISM files. This mechanism has served Sage 300 well throughout its past. However, with today's modern architectures, technologies, and implementations, there are better and safer storage options available.

While accessing, reading, and decrypting information in these ISM files requires specific access and sophisticated knowledge, this type of access with mischievous intent will be eliminated with this enhancement.

What's New

Sage 300, both the Desktop and the Web Screens, starting with version Sage 300 2023.2 in a controlled release (April 2023) and Sage 300 2024.0 will feature a security enhancement which eliminates certain ISM files in our Shared Data folder which contain Sage 300 user and database credentials. This content will be moved into a new database which we refer to as the Vault.

Moving this content into the Vault is the high-level concept. In this process, we are:

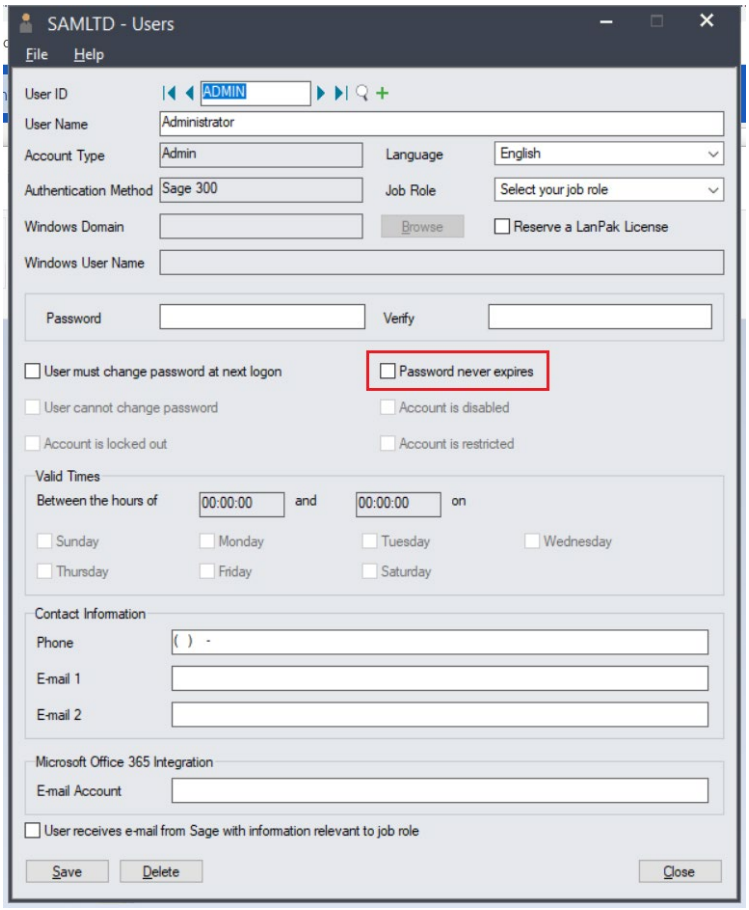
- Removing some ISM files from the file system and therefore eliminating any associated threat vector
- Leveraging MS SQL Server's authentication features to directly authenticate Sage 300 user credentials.
- Eliminating the storage of Sage 300 user credentials on the file system (in ISM files or any other forms).

Sage 300 can no longer retrieve or provide Sage 300 credentials (password) via an API since it is now leveraging MS SQL Server's authentication. Sage 300 is no longer in control of the storage of these credentials.

- Eliminating numerous security configurations and features in Sage 300 as they are now administered by not only MS SQL Server but also local machine policies (password exipration, number of retries, system lockout, etc.).
- Security for Sage 300 is always on
    - In previous versions, there has been an option to "Enable security" in the Database Setup screen which gave the user the ability to not require a password when accessing Sage 300. This option has been removed and a password (when not using Windows Authentication) will always be required.
- Complex passwords will be required
    - In previous versions, there has been an option to specify whether simple or complex passwords are required. This option has been removed and complex passwords with a minimal length of 8 characters, with a minimum of 1 lowercase character, 1 uppercase character, 1 numeric character, and 1 special character will now be required.
- Keeping high-level integration points or access points intact and only changing downstream behavior as it relates to where and how credentials are validated.
- The Global Search feature is available in the 2024.0 release. This feature was not available in product updates 2023.2 or 2023.3. Note that you must sign into Database Setup on each Sage 300 server machine using Global Search. (Refer to the Sage 300 Database Setup

Screen section)

- The user setting Password never expires is available in the 2024.0 release. This feature was not available in product updates 2023.2 or 2023.3.



