2100 Expert Security Pack

IT Site Preparation Manual

Purpose	1
Site Requirements	2
Supported User Requirements	5
IT Site Preparation	6

Purpose

This manual is intended to provide an overview about known IT requirements of the 2100 Expert Security Pack (G2949CA). Moreover, this document will provide guidance for customer IT personnel on supported features and required preparations to facilitate a successful installation by a visiting Agilent service engineer.

Site Requirements

Compliance

The Security Pack software allows your system to be compliant with 21 CFR Part 11 regulations. This includes pre-validated methods, managing electronic data and addressing aspects of data security, integrity and traceability mandated by the FDA. Agilent offers services validating full system performance and reliability after the initial installation or whenever modifications or updates were performed.

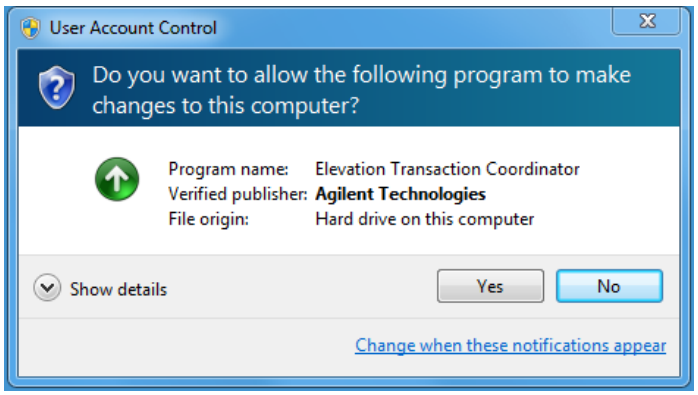
To maintain a validated status, it is mandatory that users or the IT department prevent changes to the overall system after a qualification was conducted. This can include patches applied to the operating system or changes to the overall PC settings. Renaming the PC or changing security policy settings could eventually redeem validation status.

User Access Control

Upon activation of the 2100 Expert Security Pack, a secured vault called *Secured Area* will be created within the installation directory ensuring data security and integrity. Access to this directory is limited to the two user accounts that are specified during the installation. Access to this directory must only be controlled via the software's "User & Roles" settings and not via the operating system settings (NTFS). Entering the *Secured Area* via the operating system (Windows Explorer) without pre-assigned roles, can invoke directory ownership changes resulting in a breach of data security. In case a service account is intended to make backups of the *Secured Area*, make sure to assign this account a "Backup Operator" role within the 2100 Expert Security Pack. For data security, it is recommended to not share the *Secured Area* directory across the network.

For proper operation of the 2100 Expert Security Pack, a dedicated generic user account is required and needs to be set up during the installation. This user has full control on the *Secured Area* and must be a non-human user account for compliance reasons. It is often referred to as **"2100System"** user account thus this name will be used subsequently in this document.

Local administrative rights are required for the "2100System" account to elevate actions depending on the end-user roles as assigned within the Security Pack "User & Roles" settings. To allow such user management features, the 2100 Expert Security Pack makes use of the Microsoft Windows User Access Control (UAC) system. Please be aware that some Anti-Virus software might interfere with the elevation process.



The "2100System" user checks for correct login credentials of all other users within the operating system (local) or the active directory (domain). If user accounts are managed within an active directory, the "2100System" user must be part of that active directory as well.

Deleting or modifying user accounts within the operating system or active directory will directly impact on your 2100 Expert Security Pack. If users are deactivated in the operating system or server, they will become disabled within the 2100 Expert Security Pack. Once a user was permanently deleted from the server or PC, he cannot be re-activated within the Security Pack software due to internal ID assignments.

Known Software Issues

Please review the published issues on the Software Status Bulletin (SSB):
https://www.agilent.com/cs/library/support/Patches/SSBs/G2946CA-G2949CA.html

It is recommended to operate 2100 Expert software on a PC that is part of a closed, physically separated network. Alternatively, the PC may be removed from the network connection completely.

