



SCIEX OS software

Managing security for software on stand-alone Windows 11 workstations

Authors: Blair C. James, Patrick Quinn-Paquet and Deanna Snyder



The power of precision

Introduction

Unscrupulous individuals may wish to surreptitiously alter mass spectrometry data for a variety of reasons. Among these is falsification of the data to show an untrue outcome. Proper security settings are also important 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 SCIEX OS software are tightly integrated with the Windows 11 operating system. By properly configuring Windows 11 in tandem with SCIEX OS software, a secure and reliable environment can be maintained with minimal administrative effort.

This white paper describes the process of configuring security on a stand-alone Windows 11 workstation with SCIEX OS software installed. This guidance is 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 performed incorrectly, the operations described here can severely damage the Windows operating system, rendering it unstable or unusable. For this reason, it is recommended that you carefully configure only the items described in this paper.

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 paper.

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



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 SCIEX OS software security configuration | 10 |
| Set file privileges | 11 |
| Set file privileges on the SCIEX OS software root directory | 11 |
| Manage users | 12 |
| Adding users | 12 |
| Disabling user accounts | 12 |
| Withdrawing SCIEX OS software access | 12 |
| Memory stick 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. To launch the Local Security Policy MMC, select:

[Start > Windows Administrative Tools > Local Security Policy.](#)

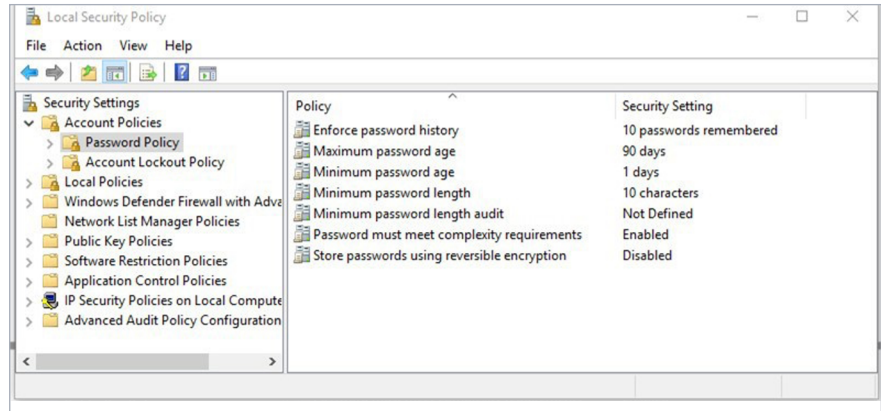


Figure 1. The Local Security Policy MMC snap-in.

Configure password policy

To secure SCIEX OS 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: [Security Settings > Account Policies > Password Policy](#) folder in the Local Security Policy MMC snap-in [Figure 2].

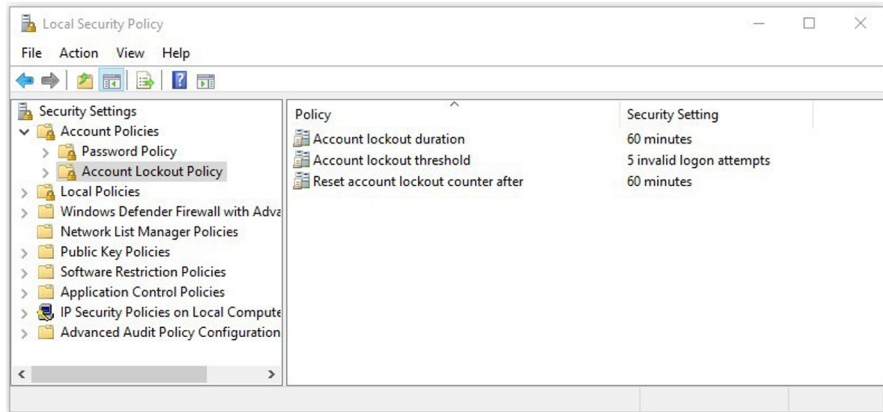


Figure 2. Password policy in the Local Security Policy MMC snap-in.

| Setting | Description |
|--------------------------|--|
| Enforce password history | The Enforce password history setting prevents the reuse of previous passwords. Set this item to the number of passwords 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. |
| Minimum password age | Suggestion: Set “Enforce password history” and “Maximum password age” so that the product of the 2 settings equals 1 year. 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. |

| Setting | Description |
|---|---|
| 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, when enabled, requires users to construct account passwords that meet the following criteria: <ul style="list-style-type: none">· Password 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: <i>English uppercase characters [A through Z]</i> <i>English lowercase characters [a through z]</i> <i>Base 10 digits [0 through 9]</i> <i>Non-alphabetic characters [for example, !, \$, #, %]</i> |
| 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].

