

Managing 32 Karat software security on stand-alone Windows 10 workstations

Authors: Patrick Quinn-Paquet and Blair C. James

Unscrupulous individuals may wish to surreptitiously alter capillary electrophoresis (CE) data for a variety of reasons, such as the falsification of the data to show an untrue outcome. Proper security settings are important not only to prevent malicious actions, but also to prevent accidental changes or mistakes by otherwise trustworthy individuals. Additionally, regulations such as 21 CFR Part 11 require that automated systems that generate electronic records be properly secured to prevent unauthorized access, help ensure the security of data and prevent data corruption, loss or falsification.

Recent versions of 32 Karat software are tightly integrated with the Windows 10 operating system. By properly configuring Windows 10 in tandem with 32 Karat software, a secure and reliable environment can be maintained with minimal administrative effort.

This guide describes how to configure security on a stand-alone Windows 10 workstation with 32 Karat software installed. It is intended for Windows administrators who are experienced in identifying items that must be configured along with implementing suggested optimal settings. It is important to note that if the operations described here are performed incorrectly, they can severely damage the Windows operating system, rendering it unstable or unusable. For this reason, be sure to carefully configure only the items described in this guide.

While the principles and best practices described here apply equally to stand-alone Windows workstations and Windows networks, these configuration settings are usually controlled by domain-level group policy in a network environment. The optimal settings in such an environment are identical to those described in this paper, but the means of configuration may differ and are beyond the scope of this guide.

Finally, there is some information included about external hard drive scanning stations to help prevent the spread of malware throughout the lab.

Users are ultimately responsible for product security and compliance. These guidelines are provided to you as-is.

Contents

➔	The workstation environment	3
➔	Configure password policy	3
	Enforce password history	3
	Maximum password age	3
	Minimum password age	4
	Minimum password length	4
	Minimum password length audit	4
	Passwords must meet complexity requirements	4
	Store passwords using reversible encryption	4
➔	Protect the system from password-guessing attacks	5
	Account lockout duration	5
	Account lockout threshold	5
	Reset account lockout counter after	5
➔	Audit logon events	6
	Audit account logon events	6
➔	Set and protect the system clock	7
	Change the system time	7
➔	Configure the Windows screen saver	7
	Screen saver	8
	Password protect the screen saver	8
	Screen saver timeout	8
	Hide screen saver tab	8
➔	Authentication	9
	Create Windows user groups	9
	Add user groups to the 32 Karat software security configuration	10
➔	Set file privileges	11
	Set file privileges on the 32 Karat software root directory	11
➔	Manage users	12
	Adding users	12
	Disabling user accounts	12
	Withdrawing 32 Karat software access	12
➔	External hard drive scanning stations	12
➔	Conclusion	12
➔	Contact us	12
➔	References	13

The workstation environment

Workstation security is configured using the Local Security Policy Microsoft Management Console (MMC) snap-in (Figure 1). To launch the Local Security Policy MMC, select **Start → Windows Administrative Tools → Local Security Policy**.

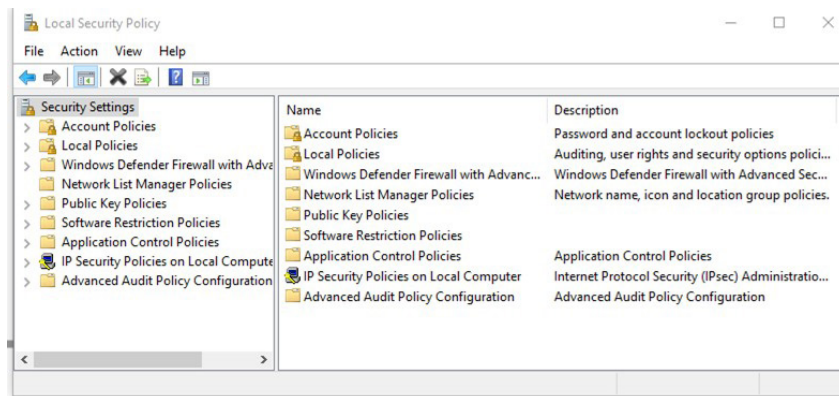


Figure 1. The Local Security Policy MMC snap-in.

