Security Guidance for SCIEX Processing and Acquisition Computers

Purpose

The purpose of this guidance is to provide supplemental information on how to protect your SCIEX instrument-attached computer. This guidance is intended to supplement rather than replace your current IT policies, requirements, and practices. We suggest that you consult with your IT department before implementing any of the recommended changes.

Introduction

Although SCIEX instrument computers are released with a general use operating system, we recommend that you treat the computer as a specialized system that is an extension of the instrument itself. To safeguard the instrument computer, use the computer only to perform the steps required for your workflows, not for additional purposes. We recommend that you follow the security best practices outlined in this document.

Do not use obsolete operating systems

Obsolete operating systems have vulnerabilities and security gaps that can be exploited by attackers. To protect the instrument computer, make sure that it is running Windows 7 or Windows 10. These operating systems have enhanced security features.

Disable USB ports

USB devices can be programmed to spread viruses to any computer they touch. They can infect computers at the boot stage, before antivirus tools can intervene. To protect the instrument computer, disable the USB ports on the front panel of the instrument computer. Make sure that the USB ports on the back panel remain enabled for Service use.

Do not browse the Internet from the instrument computer

Browsing the internet from your instrument computer greatly increases the risk of a malware infection. Certain malware can automatically infect your machine just by visiting a compromised website without any operator intervention. Downloading and installing applications from the Internet greatly increases the surface area of attack and is strongly not recommended.

Do not use email on the instrument computer

Email is the number one vector of attack for delivering malware. Most malware is delivered via email attachments or malicious links within emails. Using email on the instrument computer greatly increases the risk of a potential malware infection. We strongly recommend that no email activity be performed on the instrument computer.

Do not install any unnecessary third-party software

Installing additional software on your instrument computer increases the attack surface for potential infections. Malware authors often exploit vulnerabilities in third party applications (like Adobe Flash) to exploit the underlying operating system. We recommend that, whenever possible, you perform additional work on a non-instrument-attached computer that is intended and protected for such use. If third party applications must be installed, then we recommend that they be kept up-to-date with the latest security patches.

Establish strong password policies

Make sure that your password is at least 8 characters long (10 recommended) and a mixture of uppercase, lowercase, alphanumeric, and special characters. Enable a screen saver password and inactivity timeout (10 minutes recommended). Lock the instrument computer when stepping away from it. Do not share your password with others.

Enable Windows Update

Ensuring critical security patches are installed is essential to maintaining the security of the instrument computer. Our recommended setting is to notify about availability of updates and allow the operator to select which patches to install and when. This provides flexibility to ensure the installation does not negatively affect acquisition from the instrument. Organizations must balance their security needs and risk tolerance with their needs for usability and availability. We recommend that you install any security

patches immediately on release. However, we also recommend that you do not run any Windows updates during SCIEX software acquisition and data processing.

Install antivirus software

While it is a widely acknowledged good practice to employ antivirus and backup software, these applications can interfere with the real-time nature of the SCIEX acquisition software. Some antivirus and backup applications are configured by default to automatically scan and archive a file immediately after creation. Because SCIEX acquisition software can perform multiple writes to a single data file during an acquisition sequence, these real-time features must be disabled to prevent the antivirus or backup software from locking the data file while it is still needed by the SCIEX software application. Many widely-used applications can be configured to either disable real-time protection or ignore certain file-types and paths. Failure to do so may result in either failed acquisitions or acquisitions that take longer to complete than expected.

Follow these guidelines when configuring antivirus software on the acquisition computer:

- Disable real-time scanning and archiving of files.
- Ignore the following file types:

atms	rdb
atds	scan
journal	wiff
qsession	wiff2

- Ignore the following folders or paths:

  For Analyst® software installations:

  - 32-bit: C:\Program Files\Analyst
  - 64-bit: C:\Program Files (x86)\Analyst
  - D:\Analyst Data

  For SCIEX OS installations:

  - C:\Program Data\SCIEX
  - C:\Program Files\SCIEX
  - D:\SCIEX OS Data

  Also ignore any folders containing drivers for connected devices, such as eksigent LC systems.

Note: The default installation location for the Analyst Data folders is D:\. These folders might be installed on a different drive.