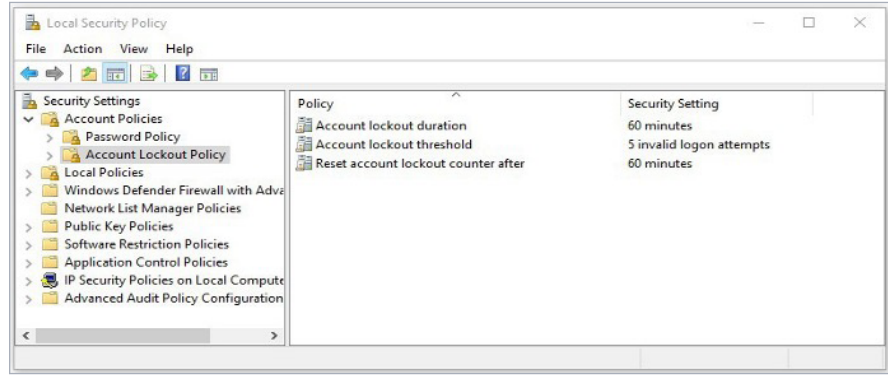


Figure 3. Account Lockout Policy in the Local Security Policy MMC snap-in.

| 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 item to either zero minutes or to 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 in 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 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 reset lockout 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 repetitive 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].

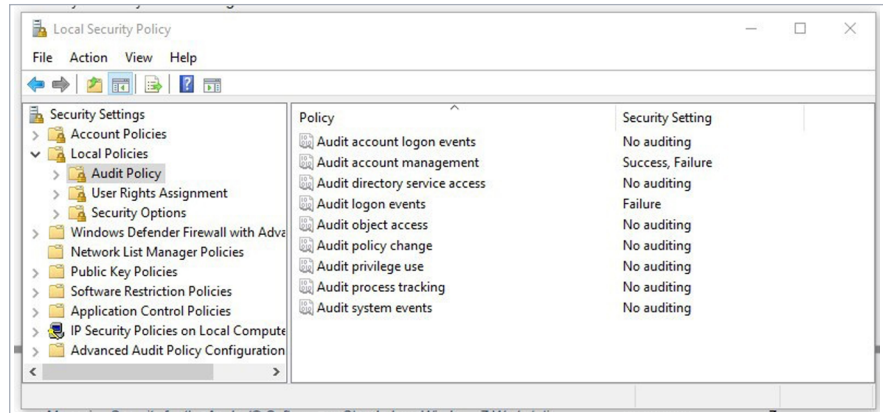


Figure 4. Audit Policy in the Local Security Policy MMC snap-in.

Setting

Description

Audit account logon events

The [Audit account logon events](#) item determines whether to audit each instance of a user logging on to or logging off from a computer. Set this item to “Failure” to cause failed logon attempts to be recorded in the Windows security event log. The log may be reviewed using:

[Start > Windows Administrative Tools > Event Viewer utility](#) [Figure 5].

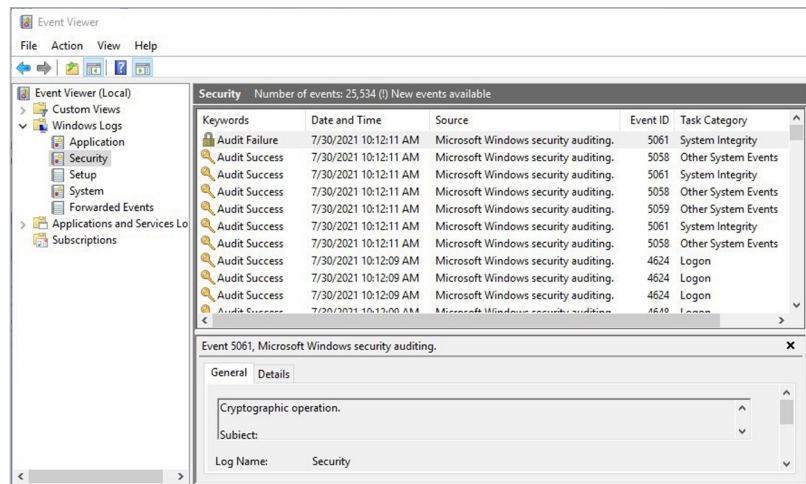


Figure 5. Sample Windows security event log. The event shown is a logon failure.

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].

