PROCESS AUTOMATION

Freelance 2019

Engineering Manual
User Management

PROCESS AUTOMATION

Freelance 2019

Engineering Manual
User Management

Document Number: 3BDD012513-111
Revision: Ad0
Release: Febuary 2019

Notice

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

Products described or referenced in this document are designed to be connected, and to communicate information and data via a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect the system, its products and networks, against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

ABB verifies the function of released products and updates. However system/product owners are ultimately responsible to ensure that any system update (including but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) is compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment they are deployed.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2014/30/EU and in Low Voltage Directive 2014/35/EU.

Trademarks

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Table of Contents

About this book

1 - User Management for Freelance

2 - Extended User Management

3 - Security Lock

About this book

Use of warning, caution, information, and tip icons

This publication includes **Warning**, **Caution**, and **Information** where appropriate to point out safety related or other important information. It also includes **Tip** to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Electrical warning icon indicates the presence of a hazard which could result in *electrical shock.*

Warning icon indicates the presence of a hazard which could result in *personal injury.*

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in *corruption of software or damage to equipment/property.*

Information icon alerts the reader to pertinent facts and conditions.

Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although **Warning** hazards are related to personal injury, and **Caution** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all **Warning** and **Caution** notices.

Terminology

The Glossary contains terms and abbreviations that are unique to ABB or have a usage or definition that is different from standard industry usage. Please make yourself familiar to that.

You will find the glossary at the end of the ***Engineering Manual System Configuration.***

Document conventions

The following conventions are used for the presentation of material:

- The words in names of screen elements (for example, the title in the title bar of a window, the label for a field of a dialog box) are initially capitalized.
- Capital letters are used for the name of a keyboard key if it is labeled on the keyboard. For example, press the ENTER key.
- Lowercase letters are used for the name of a keyboard key that is not labeled on the keyboard. For example, the **space bar**, **comma key**, and so on.
- Press CTRL+C indicates that you must hold down the CTRL key while pressing the C key (to copy a selected object in this case).
- Press **ESC, E, C** indicates that you press and release each key in sequence (to copy a selected object in this case).
- The names of push and toggle buttons are boldfaced. For example, click **OK**.
- The names of menus and menu items are boldfaced. For example, the **File** menu.
  - The following convention is used for menu operations: MenuName > MenuItem > CascadedMenuItem. For example: select **File** > **New** > **Type**.
  - The **Start** menu name always refers to the **Start** menu on the Windows Task Bar.

- System prompts/messages are shown in the Courier font, and user responses/input are in the boldfaced Courier font. For example, if you enter a value out of range, the following message is displayed:

  ```
  Entered value is not valid. The value must be 0 to 30.
  ```

  You may be told to enter the string TIC132 in a field. The string is shown as follows in the procedure:

  TIC132

  Variables are shown using lowercase letters.

  sequence name

1 User Management for Freelance

For better data security and more friendly user experience, Freelance provides Extended User Management (EUM) in addition to Security Lock for user access rights management. Therefore, the user can select preferred login methods according to the different situations. There are three deployment modes selectable with different functions supported.

Mode	Auto Log-off	Password Policies	Central Password Management
EUM-Use Local Account	√	√	-
EUM-Use Domain Account	√	√	√
Security Lock	√	-	-

The check(√) symbol in the table stands for Function is supported, and the hyphen(-) stands for Function is not supported.

2 Extended User Management

2.1 Extended User Management – General description

The Extended User Management enables system administrators to apply best practices and security considerations like access control and password policies to the Freelance DCS system. It is based on Windows Security Technologies.

With the Extended User Management enabled, the user can use either local account or domain account to login to the work stations (computers with Freelance Engineering and Freelance Operations installed).

