Managing security for software on stand-alone Windows 10 workstations

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

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 Analyst and SCIEX OS software are tightly integrated with the Windows 10 operating system. By properly configuring Windows 10 in tandem with Analyst and 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 10 workstation with Analyst or 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.

SCIEX

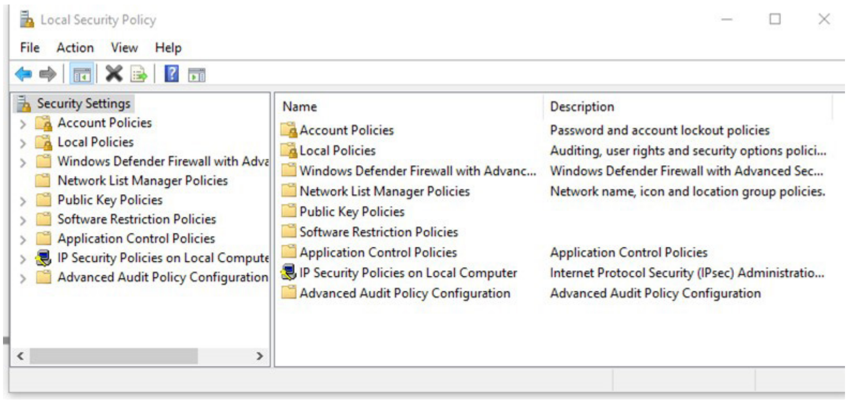
The Power of Precision

< CONTENTS

Contents

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**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

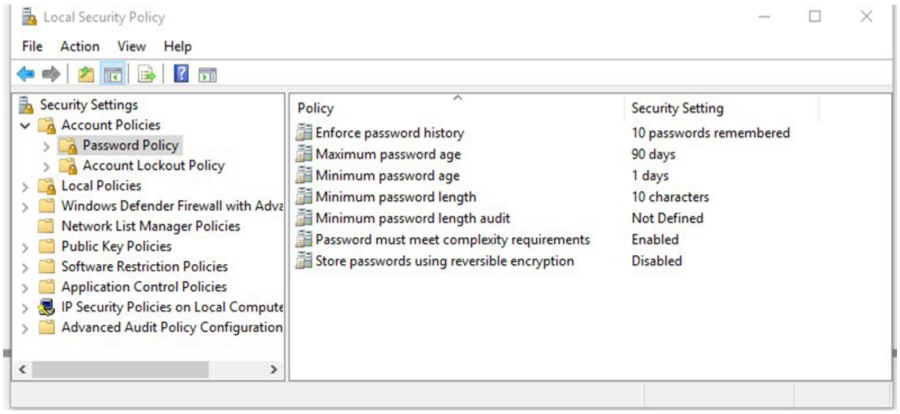
Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

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

Configure password policy

To secure Analyst or 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 the **Security Settings → Account Policies → Password Policy** folder in the Local Security Policy MMC snap-in (Figure 2).


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	10 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	10 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

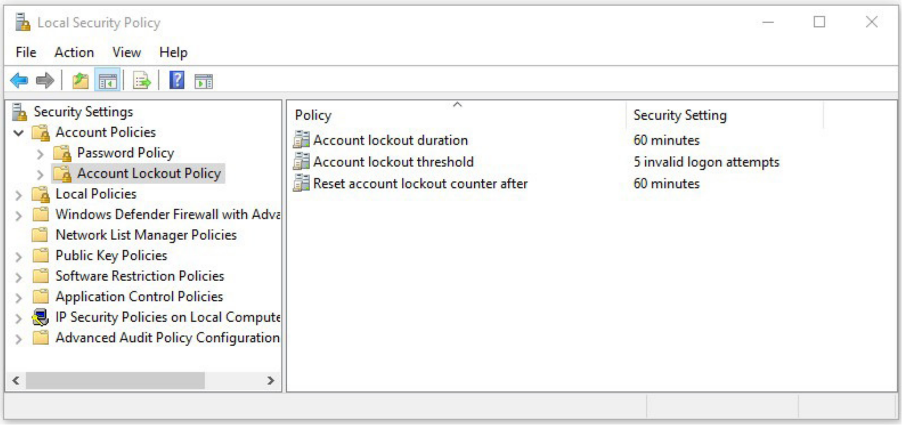
Figure 2. Password policy in the Local Security Policy MMC snap-in.