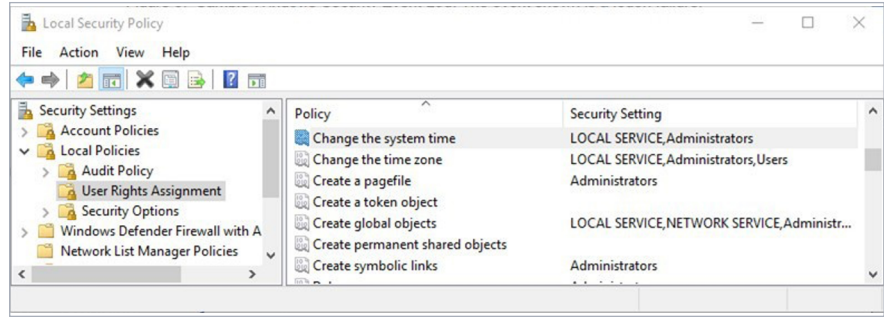


Figure 6. User Rights Assignment in the Local Security Policy MMC snap-in.

| 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 user leaves a workstation logged on but 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 11 allows screen saver settings to be set by the administrator, and for these settings to be protected from subsequent modification.

The group policy controls the screen saver settings. Group policy 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: click on the [Windows icon](#), type “[mmc](#)” and select “[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].

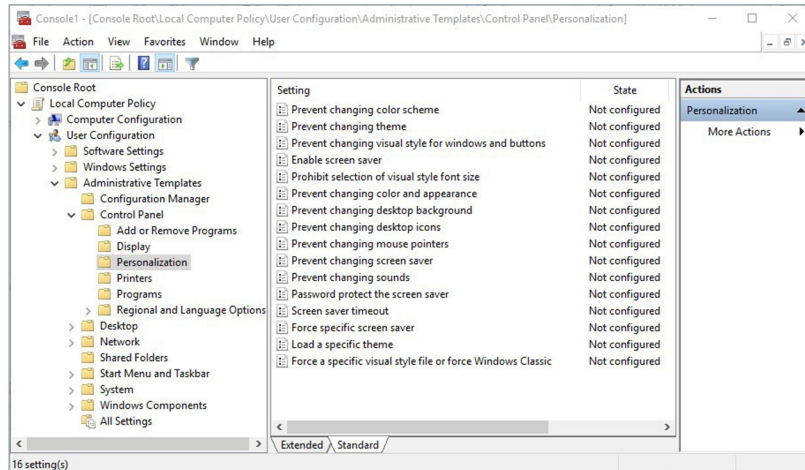


Figure 7. Audit Policy in the Local Security Policy MMC snap-in.

| Setting | Description |
|---------|-------------|
|---------|-------------|

Screen saver Turn on the Windows screen saver by enabling the [Enable screen saver](#) setting.

Password protect the screen saver Enable the [Password protect the screen saver](#) item to require that the current user's (or an Administrator's) password be entered to clear the screen saver (Figure 8).

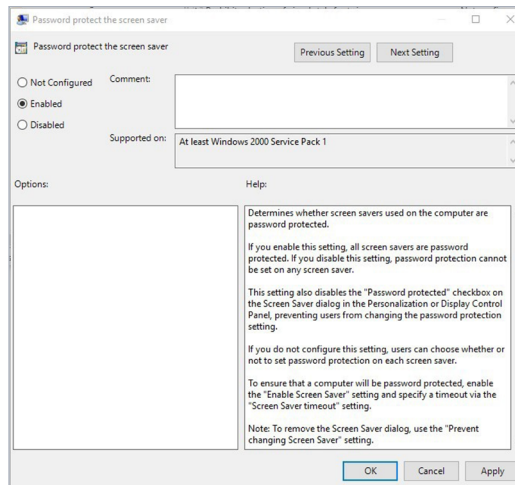


Figure 8. Enable password protection for the screen saver.

Screen saver timeout Set the [Screen saver timeout](#) item to enabled and enter the desired timeout in seconds. Typical settings range from 600 [10 minutes] to 1800 [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](#) item 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

SCIEX OS 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 the administrator from the burden of updating both Windows account settings and SCIEX OS software security configurations when users are added or removed.

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

| SCIEX OS software role | Description |
|------------------------|---|
| Administrator | Software administrator |
| Method developer | Software user who creates methods and acquires, processes and reports data |
| Analyst | Software user who operates the instrument and acquires data; does not create or modify methods, or process or analyze data |
| Reviewer | Quality assurance representative who reviews data; does not operate the instrument, or perform any operations that alter data |

Table 1. SCIEX OS software roles.

| Setting | Description |
|----------------------------|---|
| Create Windows user groups | For each role to be established in the SCIEX OS software, a single Windows user group should be established whether one or both applications are installed [Table 2]. |

| SCIEX OS software role | Windows user group |
|------------------------|------------------------|
| Administrator | analyst_administrators |
| Method developer | analyst_analysts |
| Analyst | analyst_operators |
| Reviewer | analyst_qa_reviewers |

Table 2. SCIEX OS 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 using: [Start > Windows Administrative Tools > Computer Management](#). Navigate to the [Local Users and Groups > Groups](#) folder [Figure 9].