Configure password policy

To secure 32 Karat software and to prevent unauthorized access, it is important that user accounts have strong passwords. The Windows operating system allows the establishment of password rules, which apply to all user accounts. Prior to creating user accounts, the system administrator should enable the password policy.

To set the password policy, navigate to the **Security Settings → Account Policies → Password Policy** folder in the Local Security Policy MMC snap-in (Figure 2).

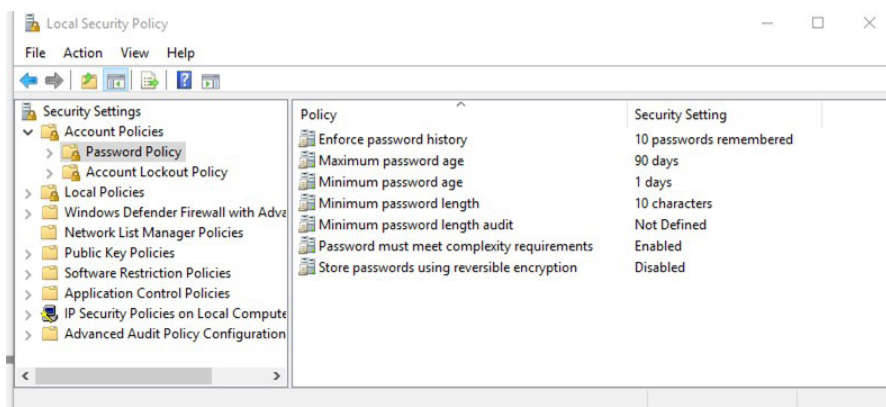


Figure 2. Password Policy in the Local Security Policy MMC snap-in.

Setting	Description
Enforce password history	The Enforce password history setting prevents the reuse of previous passwords. Set this to the number of passwords that will be remembered. In the example in Figure 2, the last 10 passwords will be remembered.
Maximum password age	The Maximum password age setting forces users to change passwords periodically. Set this to the number of days after which passwords expire. Typical settings are 30, 60 or 90 days. In the example in Figure 2, passwords expire at 90 days. Suggestion: Set “Enforce password history” and “Maximum password age” so that the product of the 2 settings equals 1 year.

Setting	Description
Minimum password age	The Minimum password age setting prevents users from changing a password repeatedly in rapid succession to get around the Enforce password history setting so they can reuse a favorite password. Set the Minimum password age to a non-zero value. Higher values are preferable, within reason. In the example in Figure 2, 1 day is the minimum password age.
Minimum password length	The Minimum password length setting determines the minimum length of account passwords. Set this to a value of 8 or more characters, as shown in Figure 2, where it is set to 10 characters. Setting it to 8 or more characters is important because password-cracking tools are readily available that can decipher a shorter password (less than 8 characters) in a matter of days or sometimes hours, depending on the complexity of the password. In contrast, the length of time to crack a password of 8 or more characters can take many years using current technology.
Minimum password length audit	The Minimum password length audit determines the minimum length for which password length audit warning events are issued. This setting may be configured from 1 to 128. This setting helps organizations gauge the effect of imposing a minimum password length. A setting of 12 is suggested.
Password must meet complexity requirements	The Password must meet complexity requirements setting determines, when enabled, requires users to construct account passwords that meet the following criteria: <ul style="list-style-type: none"> • Passwords should not contain the user's account name or parts of the user's full name that exceed 2 consecutive characters • Passwords should be at least 8 characters in length • Passwords should contain characters from 3 of the following 4 categories: <ul style="list-style-type: none"> – English uppercase characters (A through Z) – English lowercase characters (a through z) – Base 10 digits (0 through 9) – Non-alphabetic characters (for example, !, \$, #, %)
Store passwords using reversible encryption	Never enable the Store passwords using reversible encryption setting. Doing so severely compromises the security of account passwords.

Protect the system from password-guessing attacks

Account security could be compromised by an adversary repeatedly attempting to log on to the system using a known username and by guessing the password. Such an attack can be prevented using the account lockout policy.