Prerequisites

The enhanced security for Sage 300 requires specific changes and configurations to be made as well as an awareness of either deprecated features or delayed features. Please review the following items before proceeding with the migration from a version of Sage 300 that does not have this security enhancement to this version.

- Back up your Site folder within the Shared Data folder.
- Understand that the migration process will create two new MS SQL databases (Vault and Store).
- Get accustomed to security always being on, meaning that unless Windows Authentication is used, a complex password will be required.
    - See previous section for the characteristics of a complex password.
- Ensure that the Minimum Password age is set to 0 (Refer to the How to set the Minimum Password Age section).
- Be aware that the security enhancement is not compatible with Sage Partner Cloud at this time.
- Verify that any third-party products that you integrate with Sage 300 are compatible with the Sage 300 security enhancement, if applicable.

Upgrading from a previous version that already has this security enhancement

Upgrading from a version with this security enhancement to a future version does not require the steps involved in this migration section as the new databases are already in place.

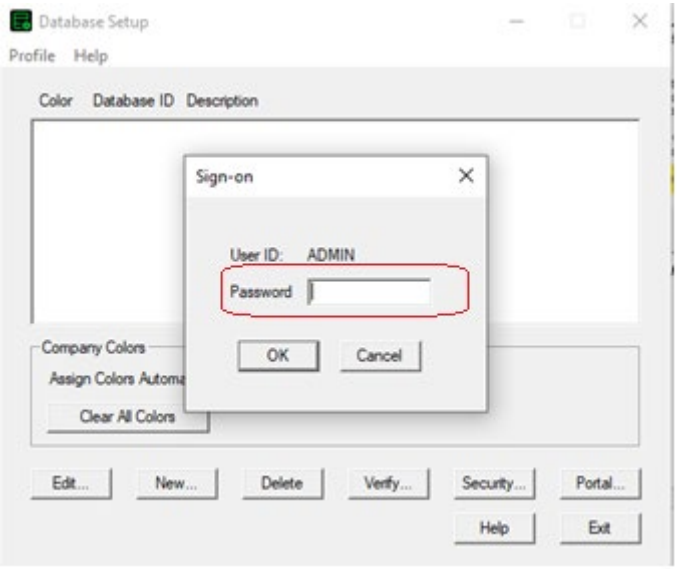
Overview

The elimination of specific ISM files from the file system will be handled by the upgrade or installation processes.

Sage 300 Database Setup Screen

Run the Sage 300 Database Setup screen from the server's Start menu – Sage 300 – Sage 300 Admin Utilities and enter the ADMIN password.

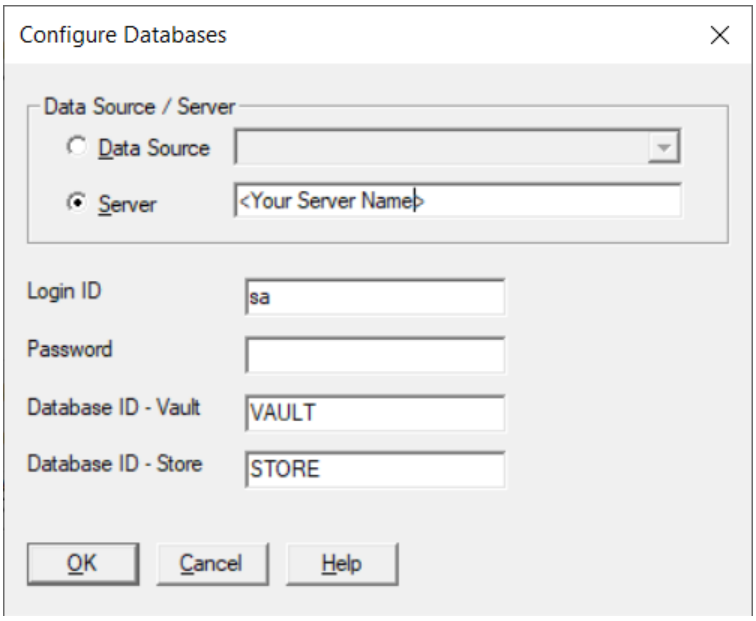
If Sage 300 is run before running the Database Setup screen, a dialog stating, "No supported databases are set up." is shown.