For example, in the *Symantec Endpoint* software, the following settings have been found to improve performance during data acquisition:

- Virus and Spyware Protection:
  - Auto-Protect > Advanced > Scan files when: Scan when a file is modified.
  - Early Launch Anti-Malware: Disable Symantec Early Launch Anti-Malware.
- Exceptions > Security Risk Exceptions:
  - Extensions: Make sure that the Extensions list includes the previously specified extensions.
  - Folder: Add the previously specified folders.
- Proactive Threat Protection Settings:
  - General: Disable SONAR.
  - Suspicious Behavior Detection: Disable Suspicious Behavior Detection.
- Network and Host Exploit Mitigation Settings
  - Firewall: Disable Smart DHCP, Smart DNS, and Smart WINS.
  - Memory Exploit Mitigation Policy: Disable Memory Exploit Mitigation.

For users running IDA and scheduled MRM (TripleTOF®, QTRAP®, and X500 QTOF systems), antivirus software might interfere with data acquisition and cause delays with acquisition of data points. We recommend that you either disable real-time antivirus protection, antivirus scheduled scans, and other data-intensive background tasks for these acquisition scenarios or perform validation for your specific antivirus and use case scenarios. After acquisition is complete, re-enable the real-time antivirus.

For instructions on how best to configure your particular antivirus or backup software, contact your antivirus or backup software provider.

Enable Windows Firewall (currently enabled by default)

As an additional layer of security, we recommend that the Windows Firewall remain enabled. The Windows Firewall has been turned on by default and is set to allow only a minimal number of necessary Windows services.

Keep other applications up to date

The SCIEX instrument computer comes with Adobe Reader to allow operators to view our guides and documentation. We recommend that updates be installed as required, to reduce possible attack vectors. If possible, we recommend viewing the user guides and documentation on an alternative computer.

Leave network discovery turned off

Network discovery allows the instrument computer to discover other machines on the network, but also allows other machines to discover the instrument computer. If the machine is discoverable, then it can be scanned for vulnerabilities. Keeping this setting disabled will have little impact on accessing any resources.

Turn off AutoPlay (currently enabled for CD/DVDs and not removable drives)

Malware can take advantage of the AutoPlay (auto run) functionality as a mechanism to infect a computer. Because of a large-scale global virus outbreak in 2008 (Conficker), Microsoft changed the behavior of AutoPlay for removable devices only. We recommend disabling AutoPlay for all media types, including removable and CD/DVD devices.

Backups

The frequency of backup of instrument computers should be commensurate with organizational requirements and the criticality of the data that is generated. Ensuring that backups are functional is a vital component of overall data management and essential to recovery in the event of a malicious attack, hardware failure, or software failure. Do not back up the instrument computer during data acquisition, or make sure that the files mentioned previously are ignored by the backup software. We strongly recommend that a full backup be taken of the instrument computer prior to installation of any security updates. This will facilitate a rollback in the rare case that a security patch affects any application functionality.

Enable Internet Explorer security settings (if browsing the Internet is absolutely required)

While we strongly recommend that Internet browsing not be conducted on the instrument computer, if you choose to do so then you should enable security settings that will help to protect your computer. These include:

- Enable Internet Explorer Enhanced Protected Mode

  To enable Internet Explorer to protect your computer and personal data, Enhanced Protected Mode isolates untrusted web content in a restricted environment known as an AppContainer. This mode limits how much access malware, spyware, and other potentially harmful code has to your system.

- Enable SmartScreen Filter

  SmartScreen Filter helps you identify reported phishing and malware websites and also helps you make informed decisions about downloads. Set the security for the Internet zone to High (if possible). Setting this zone to high will maximize all safeguards available in the browser. As a result, however, the browsing experience will be limited. For example, this setting prevents running of scripts and downloading of files.

- Security Event Log Auditing

  Security event log auditing is a powerful tool to ensure that system activity is tracked and logged. These logs can be used to ensure that regulatory compliance requirements are met, to monitor critical user activity, to detect anomalous behavior, and more. As auditing plays a key role in providing evidence for regulatory compliance, consult with the appropriate personnel prior to making any of the recommended changes. To provide a secure baseline, the following non-default auditing settings are recommended:

Audit Policy Setting	Log on Success	Log on Failure
Audit Credential Validation	Yes	No
Audit Computer Account Management	Yes	No
Audit Other Account Management Events	Yes	No
Audit Security Group Management	Yes	No
Audit Process Creation	Yes	No
Audit Logoff	Yes	No
Audit Logon	Yes	No
Audit Audit Policy Change	Yes	Yes
Audit Security State Change	Yes	Yes
Audit Security System Extension	Yes	Yes

If you have any questions regarding the security of your system, please contact SCIEX Support at https://sciex.com/support.

If you would like to arrange for SCIEX Service to perform on-site securing of your system, please email professionalservices@sciex.com.

Document number: GEN-MKT-16-6060-C

Headquarters
500 Old Connecticut Path | Framingham, MA 01701 USA
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