To access the account lockout policy, navigate to the **Security Settings → Account Policies → Account Lockout Policy** folder in the Local Security Policy MMC snap-in (Figure 3).

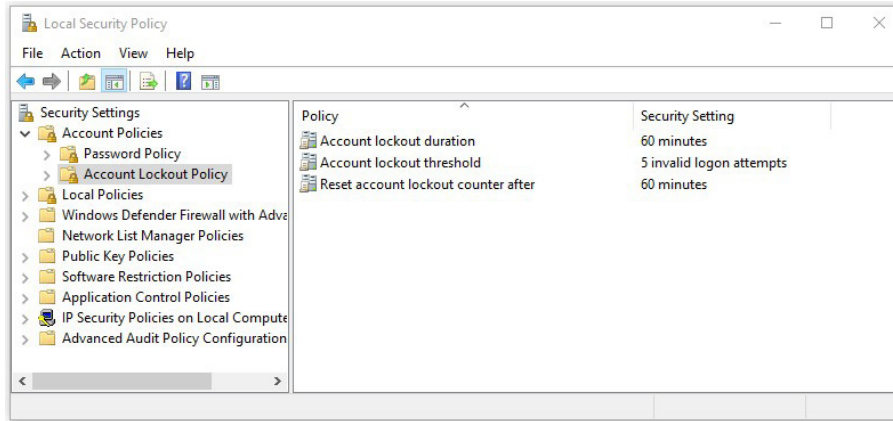


Figure 3. Account Lockout Policy in the Local Security Policy MMC snap-in.

Setting	Description
Account lockout duration	The Account lockout duration setting determines the length of time (in minutes) that a locked-out account remains locked. A setting of zero minutes causes a locked-out account to remain locked until an administrator explicitly unlocks the account. Set this to either zero minutes or a value of 60 minutes or more. The example in Figure 3 shows an account lockout duration of 60 minutes.
Account lockout threshold	The Account lockout threshold setting determines how many unsuccessful logon attempts are permitted at a given time before the affected account is disabled temporarily. Set this to a value between 3 and 5. The example in Figure 3 shows a value of 5 invalid logon attempts.
Reset account lockout counter after	The Reset account lockout counter after setting determines the time interval (in minutes) that the lockout counter is incremented. If no unsuccessful logon attempts occur after the interval specified by the reset account lockout counter, then the counter is reset to zero. This prevents the counter from being incremented indefinitely, which would cause the account to be permanently locked out. Set the reset account lockout counter to a value between 30 and 60 minutes. Figure 3 shows the counter set at 60 minutes.

Audit logon events

To detect persistent attempts to guess account passwords, failed account logon attempts should be recorded in the Windows security event log. Administrative procedures should require periodic reviews of the Windows security event log and investigation of repeated logon failures.

To access the auditing policy, navigate to the **Security Settings → Local Policies → Audit Policy** folder in the Local Security Policy MMC snap-in (Figure 4).