Sage 300 Database Setup screen

1. Configuring the Vault and Store databases

After logging into the Database Setup, the ***Configure Databases*** screen will be displayed:



Configure Databases screen

This is the screen where the information about the Vault and Store databases is entered:

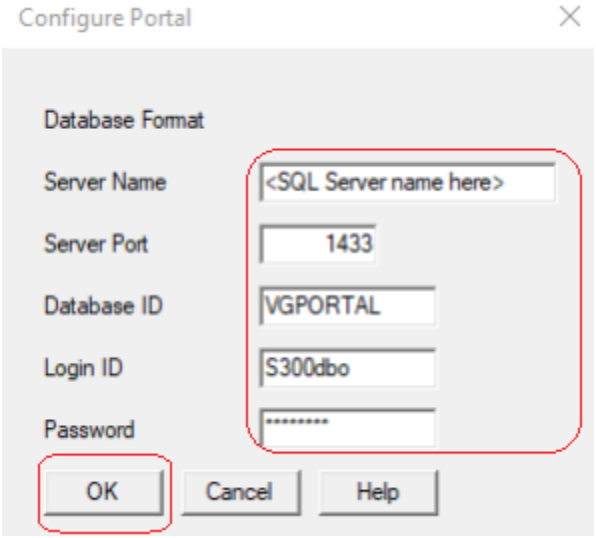
- Enter the MS SQL Server name in the Server field or select an available Data Source
- Enter the password for the MS SQL Server sa user
- Select ***OK*** when complete

Alternatively, you can overwrite any of these values

- Login ID: Ensure that the MS SQL login used has been assigned the “sysadmin” server role.
- Database ID - Vault: Enter a database name for the Vault database. It must start with a letter and contain letters, numbers or the ‘_’ character.
- Database ID - Store: Enter a database name for the Store database. It must start with a letter and contain letters, numbers or the ‘_’ character.

2. Configuring the Portal database

After the ***Configure Databases*** dialog is dismissed, the Sign-on dialog will prompt for login. After you are logged in, you should access the ***Configure Portal*** screen by selecting the Portal button.



Configure Portal screen

In previous versions, this screen would display Portal Database information. However, with this enhancement, you have to re-enter this information .

IF THIS INFORMATION IS NOT SET UP, THE SAGE 300 WEB SCREENS WILL NOT RUN AS THIS INFORMATION IS REQUIRED.

Sage 300 User Security

With this security enhancement, many Sage 300 user security policies, such as invalid password lockout, are now enforced by Windows Account Policies on the machine with the MS SQL Server containing the Store and Vault databases.

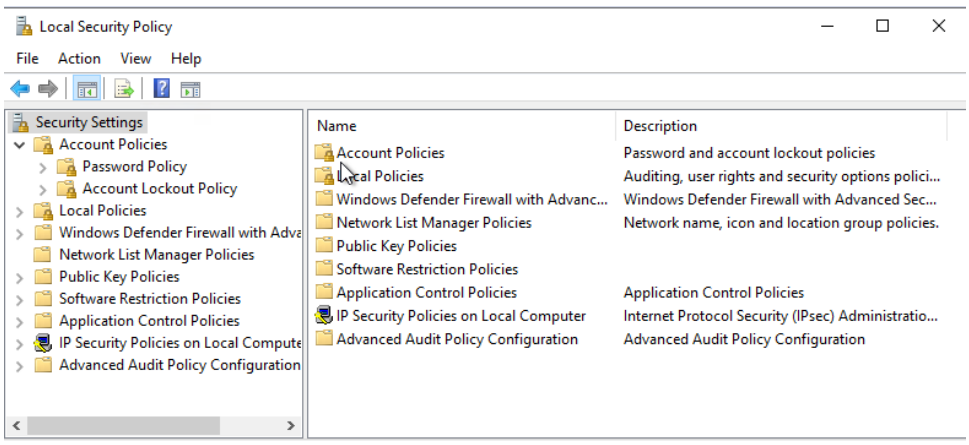
These options have been removed from the Advanced Security Settings screen in the Database Setup screen.

IT IS RECOMMENDED TO SET THE PASSWORD POLICIES ON THE MS SQL SERVER MACHINE BEFORE CONFIGURING THE DATABASES (ALSO KNOWN AS MIGRATION).

On password expiry, users can change their own passwords before they expire. With this security enhancement, after passwords have expired, users can no longer change their own password. ***This includes the Sage 300 ADMIN user.*** *This is a change from previous versions of Sage 300. A user's expired password must be changed in Sage 300 by the Sage 300 ADMIN or another Sage 300 user with Administrative Services rights to edit User records.*

NOTE: Do not let the Sage 300 ADMIN user's password expire since only the ADMIN user can perform certain crucial maintenance tasks. If the Sage 300 ADMIN user's password does expire, it can be reset using a tool from Sage Support.