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. **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 item 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 upon the complexity of the password. However, 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, when enabled, requires users to construct account passwords that meet the following criteria: • 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: o English uppercase characters (A through Z) o English lowercase characters (a through z) o Base 10 digits (0 through 9) o 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).


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	60 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	60 minutes

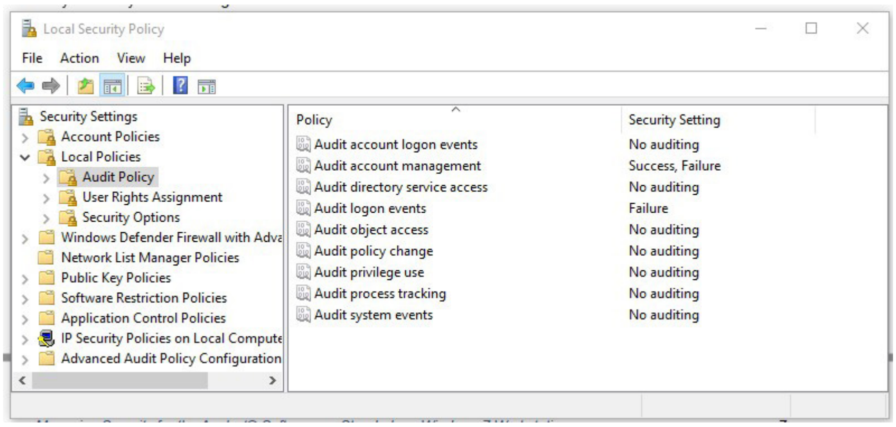
Figure 3. Account Lockout Policy in the Local Security Policy MMC snap-in.

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.

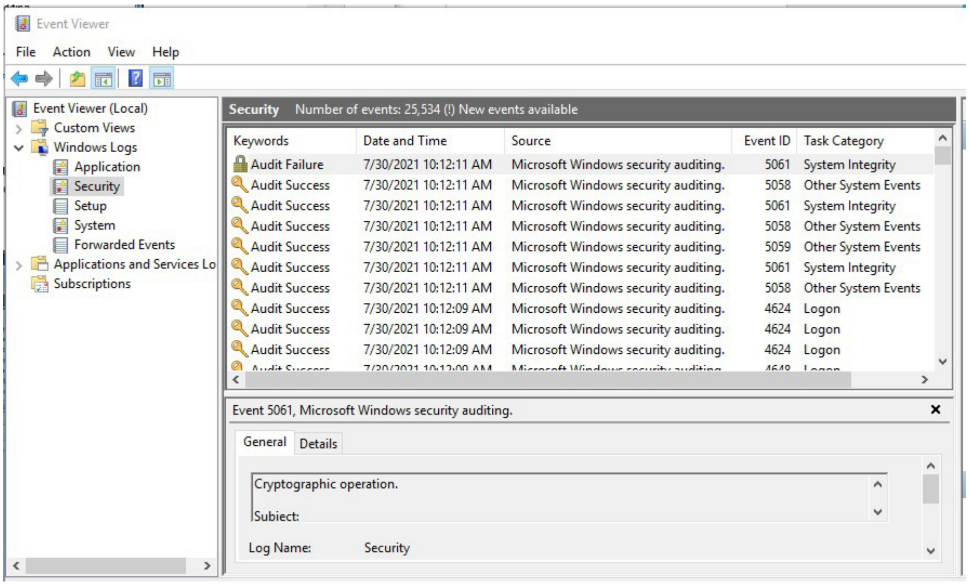
To access the auditing policy, navigate to the **Security Settings → Local Policies → Audit Policy** folder in the Local Security Policy MMC snap-in (Figure 4).