2.2 Extended User Management operations

2.2.1 Enable Extended User Management

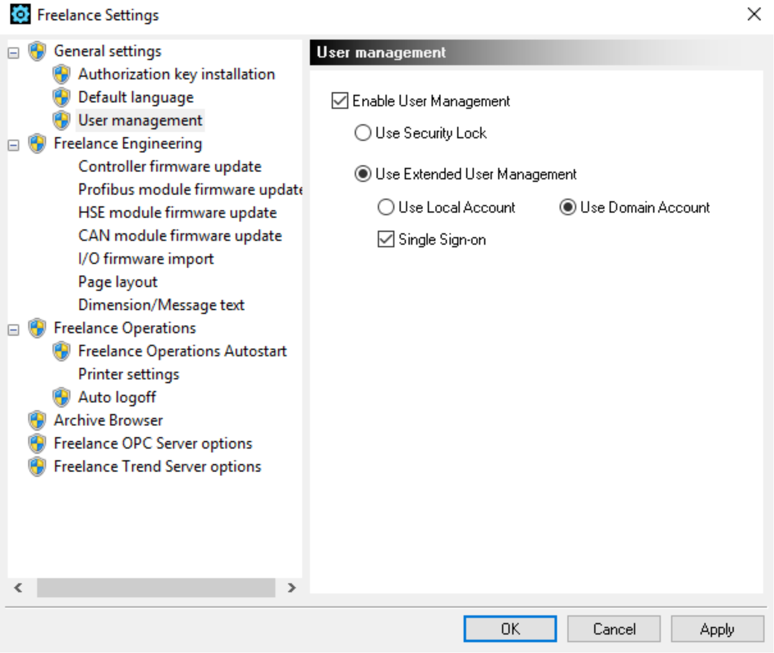
If user wants to enable Extended User Management, user needs to configure it through Freelance Settings.

User has to have the administrative rights to operate in Freelance Settings, otherwise the configuration page is grayed-out.

- Launch Freelance Settings.
- Go to General Settings in the left panel and click **User Management**.
- Enable the checkbox “Enable User Management”.

If the User Management function is disabled, the system requires no user to log in.

- Click **Use Extended User Management** and select **Use Local Account** or **Use Domain Account**.
- (Optional) Check Single Sign-on if user wants to login to Freelance automatically.


Freelance Settings
General settings
Authorization key installation
Default language
User management
Freelance Engineering
Controller firmware update
Profibus module firmware update
HSE module firmware update
CAN module firmware update
I/O firmware import
Page layout
Dimension/Message text
Freelance Operations
Freelance Operations Autostart
Printer settings
Auto logoff
Archive Browser
Freelance OPC Server options
Freelance Trend Server options
OK
Cancel
Apply