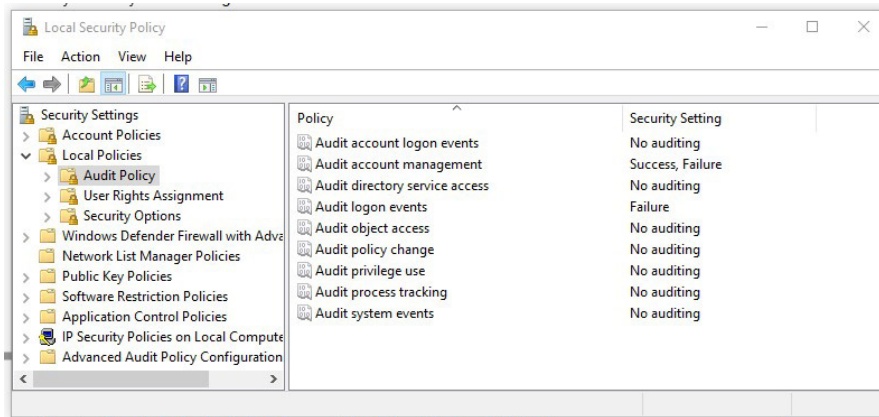
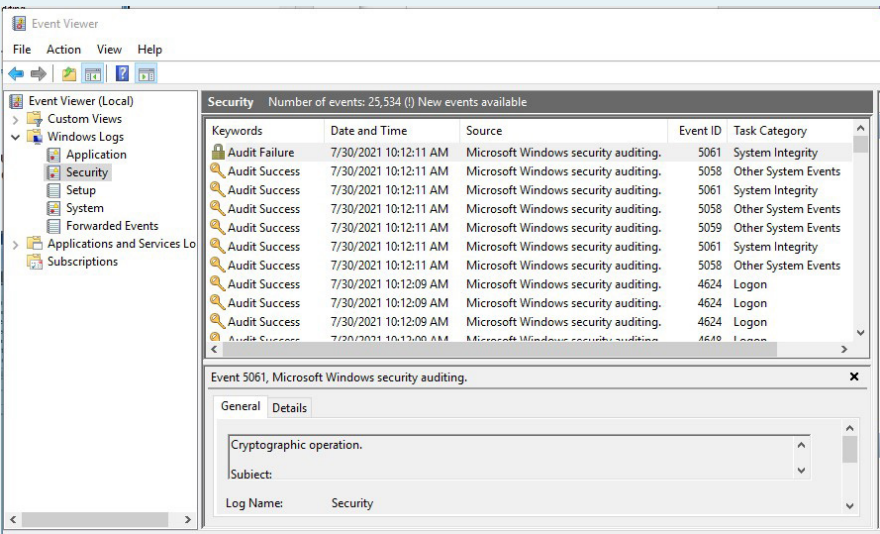


Figure 4. Audit Policy in the Local Security Policy MMC snap-in.

Setting	Description
Audit account logon events	The Audit account logon events setting determines whether to audit each instance of a user logging on to or logging off from a computer. Set this to “Failure” to cause failed logon attempts to be recorded in the Windows security event log. The log may be reviewed using the Start → Windows Administrative Tools → Event Viewer utility (Figure 5).

The screenshot shows the 'Event Viewer' window with the 'Security' log selected. A list of events is displayed, with event 5061 (Audit Failure) selected. The details pane for event 5061 is open, showing the event description: 'Cryptographic operation.' and the log name: 'Security'.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5061	Other System Events
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5058	Other System Events
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5058	Other System Events
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5059	Other System Events
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	7/30/2021 10:12:11 AM	Microsoft Windows security auditing.	5058	Other System Events
Audit Success	7/30/2021 10:12:09 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	7/30/2021 10:12:09 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	7/30/2021 10:12:09 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	7/30/2021 10:12:09 AM	Microsoft Windows security auditing.	4624	Logon

Figure 5. Sample Windows security event log. The event shown is a logon failure.

Set and protect the system clock

Altering the system clock can facilitate data falsification. Users should be prevented from changing the system date, time and time zone.

Permission to change the system clock is controlled by a setting in the Local Security Policy MMC snap-in. To launch the Local Security Policy MMC, select **Start → Windows Administrative Tools → Local Security Policy**. Navigate to the **Security Settings → Local Policies → User Rights Assignment** folder (Figure 6).

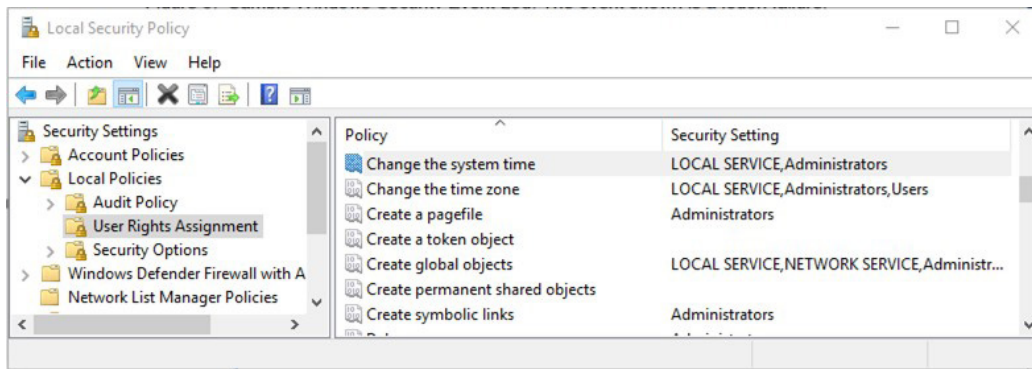


Figure 6. User Rights Assignment in the Local Security Policy MMC snap-in.