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

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 the **Start → Windows Administrative Tools → Event Viewer** utility (Figure 5).



Security Number of events: 25,534 (!) New events available

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.	5058	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.	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.	4648	Logon

Event 5061, Microsoft Windows security auditing.

Cryptographic operation.

Subject:

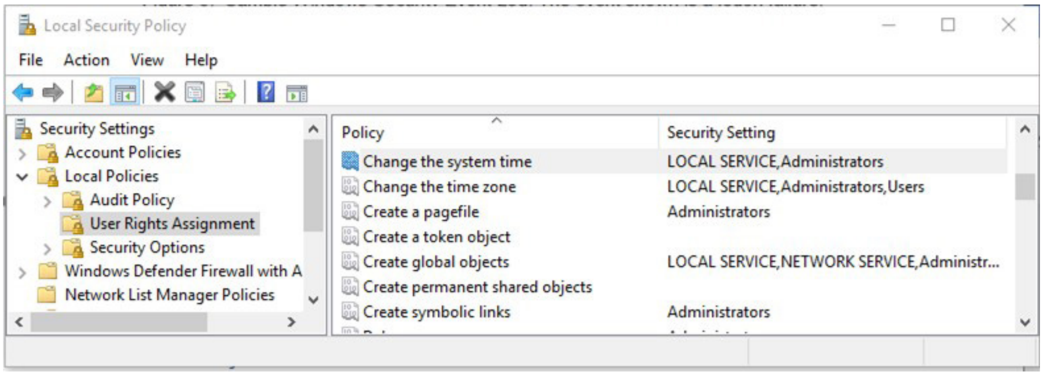
Log Name: Security

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).



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with A
  - Network List Manager Policies

Policy	Security Setting
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,Users
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administr...
Create permanent shared objects	
Create symbolic links	Administrators

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.

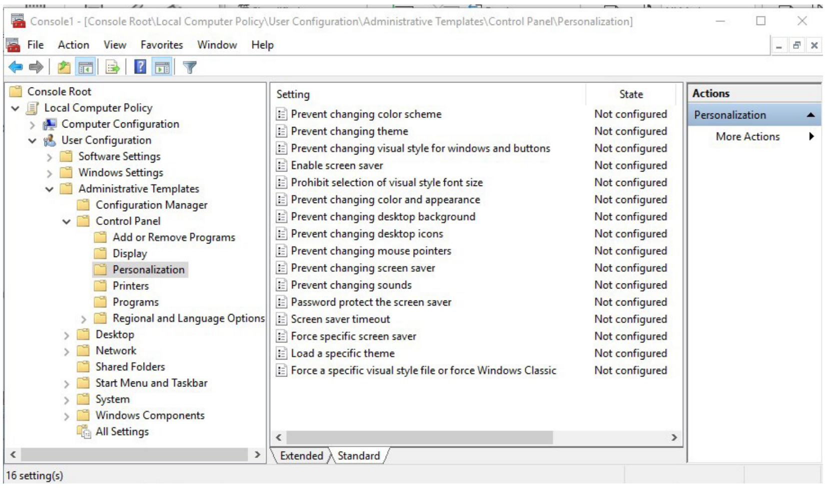
By default, Windows screen saver settings can be modified by any workstation account. Windows 10 allows screen saver settings to be set by the administrator, and for these settings to be protected from subsequent modification. The group policy controls the screen saver settings. Group policy is maintained 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**.

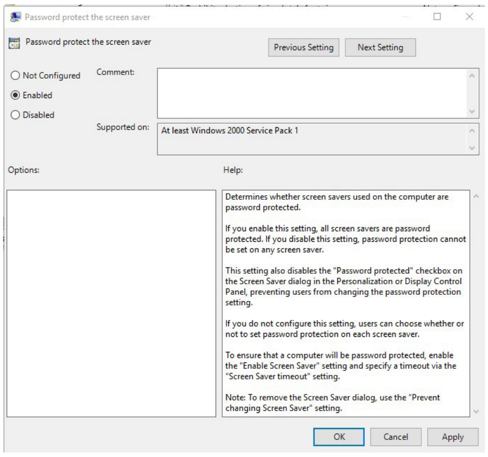
Alternatively, the Group Policy Object Editor can be accessed by pressing the Windows + R keys and typing "gpedit.msc" in the run program prompt.