User management

☑ Enable User Management

○ Use Security Lock

● Use Extended User Management

○ Use Local Account ● Use Domain Account

☑ Single Sign-on

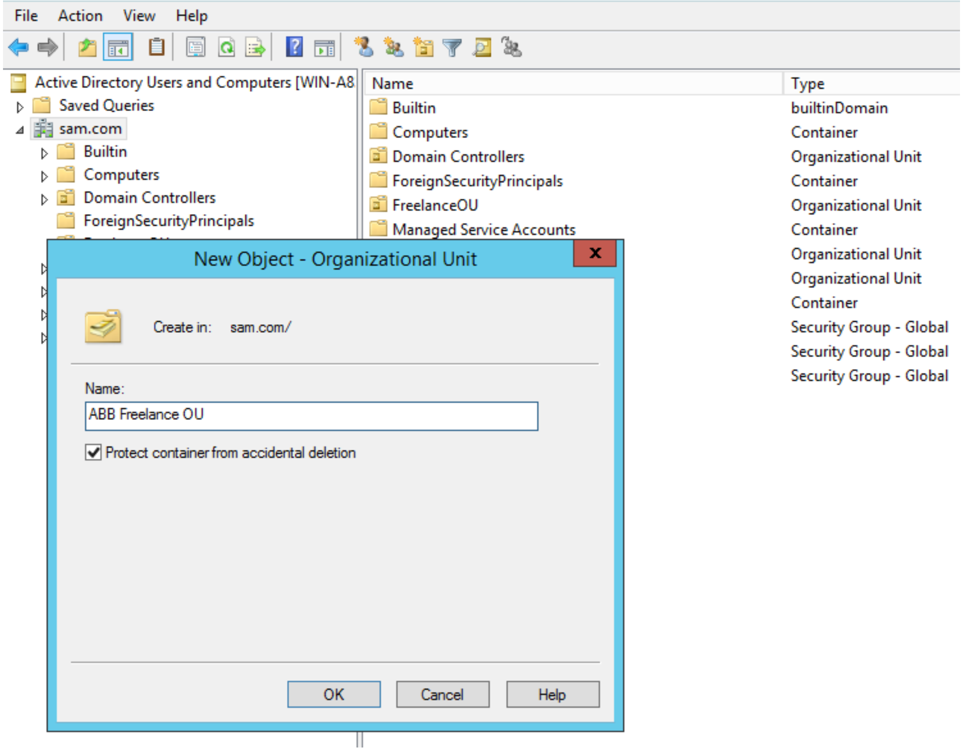
Enable Extended User Management

2.2.2 Use domain account

Configure domain server

Domain server configuration is prerequisite before user use the domain account. Complete the domain server settings by the following steps.

- Build a domain. Please refer to Microsoft documentation for detailed steps to set up a domain,e.g.: https://blogs.technet.microsoft.com/canitpro/2017/02/22/step-by-step-setting-up-active-directory-in-windows-server-2016/
- Create Organization Unit (OU): right click on the domain, and select **New > Organization Unit**. Input the customized OU name in the pop-up box, and click **OK** to complete.


File
Action
View
Help
Active Directory Users and Computers [WIN-A8
Saved Queries
sam.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
New Object - Organizational Unit
OK
Cancel
Help

Name	Type
Builtin	builtinDomain
Computers	Container
Domain Controllers	Organizational Unit
ForeignSecurityPrincipals	Container
FreelanceOU	Organizational Unit
Managed Service Accounts	Container
	Organizational Unit
	Organizational Unit
	Container
	Security Group - Global
	Security Group - Global
	Security Group - Global

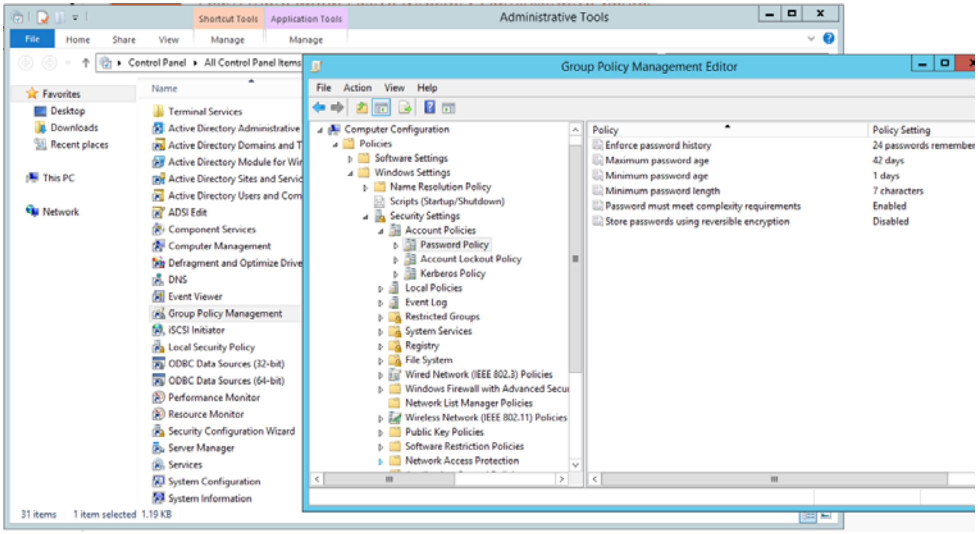
Create in: sam.com/

Name: ABB Freelance OU

☑ Protect container from accidental deletion

Create OU

- Configure password policies in group policy: Launch the Administrative Tool and configure the password age, password complexity, and password length, etc.