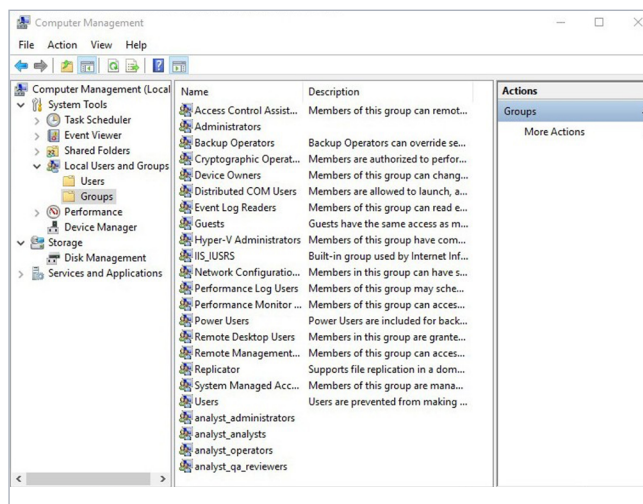


Figure 9. User groups in the Computer Management MMC snap-in.

Create a group for each software role, as in Table 2.

To add a group, [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.

Add user groups to the SCIEX OS software security configuration

To enable users to launch SCIEX OS software via the Windows user groups created previously, the groups must be added to the SCIEX OS software security configuration.

In SCIEX OS software, log on as an administrator user. Launch the configuration tile and click on the User Management tab. Select the Users tab. Click the Add User button (the blue plus sign), which will display the Select Users or Groups dialog box. Use the Select Users or Groups dialog to search for and select each Windows user group created previously. Associate each Windows user group with the corresponding SCIEX OS software role by selecting the Windows user in the drop-down window and then clicking the appropriate role (Figure 10).

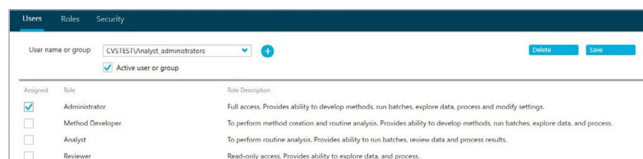


Figure 10. SCIEX OS software User Management tab.

Set file privileges

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

By default, SCIEX OS software store data in folders under a root directory.

While this root directory is typically D:\SCIEX OS Data, it can be changed depending on the workstation configuration. File privileges should be set on the SCIEX OS software root directory so files and folders within the root directory will then inherit the privileges.

| Setting | Description |
|---|--|
| Set file privileges on the SCIEX OS root directory | <p>File privileges are assigned using the Windows user groups that were created previously: analyst_administrators, analyst_analysts, analyst_operators and analyst_qa_reviewers.</p> <p>Using Windows Explorer, navigate to the SCIEX OS software root directory. Right-click to display the Properties dialog box, select the Security tab and click the Advanced button. First, 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> |

| Privilege | Analyst_administrators, system | analyst_analysts, analyst_operators, analyst_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 | |
| Delete | Allow | |
| Read permissions | Allow | Allow |
| Change permissions | Allow | |
| Take ownership | Allow | |

Table 3. SCIEX OS software root directory file privileges by role.

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.

Manage users

Maintenance of SCIEX OS software user accounts can now be performed solely in Windows 11, without the need to modify the SCIEX OS software security configuration.

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

| Setting | Description |
|---|---|
| Adding users | For each SCIEX OS software user, create a Windows user account. Be sure to enter the user's full name (as this name will be recorded in the SCIEX OS software audit trail). Select the "User must change password at next login" checkbox. Make sure that the "Password never expires" checkbox is cleared. |
| Disabling user accounts | To disallow a user all access to the workstation or the SCIEX OS software and data, edit the user's account and place a check in the "Account is disabled" checkbox. This prevents the user from logging into the workstation. |
| Withdrawing SCIEX OS software access | To prevent a user from accessing either the SCIEX OS 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 the SCIEX OS software: analyst_administrators, analyst_analysts, analyst_operators and/or analyst_qa_reviewers. |

Memory stick 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 infected memory sticks 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 memory sticks. Once the memory stick has been scanned and shown to be free of malware, then 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 11 workstations will provide guidance for experienced Windows administrators in identifying items that must be configured along with implementing suggested optimal settings to secure the SCIEX OS software.

Contact us

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

References

1. SCIEX OS software: laboratory director guide, SCIEX, July 2025, RU0-IDV-05-7370-P
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
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

Headquarters

250 Forest Street in Marlborough, MA 01752
Phone 508-383-7700
sciex.com

International Sales

For our office locations please call the division
headquarters or refer to our website at
sciex.com/offices