Setting	Description
Change the system time	Set Change the system time to “Administrators” to prevent any user not in the Administrators group from modifying system clock settings.

Configure the Windows screen saver

If a workstation is logged in to a user account but left unattended, it is possible for sensitive information to be disclosed to unauthorized individuals or for unauthorized individuals to access system resources. To prevent these security lapses, the Windows screen saver should be configured to obscure the screen and lock the computer after a period of inactivity.

By default, Windows screen saver settings can be modified by any workstation account. Windows 10 allows screen saver settings to be set by the administrator and protected from subsequent modification. The group policy controls the screen saver settings and is maintained using the Group Policy MMC snap-in.

To access the Group Policy MMC snap-in, follow these steps:

1. Launch the MMC from the Windows menu by clicking on the Windows icon, typing “mmc” and selecting “MMC” from the menu.
2. Select **File → Add/Remove Snap-in**.
3. From the “Available snap-ins” list, select the Group Policy Object Editor and then click on **Add → Finish → OK**.

Alternatively, the Group Policy Object Editor can be accessed by pressing the Windows + R keys and typing “gpedit.msc” in the run program prompt.

In the Group Policy MMC snap-in, navigate to the **Local Computer Policy → User Configuration → Administrative Templates → Control Panel → Personalization** folder (Figure 7).

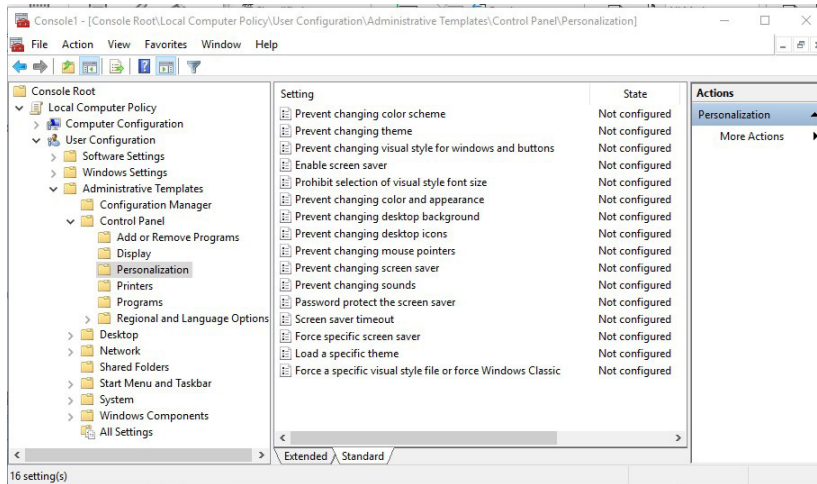


Figure 7. Personalization in the Group Policy MMC snap-in.

Setting	Description
Screen saver	Turn on the Windows screen saver by activating the Enable screen saver setting.

Password protect the screen saver Enable the **Password protect the screen saver** setting to require that the current user’s (or an Administrator’s) password be entered to clear the screen saver (Figure 8).

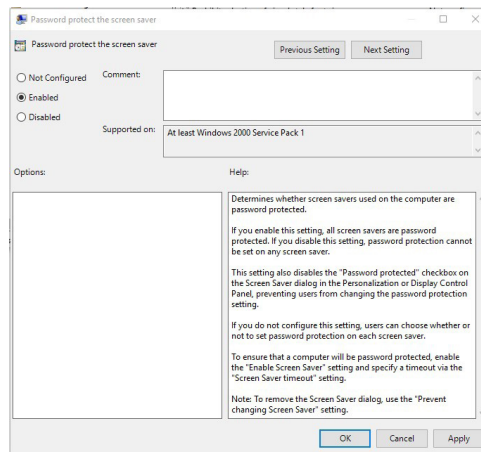


Figure 8. Enable password protection for the screen saver.