Requirements of the “2100System” user account

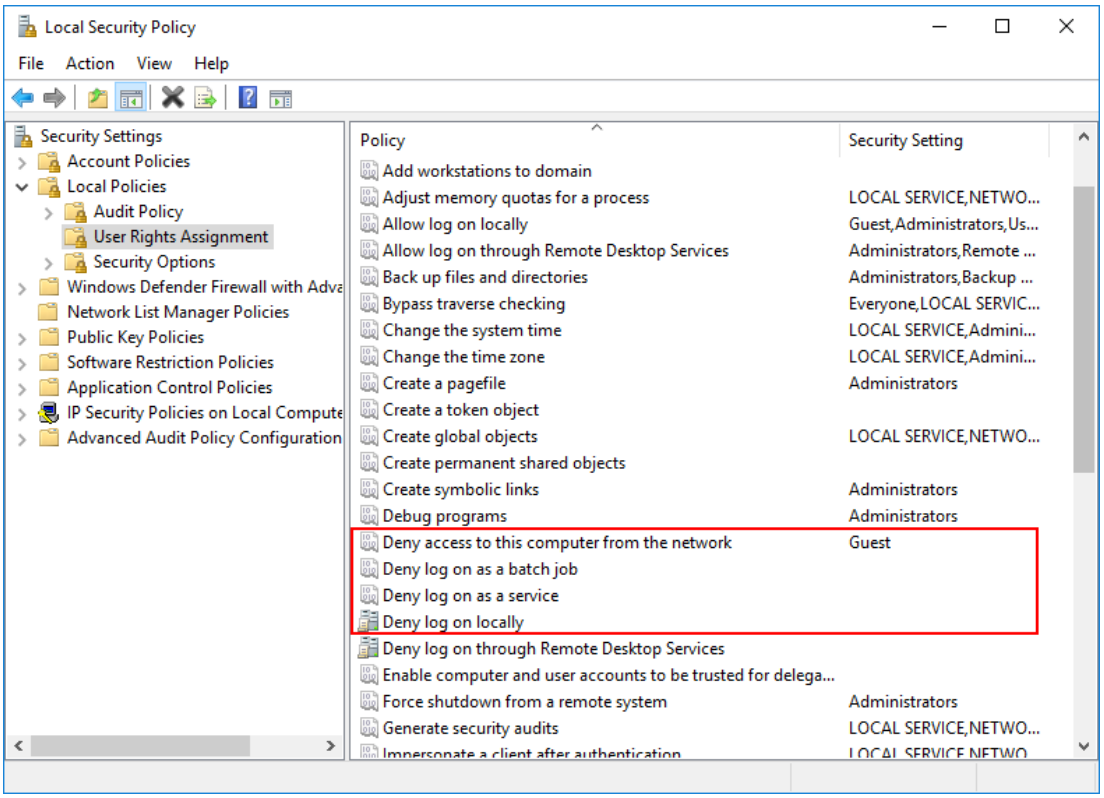
- ✓ Local administrative rights on the PC attached to the instrument.
- ✓ No cached or roaming user profiles.
- ✓ Must not change password on next logon.
- ✓ Password should never expire.
- ✓ Regional settings set to English (US).
- ✓ Default printer is defined.
- ✓ Full domain account (optional if using only local user accounts).

Required Security Policy Settings

Verify the following policy settings are correct for your local system or the domain group policy settings:

The “Administrators” group must **not** be listed in the security settings below (see red square):

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service



Roaming or cached user profiles should not be allowed for the generic “2100System” account.

Supported User Requirements

This chapter will list anticipated and supported user requirements expected from the 2100 Expert Security Pack.

IT System Requirements

- ✓ System backups are supported only when the software is idle (e.g. Acronis backup solutions or NAS devices).
- ✓ Restoring the operating system to a recovery point is supported (potential data loss).
- ✓ The software can authenticate users against an active directory.
- ✓ Remote access to the PC is supported.
- ✓ Instrument and PC are connected via serial RS-232 connection. A USB-to-serial adapter is available (requires specific drivers to be installed).

Regulatory Requirements

- ✓ Supporting 21 CRF Part 11 compliance by providing features:
    - User login:
        - Amount of user accounts is not limited.
        - More user accounts can be added to the software.
        - Password policy is retrieved from operating system.
    - User Roles and permissions:
        - The software allows to assign specific user roles.
        - Permissions are based on the assigned user role.
    - Audit trails:
        - Changes made by any user is tracked.
        - Software displays previous and new values including time stamps.
    - Electronic signatures:
        - The software has date and time stamps for each electronic signature.
        - Signatures can be assigned to pre-defined groups of actions.

Validation Requirements

- ✓ The system is fully compliant for use. Installation Qualification (IQ) and Operational Qualification (OQ) can be performed upon system installation. This service can be provided by Agilent with the necessary IQ and OQ documents.
- ✓ To meet 21 CFR Part 11 requirements, the software must be in a validated state. Specific software Operational Qualification (OQ) can be performed upon request. This service can be provided by Agilent with the necessary OQ documents.

Protocol information about the 2100 Bioanalyzer qualification services can be found online:
https://www.agilent.com/en-us/products/crosslab-instrument-services/compliance/qualification/inkapproval

IT Site Preparation

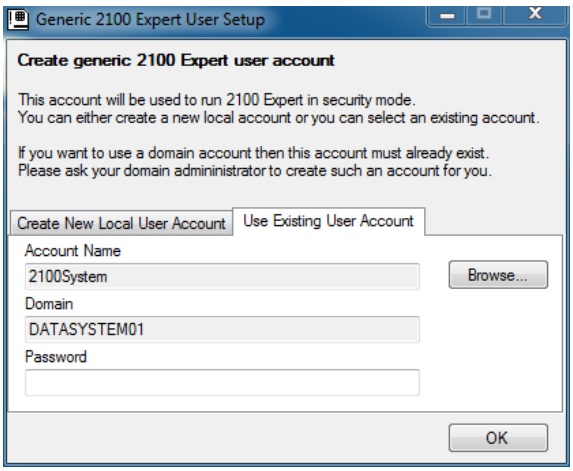
Prior to a Security Pack installation, customers need to define if the system is going to be operated with local or domain user accounts. A mixture of both types will require preparations made as described in section “Using Domain User Accounts”. Due to known issues it is recommended to operate the software in a closed and separated network.