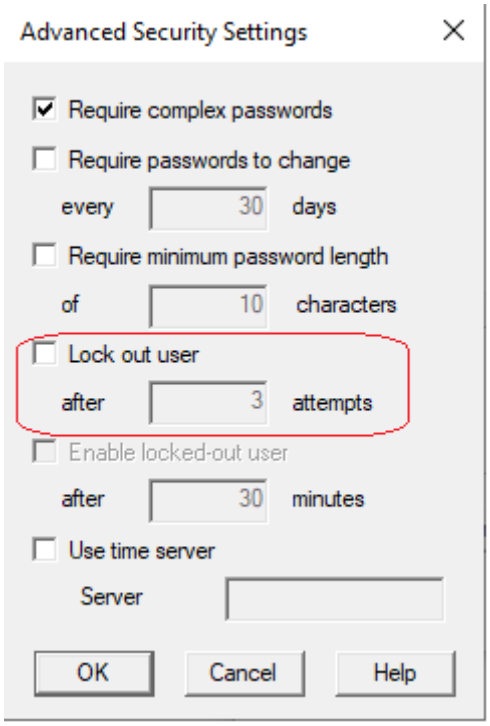
The following Local Security policy screen is where the options and features removed from the Advanced Security Settings in Sage 300 will now be found.



Local Security Policy screen

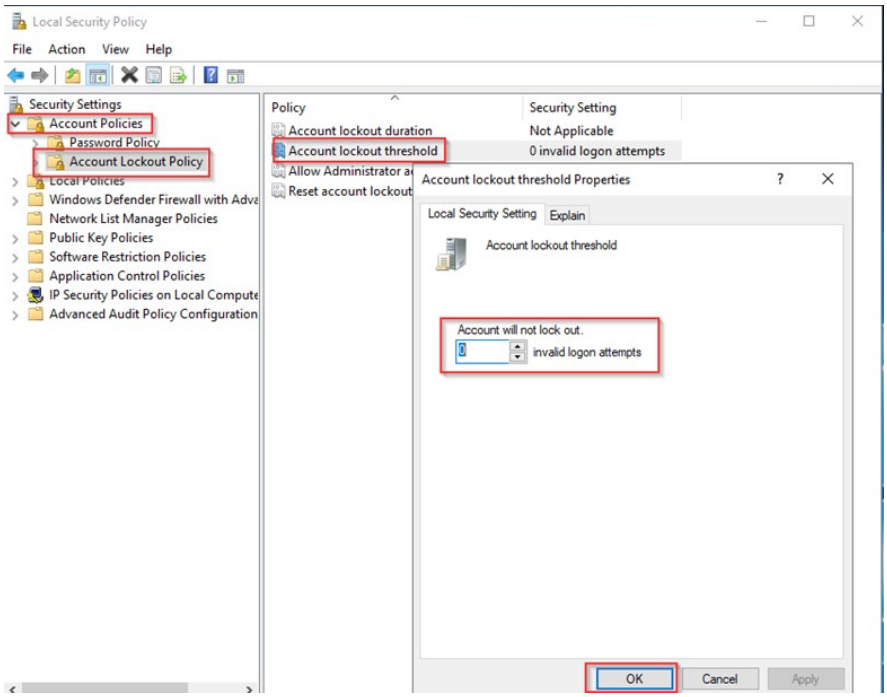
3. How to set Number of Lockout Attempts before the account is locked out

This setting is the replacement for Sage 300's Lockout User After x Attempts feature previously found in the Database Setup's Advanced Security Settings.



Previous version of Lock out user option

- On the computer running MS SQL Server (containing the Vault and Store databases), access ***Windows Administrative Tools → Local Security Policy → Account Policies → Account Lockout Policy***, and double-click on the ***Account Lockout Threshold*** option



Account Lockout Threshold Properties screen

- Enter a number in the ***invalid logon attempts*** field, the number of invalid attempts that will lockout the account.

If 0 is entered, accounts will not lock out.

- Click ***OK***.
- Suggested settings for ***Account Lockout Duration*** and ***Reset Account Lockout After*** will appear next and the defaults can be accepted or new values entered for these two settings.