Screen saver timeout	Enable the Screen saver timeout setting and enter the desired timeout in seconds. Typical settings range from 600 (10 minutes) to 1,800 (30 minutes). This value should be low enough to keep the workstation secure, but high enough that the user’s productivity is not hampered.
-----------------------------	--

Hide Screen Saver tab Optionally, enable the **Hide Screen Saver tab** setting to remove the Screen Saver tab from the display preferences dialog. This is not strictly necessary, because users will not be able to change the screen saver settings even if access to the Screen Saver tab is permitted.

Authentication

32 Karat software can be configured to use Windows groups rather than individual user account names to control authentication and role assignments. Using Windows groups for authentication allows all user provisioning to be performed at the Windows level, freeing administrators from the burden of updating both Windows account settings and 32 Karat software security configurations when users are added or removed.

For purposes of discussion, the simple hierarchy summarized in Table 1 will be used.

32 Karat software role	Description
System administrator	Software administrator
Method developer	Software user who creates methods and acquires, processes and reports data
Technician	Software user who operates the instrument and acquires data; does not create or modify methods and does not process or analyze data
QA reviewer	Quality assurance representative who reviews data; does not operate the instrument or perform any operations that alter data

Table 1. 32 Karat software roles.

Setting	Description
Create Windows user groups	For each role to be established in 32 Karat software, a single Windows user group should be established whether one or both applications are installed (Table 2).

32 Karat software role	Windows user group
System Administrator	ce_administrators
Method developer	ce_methoddevs
Technician	ce_technicians
QA reviewer	ce_qa_reviewers

Table 2. 32 Karat software roles and user groups.

Windows user groups are created using the Computer Management MMC snap-in. Log on to the Windows operating system as a user with local computer administrator privileges. Launch the Computer Management MMC snap-in by navigating to **Start → Windows Administrative Tools → Computer Management**. Navigate to the **Local Users and Groups → Groups** folder (Figure 9).

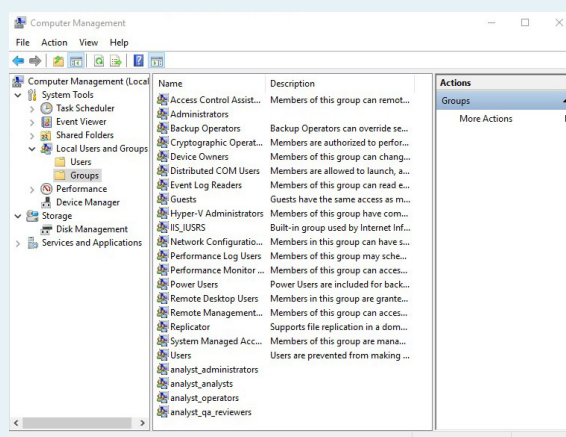


Figure 9. Groups in the Computer Management MMC snap-in.

Create a group for each software role, as in Table 2. To add a group, navigate to **Main Menu → Action → New Group**. Enter the group name and a description, and click the OK button. Do not add user accounts to the groups at this time. Group names can be tailored to your policies.

Add user groups to the 32 Karat software security configuration

To enable users to launch 32 Karat software via the Windows user groups created previously, the groups must be added to the 32 Karat software security configuration. Log in to the application using the Enterprise Login function with the “pa800” user. In the Options dialog, select the Enterprise tab. From the “Obtain user logins and permissions” dropdown menu, select Windows domain controller to use network users. Add the domain the users will come from. If you plan to use local users, select Windows local PC. **IMPORTANT:** Assign at least 1 user with the “System administration” role before restarting the application.



Figure 10. 32 Karat software Administrative Privileges dialog.

In 32 Karat software, open the System Administration wizard and select the User option. Enter the network user or group and move it to the selected user. Select the instrument(s) and the project(s) to be assigned to the user, and then select the specific privileges you want the user to have (Figure 11). Next, set the level of electronic signature required for the user, and then click Finish. Repeat this step for all users/groups on that specific workstation.