Using Local User Accounts

This chapter described the preparations that need to be performed to use local user accounts only.

Preparations for using local user accounts

Steps		Detailed Instructions		Comments
1	Create a new non-human local user account for the 2100 Expert Software.	**a** **b** **c**	Requires local administrative rights on the PC being attached to the instrument. “User must change password at next logon” setting should be disabled. “Password never expires” setting should be enabled.	• This step is optional but recommended. See comment of Step 4.
2	Logon to the PC with the new “2100System” local user account once for initialization.	**a** **b**	Setup a default printer. Make sure that the regional settings are set to English (US).	• The default printer can be a generic printer like Windows XPS or a PDF printer. • Regional settings must be correct for the system user account.
3	Create local user accounts for software demonstration purpose.	**a** **b** **c** **d**	2100admini Password: 2100admini 2100advanced Password: 2100advanced 2100standard Password: 2100standard 2100validation Password: 2100validation	• Users can be deleted after the demonstration by your Agilent service engineer. • The “2100admini” does not need to be a local administrator on the PC.
4	Provide the “2100System” user details to the Agilent service engineer during setup.	**a**	During Security Pack setup “Use Existing Account” should be used.	• The software also allows to create a new local account during setup. Make sure to repeat step 2 in case the system account is created during the software installation.



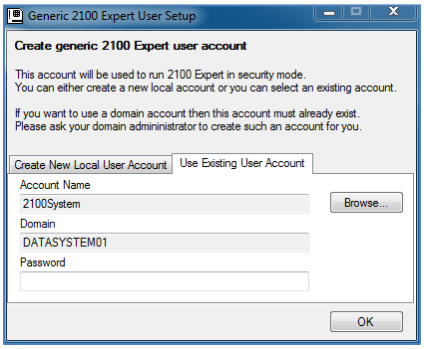
Using Domain User Accounts

This chapter describes IT preparations to use domain users for the Security Pack. In case your company setup is designed to use network/domain user accounts that shall operate the 2100 Expert Security Pack, it is mandatory that the generic “2100System” user account is also a member of the same company network/domain and not a local user profile.

If a local user profile is installed during Security Pack setup as generic system account by accident, this local user might have issues contacting the domain controller to confirm login credentials. Such situation can manifest in diverse errors and user logon problems.

After below preparations, the Agilent service engineer can continue with the software setup as described in chapter 5 of the general software “Readme” file.

Preparations for using domain user accounts

Steps		Detailed Instructions		Comments
1	Create a new user in the same network domain as the final operators.	**a** **b** **c** **d**	Must be a full/default domain user Requires local administrative rights on the PC being attached to the instrument. “User must change password at next logon” setting should be disabled. “Password never expires” setting should be enabled.	• This is a non-human system account. • The user name is not limited to “2100System”, but recommended
2	Access the PC being used with the instrument with this new “2100System” domain user.	**a** **b** **a**	Setup any network resources if required. Setup a default printer. Make sure that the regional settings are set to English (US).	• Shared Network drives or printers need to be setup for this system user. • The default printer can be a generic printer like Windows XPS. • Regional settings must be correct for the system user account.
3	Create local user accounts for software demonstration purpose.	**a** **b** **c** **d**	2100admini Password: 2100admini 2100advanced Password: 2100advanced 2100standard Password: 2100standard 2100validation Password: 2100validation	• Users can be deleted after the demonstration by your Agilent service engineer. • The “2100admini” does not need to be a local administrator on the PC.
4	Add user accounts for Agilent service engineers (IQ/OQ services).	**a** **b** **c**	Add a human user for the service engineer to logon to the system. For the software OQ procedure, add a local user called “OQADMIN”. For the software OQ procedure, add a local user called “OQUSER”.	• The service engineer human account can be a local or domain user account. • Accounts for the OQ procedure can be local accounts without administrative rights. • Make sure to share the password with the engineer.
5	Agilent will proceed with Security Pack installation.	**a** **b**	Choose “Use Existing User Account” Browse for the correct domain “2100System” user account created in step 1.	

In This Document

The manual describes the following:

- Purpose
- Site Requirements
- Supported User Requirements
- IT Site Preparation

www.agilent.com

Revision A.03

Document number: D0000809

Agilent