Policy	Policy Setting
Enforce password history	24 passwords remember
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Configure Password Policy

- – Maximum password age means the period of time that a password can be used before the system requires the user to change it. Configure the maximum password age and the minimum password age accordingly;
- – Password must meet complexity requirements means that passwords contain characters from at least three of the following four categories: upper case letters, lower case letters, westernized Arabic numerals, and non-alphanumeric;
- – Minimum password length sets the minimum number of characters for a password. The minimum password length is 8 characters. If greater security is needed, the minimum password length can be set to a maximum of 14 characters.

- Assign domain to every computer with Freelance Engineering, Freelance Operations or Formulation installed.

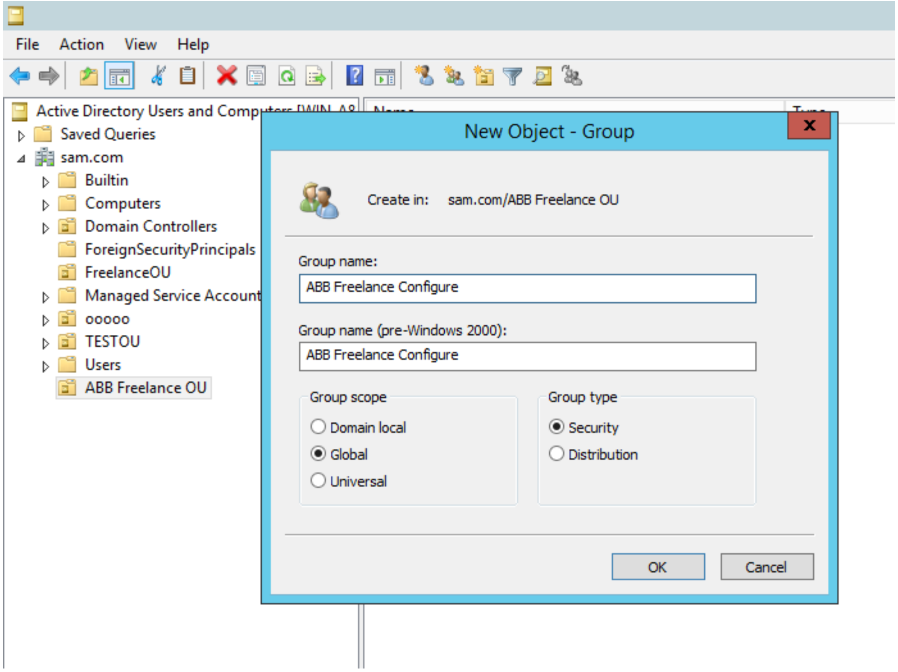
After user completes the group policy, right click menu and select Group Policy Update in the Group Policy Management of Domain Controller to update all the domain computers immediately.

Create groups on domain server

In Freelance system, the permissions are granted to security groups rather than to individual users. Users that are added to the groups assume the permission of that group.

- Create Groups. Right click on the OU, and select New > **Group**, input the group name, choose **Global** in Group scope and **Security** in Group type, then click **OK** to complete.

Please refer to the following section for the group name and the corresponding permissions.



Create in: sam.com/ABB Freelance OU

Group name: ABB Freelance Configure

Group name (pre-Windows 2000): ABB Freelance Configure

Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

Create Group

Group Privilege

As the privilege group is used to control the permissions for Freelance, users are suggested to create the groups according to the different permissions. Refer to the table below for the detailed group type.

Among the groups in the table, the name of the privilege groups, including ABB Freelance Configure, ABB Freelance Commissioning, ABB Freelance Extended Diagnostic, and ABB Freelance Basic Access are fixed. While for the user groups, the names are customized. The format to customize the user group is ABB Freelance Group <name of the group>, e.g.: ABB Freelance Group Guest. Users can create different user groups, but one user has to be in and should only be in one user group.