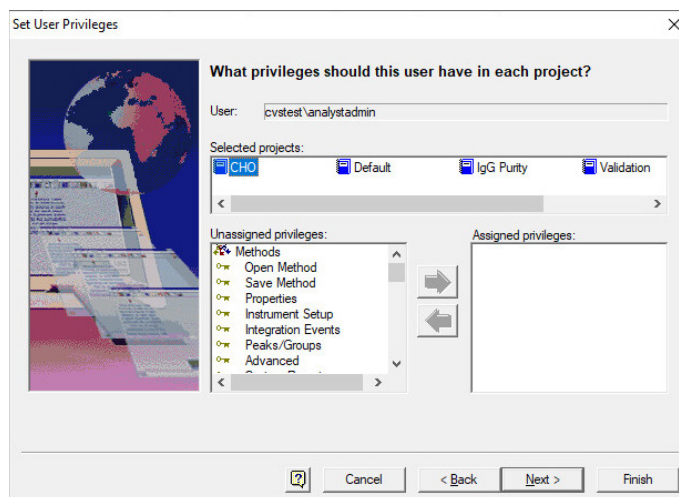


Figure 11. 32 Karat software Set User Privileges dialog.

Set file privileges

21 CFR Part 11 requires that electronic records be protected from accidental or deliberate deletion. In 32 Karat software environments, file privileges must be set on the operating system data files used by the software to store data.

By default, 32 Karat software stores data in folders under a root directory. While this is root directory is typically C:\32Karat\projects, the root directory can be changed depending on the workstation configuration. File privileges should be set on the 32 Karat software root directories so files and folders within the root directory will inherit the privileges.

Setting	Description																																													
Set file privileges on the 32 Karat root directory	<p>File privileges are assigned using the Windows user groups that were created previously: ce_administrators, ce_methoddevs, ce_technicians and ce_qa_reviewers.</p> <p>Using Windows Explorer, navigate to the 32 Karat software root directory. Right-click to display the Properties dialog box, select the Security tab and click the Advanced button. Click the Add button and then click “Select a principal” to add a group. Type in the Windows group and then set the permissions by checking the corresponding checkboxes by each permission. Repeat setting the file privileges for each Windows group, as shown in Table 3.</p> <table border="1"> <thead> <tr> <th>Privilege</th> <th>ce_administrators, system</th> <th>ce_methoddevs, ce_technicians, ce_qa_reviewers</th> </tr> </thead> <tbody> <tr><td>Full control</td><td>Allow</td><td>No entry</td></tr> <tr><td>Traverse folder / execute file</td><td>Allow</td><td>Allow</td></tr> <tr><td>List folder / read data</td><td>Allow</td><td>Allow</td></tr> <tr><td>Read attributes</td><td>Allow</td><td>Allow</td></tr> <tr><td>Read extended attributes</td><td>Allow</td><td>Allow</td></tr> <tr><td>Create files / write data</td><td>Allow</td><td>Allow</td></tr> <tr><td>Create folders / append data</td><td>Allow</td><td>Allow</td></tr> <tr><td>Write attributes</td><td>Allow</td><td>Allow</td></tr> <tr><td>Write extended attributes</td><td>Allow</td><td>Allow</td></tr> <tr><td>Delete subfolders and files</td><td>Allow</td><td>No entry</td></tr> <tr><td>Delete</td><td>Allow</td><td>No entry</td></tr> <tr><td>Read permissions</td><td>Allow</td><td>Allow</td></tr> <tr><td>Change permissions</td><td>Allow</td><td>No entry</td></tr> <tr><td>Take ownership</td><td>Allow</td><td>No entry</td></tr> </tbody> </table> <p>Table 3. 32 Karat software root directory file privileges by role.</p> <p>Once all groups are added, click the checkbox to “Replace all child object permission entries with inheritable permission entries from this object” and then click OK to cascade the permissions.</p>	Privilege	ce_administrators, system	ce_methoddevs, ce_technicians, ce_qa_reviewers	Full control	Allow	No entry	Traverse folder / execute file	Allow	Allow	List folder / read data	Allow	Allow	Read attributes	Allow	Allow	Read extended attributes	Allow	Allow	Create files / write data	Allow	Allow	Create folders / append data	Allow	Allow	Write attributes	Allow	Allow	Write extended attributes	Allow	Allow	Delete subfolders and files	Allow	No entry	Delete	Allow	No entry	Read permissions	Allow	Allow	Change permissions	Allow	No entry	Take ownership	Allow	No entry
Privilege	ce_administrators, system	ce_methoddevs, ce_technicians, ce_qa_reviewers																																												
Full control	Allow	No entry																																												
Traverse folder / execute file	Allow	Allow																																												
List folder / read data	Allow	Allow																																												
Read attributes	Allow	Allow																																												
Read extended attributes	Allow	Allow																																												
Create files / write data	Allow	Allow																																												
Create folders / append data	Allow	Allow																																												
Write attributes	Allow	Allow																																												
Write extended attributes	Allow	Allow																																												
Delete subfolders and files	Allow	No entry																																												
Delete	Allow	No entry																																												
Read permissions	Allow	Allow																																												
Change permissions	Allow	No entry																																												
Take ownership	Allow	No entry																																												