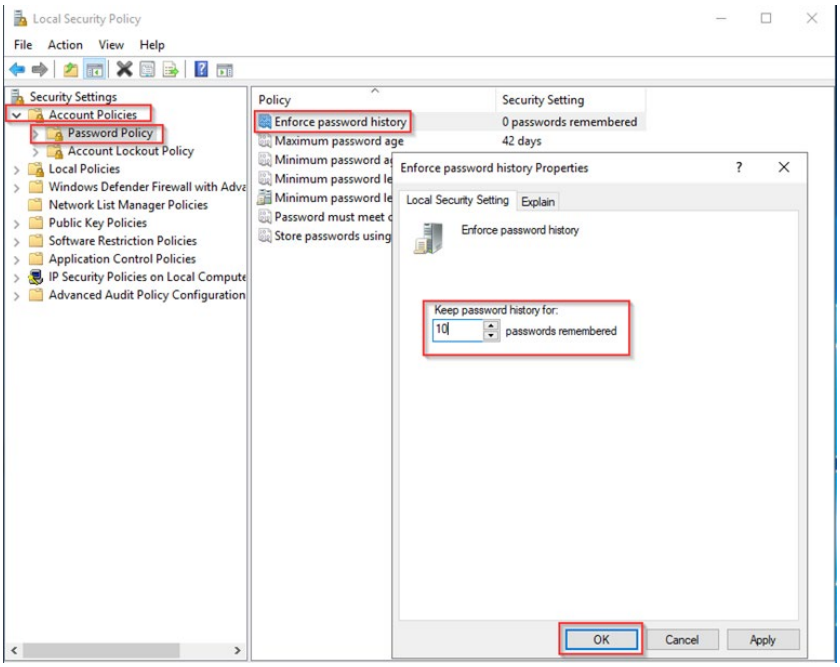
4. How to set whether to Enforce Password History (ability to reuse passwords)

Enforcing password history means that users can't reuse their passwords when they are changed.

This setting determines how many passwords are to be remembered. For example, if the number is 5, the user must change their password 5 times to 5 different passwords before they can reuse the first password on the sixth change.

This setting was not previously visible in Sage 300 Security Settings.

- On the computer running MS SQL Server (containing the Vault and Store databases), access ***Windows Administrative Tools → Local Security Policy → Account Policies → Password Policy***, and double-click on ***Enforce Password History***.

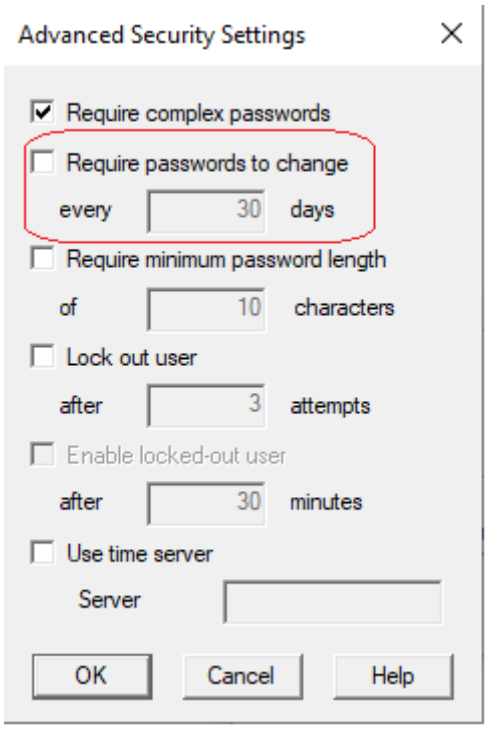


Enforce Password History Properties screen

- In the ***passwords remembered*** field, enter a number of passwords to be remembered for the account.
- Click ***OK***.

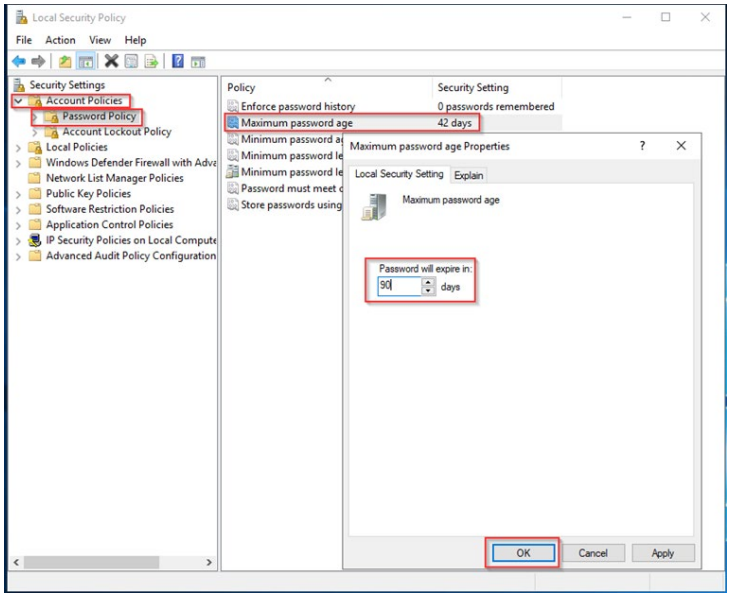
5. How to set the Maximum Password Age

This setting is the replacement for Sage 300's Require Passwords to Change Every x Days feature previously found in the Database Setup's Advanced Security Settings.