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



Setting	State
Prevent changing color scheme	Not configured
Prevent changing theme	Not configured
Prevent changing visual style for windows and buttons	Not configured
Enable screen saver	Not configured
Prohibit selection of visual style font size	Not configured
Prevent changing color and appearance	Not configured
Prevent changing desktop background	Not configured
Prevent changing desktop icons	Not configured
Prevent changing mouse pointers	Not configured
Prevent changing screen saver	Not configured
Prevent changing sounds	Not configured
Password protect the screen saver	Not configured
Screen saver timeout	Not configured
Force specific screen saver	Not configured
Load a specific theme	Not configured
Force a specific visual style file or force Windows Classic	Not configured

Figure 7. Personalization in the Group 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).  Password protect the screen saver Previous Setting Next Setting Comment: Supported on: Options: Help: OK Cancel Apply Password protect the screen saver ○ Not Configured ● Enabled ○ Disabled Supported on: At least Windows 2000 Service Pack 1 Determines whether screen savers used on the computer are password protected. If you enable this setting, all screen savers are password protected. If you disable this setting, password protection cannot be set on any screen saver. This setting also disables the "Password protected" checkbox on the Screen Saver dialog in the Personalization or Display Control Panel, preventing users from changing the password protection setting. If you do not configure this setting, users can choose whether or not to set password protection on each screen saver. To ensure that a computer will be password protected, enable the "Enable Screen Saver" setting and specify a timeout via the "Screen Saver timeout" setting. Note: To remove the Screen Saver dialog, use the "Prevent changing Screen Saver" setting. **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

Analyst and 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 Analyst or 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.

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

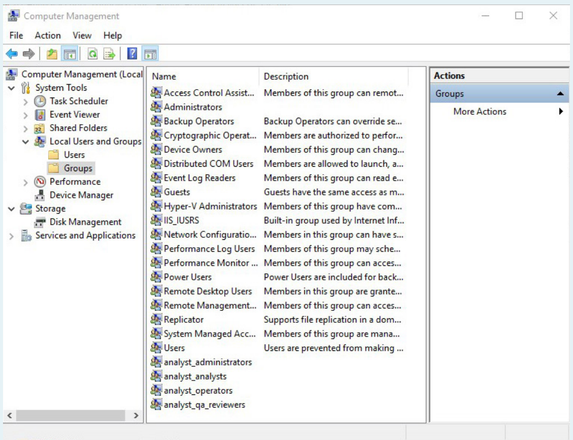
Table 1. Analyst and SCIEX OS software roles.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><b>Create Windows user groups</b></td><td>
For each role to be established in Analyst and/or SCIEX OS software, a single Windows user group should be established whether one or both applications are installed (Table 2).

<table>
<tr><th>Analyst software role</th><th>SCIEX OS software role</th><th>Windows user group</th></tr>
<tr><td>Administrator</td><td>Administrator</td><td>analyst_administrators</td></tr>
<tr><td>Analyst</td><td>Method developer</td><td>analyst_analysts</td></tr>
<tr><td>Operator</td><td>Analyst</td><td>analyst_operators</td></tr>
<tr><td>QA reviewer</td><td>Reviewer</td><td>analyst_qa_reviewers</td></tr>
</table>

Table 2. Analyst and SCIEX OS 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).