Manage users

Maintenance of 32 Karat software user accounts can now be performed solely in Windows 10, without the need to modify the 32 Karat software security configuration.

Warning: Under no circumstances should an established user account be deleted. Doing so dissociates the user account from entries in the 32 Karat software audit trail and makes it possible to inadvertently reuse the account name.

Setting	Description
Adding users	<p>For each 32 Karat software user, create a Windows user account. Be sure to enter the user's full name (this name will be recorded in the 32 Karat software audit trail). Select the "User must change password at next login" checkbox. Make sure that the "Password never expires" checkbox is cleared.</p> <p>Add the user account to the appropriate Windows group, depending on the user's role. For example, add the administrator for 32 Karat software to the ce_administrators Windows group.</p>
Disabling user accounts	<p>To disallow a user all access to the workstation or the 32 Karat software and data, edit the user's account and select in the "Account is disabled" checkbox. This prevents the user from logging in to the workstation.</p>
Withdrawing 32 Karat software access	<p>To prevent a user from accessing 32 Karat software and data, but still allow the user to log on to the workstation, remove the user's account from all the Windows-created user groups for 32 Karat software: ce_administrators, ce_methoddevs, ce_technicians and ce_qa_reviewers.</p>

External hard drive scanning stations

Even with proper workstation security configuration and industry-standard malware precautions (antivirus/firewall software and network security), computer viruses and other destructive software can still infect the workstation when corrupted external hard drives are used to share data. A simple but important defense is a scanning station. A scanning station is a separate computer with antivirus software installed that is used only for scanning external hard drives. Once the memory stick has been scanned and shown to be free of malware, it can be used to share data with the lab workstation. This extra precaution can be a good way to keep malware from spreading.

Conclusion

The principles and best practices described here for stand-alone Windows 10 workstations can help experienced Windows administrators identify items that must be configured and implement suggested optimal settings to secure 32 Karat software.

Contact us

Contact your local SCIEX sales representatives or contact SCIEX compliance and consulting services at complianceservices@sciex.com.

References

1. PA 800 Plus Pharmaceutical Analysis System – System Administration Guide, Jan 2018
2. Good Laboratory Practice Regulations: Ministry of Health and Welfare Ordinance No. 21, June 13, 2008
3. The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems, GAMP 4 ISPE/GAMP Forum
4. 21 CFR Part 58, Good Laboratory Practices for non-clinical laboratory studies
5. OECD Principles of Good Laboratory Practice and compliance monitoring, revised in 1997 – Number 1, ENV/MC/CHEM(98)17
6. 21 CFR Part 11 – Electronic Records; Electronic Signatures, September 2003
7. OECD GLP Consensus on Computer Systems in the Laboratory
8. GAMP 5 Guide: Compliant GXP Computerized Systems
9. European Union GMP Annex 11 Computerised Systems, effective June 30, 2011