The <name of the group> may have a maximum length of 32 characters. It must not contain any other special characters than those allowed by Windows. The following Windows-compliant rules apply:

Names of groups must not solely consist of dots and/or spaces.

The following special characters are permissible:
\/” [] : | <>+=;,?*@

Group Name	Group Type	Description
ABB Freelance Configure	Privilege Group	Members are allowed to enter the configuration mode in Freelance Engineering and edit the project configuration.
ABB Freelance Commissioning	Privilege Group	Members are allowed to enter the commissioning mode in Freelance Engineering and, for example, establish the connection to process stations and download configuration.
ABB Freelance Extended Diagnostic	Privilege Group	Members are allowed to enter the extended diagnostic mode in Freelance Operations and, for example, operate device parameters and launch DTMs on Freelance Operations.

Group Name	Group Type	Description
ABB Freelance Basic Access	Privilege Group	All Freelance users are required to be added to this group, otherwise the Freelance will not judge the user account as a Freelance User.
ABB Formulation View	Privilege Group	This group is for Formulation only. User in this group is allowed to see all recipe information. No change is permitted.
ABB Formulation Operate	Privilege Group	This group is for Formulation only. User in this group is allowed to create, check, modify, download, delete Control Recipe.
ABB Formulation Approve	Privilege Group	This group is for Formulation only. User is this group is allowed to sign the approval of a Master Recipe.
ABB Freelance Group Guest	User group	Customized group. Group name follows pattern ABB Freelance Group <name of the group>.

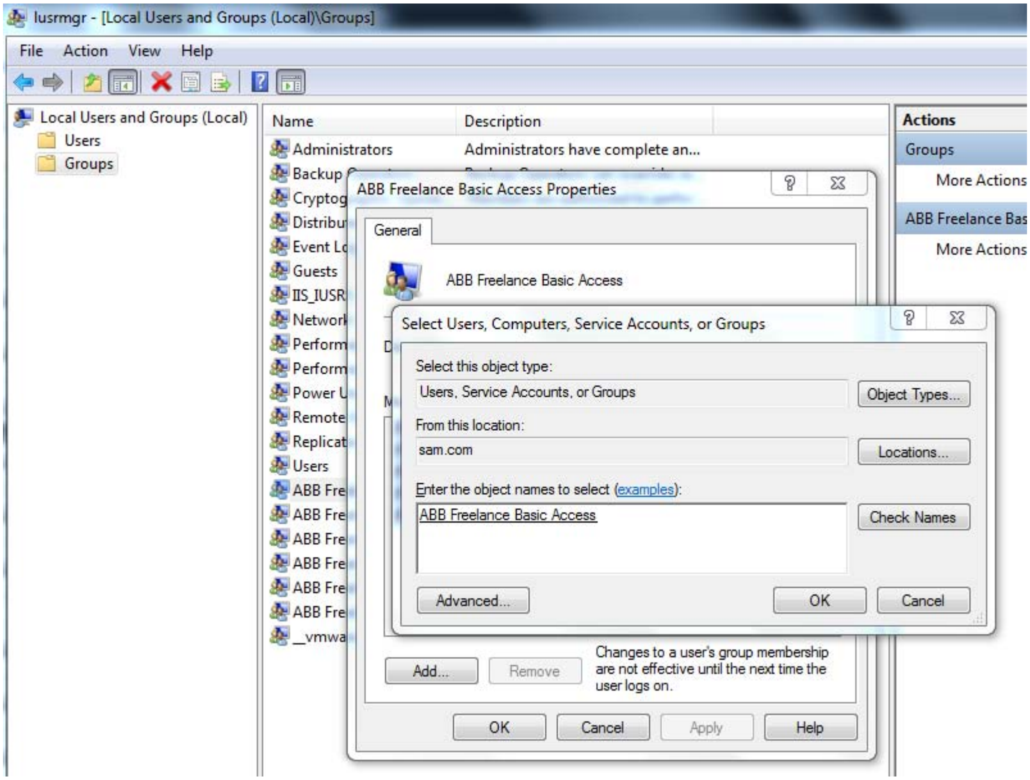
The three Formulation groups are only for Formulation users using Extended User Management. For more information about Formulation user access, please refer to the Engineering Manual - Formulation.