<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Access Control Assist...</td><td>Members of this group can remot...</td></tr>
<tr><td>Administrators</td><td></td></tr>
<tr><td>Backup Operators</td><td>Backup Operators can override se...</td></tr>
<tr><td>Cryptographic Operat...</td><td>Members are authorized to perfor...</td></tr>
<tr><td>Device Owners</td><td>Members of this group can chang...</td></tr>
<tr><td>Distributed COM Users</td><td>Members are allowed to launch, a...</td></tr>
<tr><td>Event Log Readers</td><td>Members of this group can read e...</td></tr>
<tr><td>Guests</td><td>Guests have the same access as m...</td></tr>
<tr><td>Hyper-V Administrators</td><td>Members of this group have com...</td></tr>
<tr><td>IIS_IUSRS</td><td>Built-in group used by Internet Inf...</td></tr>
<tr><td>Network Configuratio...</td><td>Members in this group can have s...</td></tr>
<tr><td>Performance Log Users</td><td>Members of this group may sche...</td></tr>
<tr><td>Performance Monitor ...</td><td>Members of this group can acces...</td></tr>
<tr><td>Power Users</td><td>Power Users are included for back...</td></tr>
<tr><td>Remote Desktop Users</td><td>Members in this group are grante...</td></tr>
<tr><td>Remote Management...</td><td>Members of this group can acces...</td></tr>
<tr><td>Replicator</td><td>Supports file replication in a dom...</td></tr>
<tr><td>System Managed Acc...</td><td>Members of this group are mana...</td></tr>
<tr><td>Users</td><td>Users are prevented from making ...</td></tr>
<tr><td>analyst_administrators</td><td></td></tr>
<tr><td>analyst_analysts</td><td></td></tr>
<tr><td>analyst_operators</td><td></td></tr>
<tr><td>analyst_qa_reviewers</td><td></td></tr>
</table>

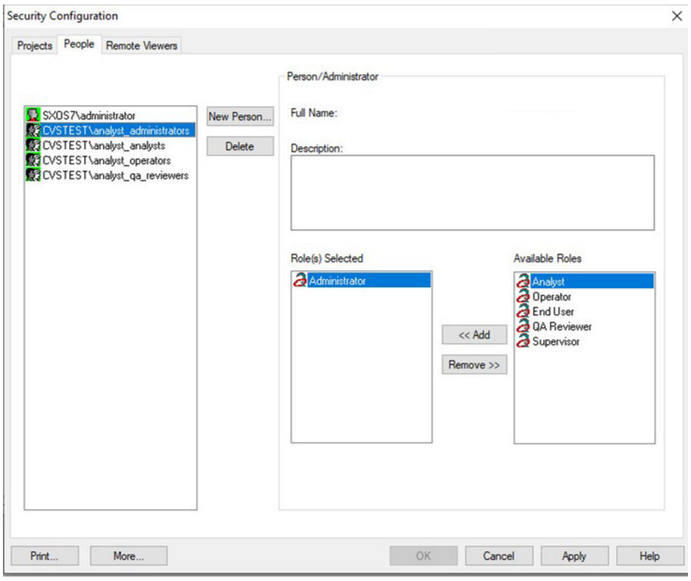
Figure 9. User groups in the Computer Management MMC snap-in.

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.
</td></tr>
</table>

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><b>Add user groups to the Analyst software security configuration</b></td><td>

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

In Analyst software, open the Security Configuration dialog box. Ensure that the security mode is set to either integrated or mixed-mode security. Select the People tab. Click the New Person... button, which will display the Select Users or Groups dialog box. Change the object types to Groups. 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 Analyst software role by selecting the Windows user and clicking the << Add button to add the appropriate role (Figure 10).



SXOS7\administrator
CVSTEST\analyst_administrators
CVSTEST\analyst_analysts
CVSTEST\analyst_operators
CVSTEST\analyst_qa_reviewers

Person/Administrator

Full Name:

Description:

Role(s) Selected: Administrator

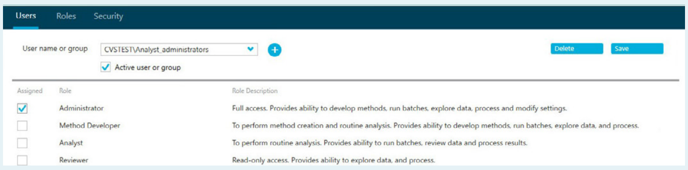
Available Roles: Analyst, Operator, End User, QA Reviewer, Supervisor

Figure 10. Analyst software Security Configuration dialog.