Previous version of Require passwords to change option

- On the computer running MS SQL Server (containing the Vault and Store databases), access ***Windows Administrative Tools → Local Security Policy → Account Policies → Password Policy***, and double-click on ***Maximum Password Age***



Maximum Password Age Properties screen

- In the ***days*** field, enter a number of days that the passwords will expire in.

If 0 is entered, the passwords will not expire.

- Click ***OK***.

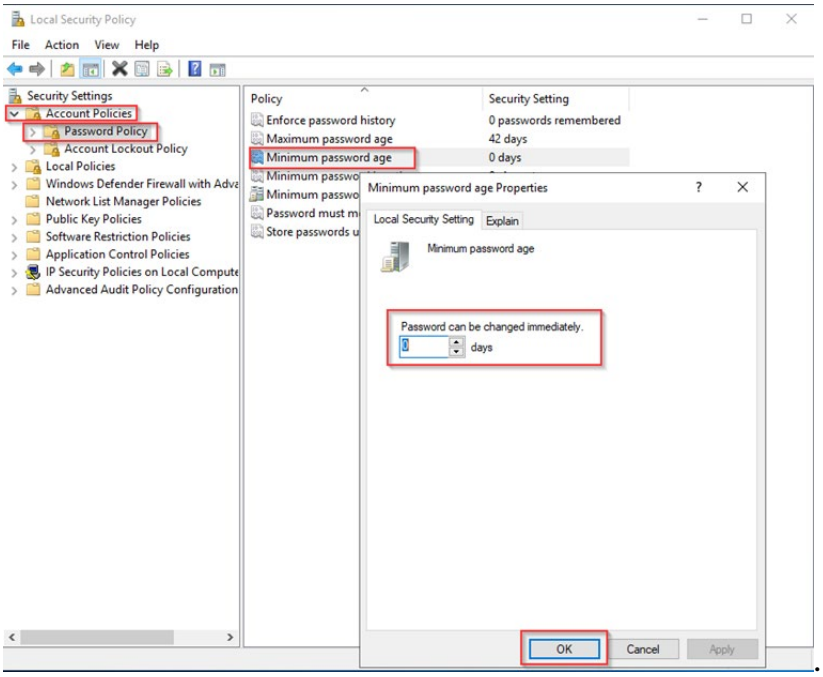
6. How to set the Minimum Password Age

This setting works in conjunction with the Maximum Password Age just described.

A Maximum Password Age must be specified to enable the Minimum Password Age.

NOTE: You should set the Minimum Password Age to 0 (no Minimum Password Age) until you have migrated your system to use the Store and Vault databases and made any necessary password changes.

- On the computer running MS SQL Server (containing the Vault and Store databases), access ***Windows Administrative Tools → Local Security Policy → Account Policies → Password Policy***, and double-click on ***Minimum Password Age***



Minimum Password Age Properties screen

- In the **days** field, enter a number of days that the password can be changed in.

If 0 is entered, the password can be changed immediately.

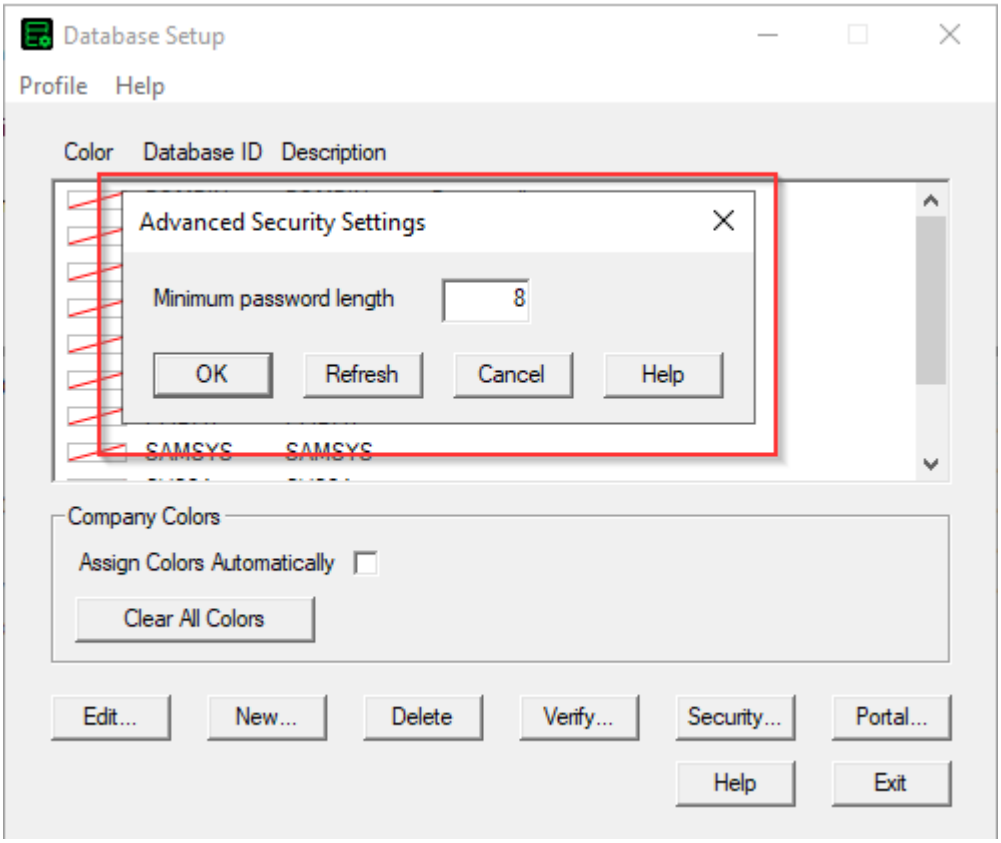
- Click ***OK***.