</td></tr>
<tr><td><b>Add user groups to the SCIEX OS software security configuration</b></td><td>

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 11).



User name or group: CVSTEST\Analyst_administrators

☑ Active user or group

<table>
<tr><th>Assigned</th><th>Role</th><th>Role Description</th></tr>
<tr><td>☑</td><td>Administrator</td><td>Full access. Provides ability to develop methods, run batches, explore data, process and modify settings.</td></tr>
<tr><td>☐</td><td>Method Developer</td><td>To perform method creation and routine analysis. Provides ability to develop methods, run batches, explore data, and process.</td></tr>
<tr><td>☐</td><td>Analyst</td><td>To perform routine analysis. Provides ability to run batches, review data and process results.</td></tr>
<tr><td>☐</td><td>Reviewer</td><td>Read-only access. Provides ability to explore data, and process.</td></tr>
</table>

Figure 11. SCIEX OS software User Management tab.

</td></tr>
</table>

Set file privileges

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

By default, Analyst software and SCIEX OS software store data in folders under a root directory. While this root directory is typically D:\Analyst Data or D:\Sciex OS Data, it can be changed depending on the workstation configuration. File privileges should be set on the Analyst software and SCIEX OS software root directories so files and folders within the root directory will then inherit the privileges.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><b>Set file privileges on the Analyst or SCIEX OS root directory</b></td><td>
<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 Analyst or 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>
<table>
<tr><th>Privilege</th><th>analyst_administrators, system</th><th>analyst_analysts, analyst_operators, analyst_qa_reviewers</th></tr>
<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>
</table>
<p><b>Table 3.</b> Analyst and SCIEX OS 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>
</td></tr>
</table>

Manage users

Maintenance of Analyst or SCIEX OS software user accounts can now be performed solely in Windows 10, without the need to modify the Analyst or 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 Analyst software audit trail and makes it possible to inadvertently reuse the account name.

Setting	Description
Adding users	For each Analyst or 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 Analyst or 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. Add the user account to the appropriate Windows group, depending on the user's role. For example, add the administrator for Analyst software to the analyst_administrators Windows group.
Disabling user accounts	To disallow a user all access to the workstation or or the Analyst or 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 Analyst or SCIEX OS software access	To prevent a user from accessing either Analyst or 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 Analyst or 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 10 workstations will provide guidance for experienced Windows administrators in identifying items that must be configured along with implementing suggested optimal settings to secure Analyst and SCIEX OS software.

Contact us

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

References

1. Analyst software: laboratory director’s guide, SCIEX, April 2019, RUO-IDV-05-0268-D
2. SCIEX OS software: laboratory director guide, SCIEX, May 2021, RUO-IDV-05-7370-G
3. Good Laboratory Practice Regulations: Ministry of Health and Welfare Ordinance No. 21, June 13, 2008
4. The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems, GAMP 4 ISPE/GAMP Forum
5. 21 CFR Part 58, Good Laboratory Practices for non-clinical laboratory studies
6. OECD Principles of Good Laboratory Practice and compliance monitoring, revised in 1997 – Number 1, ENV/MC/CHEM(98)17
7. 21 CFR Part 11 – Electronic Records
8. OECD GLP Consensus on Computer Systems in the Laboratory
9. GAMP 5 Guide: Compliant GXP Computerized Systems
10. European Union GMP Annex 11 Computerised Systems, effective June 30, 2011

SCIEX
The Power of Precision

The SCIEX clinical diagnostic portfolio is For In Vitro Diagnostic Use. Rx Only. Product(s) not available in all countries. For information on availability, please contact your local sales representative or refer to www.sciex.com/diagnostics. All other products are For Research Use Only. Not for use in Diagnostic Procedures. Trademarks and/or registered trademarks mentioned herein, including associated logos, are the property of AB Sciex Pte. Ltd. or their respective owners in the United States and/or certain other countries (see www.sciex.com/trademarks). © 2022 DH Tech. Dev. Pte. Ltd.

< CONTENTS