7. How to Refresh the Windows security settings

We advise you to set the security settings which are governed by windows Local Security policy before you migrate. This way, the settings take effect immediately after migration.

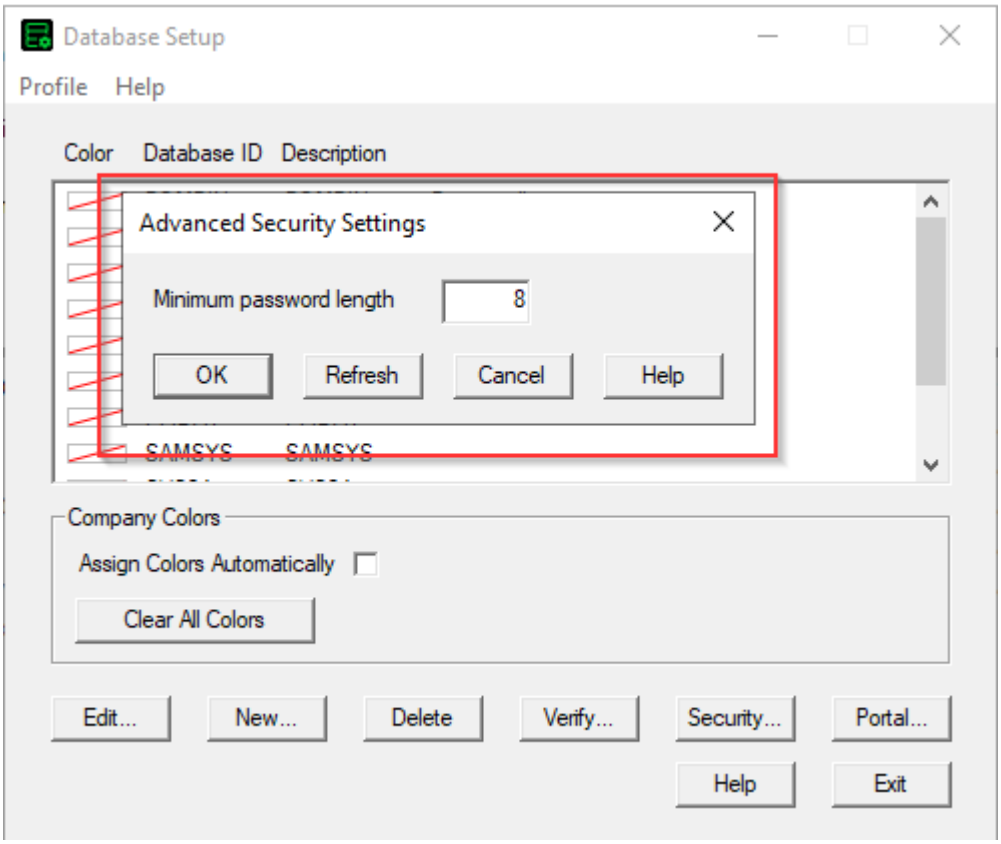
If you make any security policy changes **after** migration, you have to refresh in order for the settings to take effect.

To refresh the Windows security settings, open Database Setup, click the Security... button to open the Advanced Security Settings dialog and then click the Refresh button.



8. How to set the Minimum Password Length

The Minimum password length is still set in the Sage 300 Advanced Security Settings screen, accessed by clicking the Security... button in the Database Setup screen. All other previous settings have been removed from this screen.



Note that the minimum password length is now 8 characters, and all passwords must contain the following:

- An uppercase letter
- A lowercase letter
- A number
- A special character (such as #)

If your system used simple passwords prior to the 2023.2 product update, then users are asked to change their passwords the first time they log in to Sage 300 with this security enhancement.

9. More Security Notes:
Security is now always turned on: the option to turn off Security has been removed from the system database profile in Database Setup.

If your system had security turned off prior to the 2023.2 product update, then users are asked to change their passwords the first time they log in to Sage 300 with this security enhancement. Since users did not use passwords in such a system previously, and likely won't know their original passwords, the Sage 300 ADMIN user can instead log in and update the users' passwords in the Users UI.

10. Workstation Setup Note:

You must reinstall workstation setup after installing and migrating with this security enhancement.

Appendix

Known Issues

This section will present known issues with the security enhancement.

- Cannot sign into Sage 300 Web Screens
    - After successfully migrating Sage 300 to the enhanced security version, the *Portal* database credentials need to be reentered by clicking the Portal button within the Database Setup program. This will allow access to the web screens.
- Cannot sign into Sage 300 due to inability to change password
    - You may encounter a “Password is incorrect” error if the Local Security Policy is set with a Minimum Password age, and you are asked to change the password after migrating.
    - To fix this, ensure that the Minimum Password age is set to 0 (Refer to the How to set the Minimum Password Age section), then restore the SITE folder with a backup and migrate again.
- Sage 300 has provided a Sage 300 Security Guidelines document which contains recommendations and suggestions for implementing security in Sage 300.
    - For the databases, it is recommended to install a certificate on MS SQL Server and to enable TLS encryption. Please refer to this document for more information.
- Migration failure. Here are some potential causes:
    - The Name of the Vault or Store database starts with a number or symbol
    - The Login ID used in the Configure Databases screen does not have the proper MS SQL Server administrator rights
    - The credentials for the ODBC System DSN entry are not valid (“Test Data Source…” must succeed in the System DSN configuration - odbcad32.exe)
    - Not running Database Setup as administrator
    - The Shared Data Folder was entered in UNC (rather than a local path) during the main Sage 300 installation
    - A folder with the name of “Vault” already exists in the SITE folder before migration

- The system requires a reboot

- Backing up your Sage 300 system after migration
    - In the past, users can back up their Sage 300 system setup by making a copy of the SITE folder located in the Shared Data folder. While this is still a necessary step, it alone will not be sufficient for restoring a security enhanced environment. At this time, there is no supported way of backing up and restoring a security enhanced environment. This is a known issue and we are working diligently to release the tools and/or procedures necessary to back up your system setup.
    - The procedures for backing up of your company and system databases remain the same.

- Windows security and local machine policies
    - Several Sage 300 security policies have been removed and replaced with MS SQL Server and local machine policies. The steps in the Migration section explained in detail these replacement policy locations and settings.

- The “Last 10 Passwords” will be reset after migration
    - This policy has been removed from Sage 300 and replaced with MS SQL policy regarding passwords. Therefore, after migration the “Last N Passwords” will start anew.

- No password access or a simple password access to Sage 300 is no longer possible
    - The complexity of a password is directly related to the ease that an actor with nefarious intent can obtain or discover a password. Therefore, with enhanced security in mind, Sage 300 has removed the ability to access Sage 300 without a password and with a simple password as well (no special characters, any length, etc.)

- IIS on different servers
    - The instructions in this document assume IIS is installed on a single server. If IIS is installed on multiple servers, you will need to manually re-configure the portal database on each server for which IIS is installed. Otherwise, the Web screens will not work.
    - Please see the section on Portal database

- Advance Security Settings dialog simplified
    - The Advance Security Settings dialog now has one field to allow you to set the minimum password length.
    - With this security enhancement, the previous Sage 300 user security policies, such as invalid password lockout, are now enforced by Windows Account Policies

on the machine with the MS SQL Server containing the Store and Vault databases.

    - Please see the section on Sage 300 User Security

- Password Expirations

    - Password expirations are now set through the Local Security policy on the machine with the MS SQL server containing the Store and Vault databases

    - Please see the section on Sage 300 Security policy and how to set the maximum password age.

- Local Policy changes

    - If you make any security policy changes after migration, you will have to refresh in order for the settings to take effect.

    - Please see the section on How to refresh windows security settings

- The security enhancement is not compatible with Sage Partner Cloud at this time

- The following features are not compatible with the Security Enhancement. These issues will be addressed for a future release

    - Running certain macros outside of the Sage 300 Desktop

    - Microsoft Project integration

sage.com
0191 479 5911

Sage

acutedata