Permission Activation

After user creates the domain groups in the domain server, it is required to activate ABB Freelance Basic Access group on the local engineering station before user can operate the Freelance system with the domain account.

- Press WINDOWS + R (hot-key) to pop up the Run window,
- Type lusrmgr.msc and hit **Enter** to go to the Local Users and Groups interface.

- Click **Groups** in the left panel and find the group of ABB Freelance Basic Access,
- Double click on the group and hit **Add**,
- Input the domain group of ABB Freelance Basic Access, click **Check Names** and type in the domain user name and password as it requires.



Select this object type:
Users, Service Accounts, or Groups

From this location:
sam.com

Enter the object names to select (examples):
ABB Freelance Basic Access

Changes to a user's group membership are not effective until the next time the user logs on.

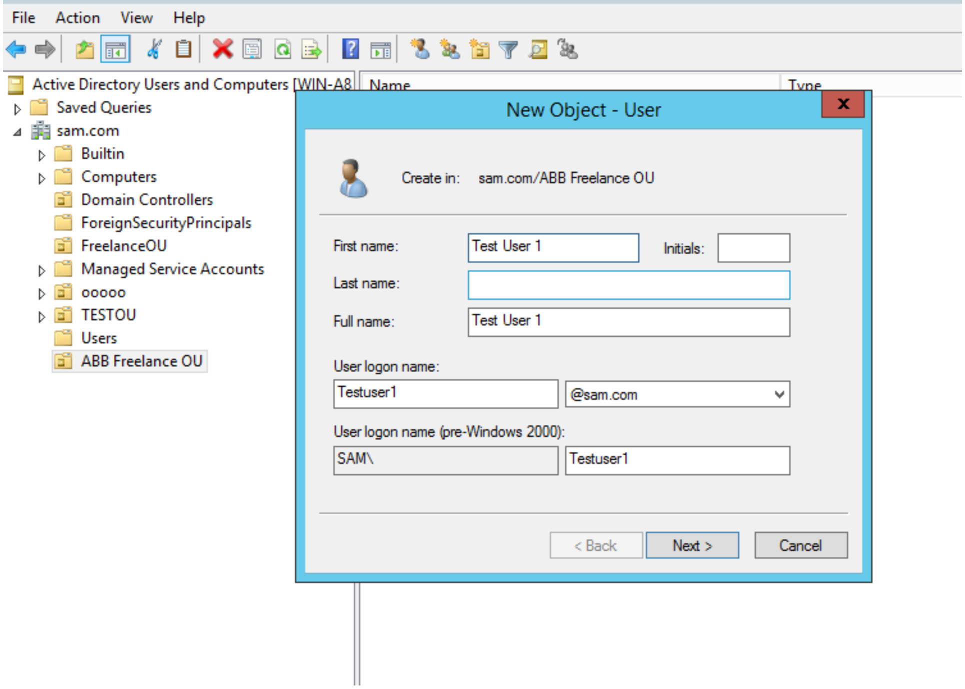
Add Domain Group to Local

- Click **OK** to save the settings and reboot the computer for the settings to take effect.

Without adding this domain group of ABB Freelance Basic Access to the local, domain user will encounter the error of insufficient permissions to access the Freelance Data, neither can user operate in Freelance system.

Create users on domain server

- Create Users. Right click on the OU, select **New** > **User**, and input the customized user name and click **Next** to continue.



Create in: sam.com/ABB Freelance OU

First name: Test User 1

Initials:

Last name:

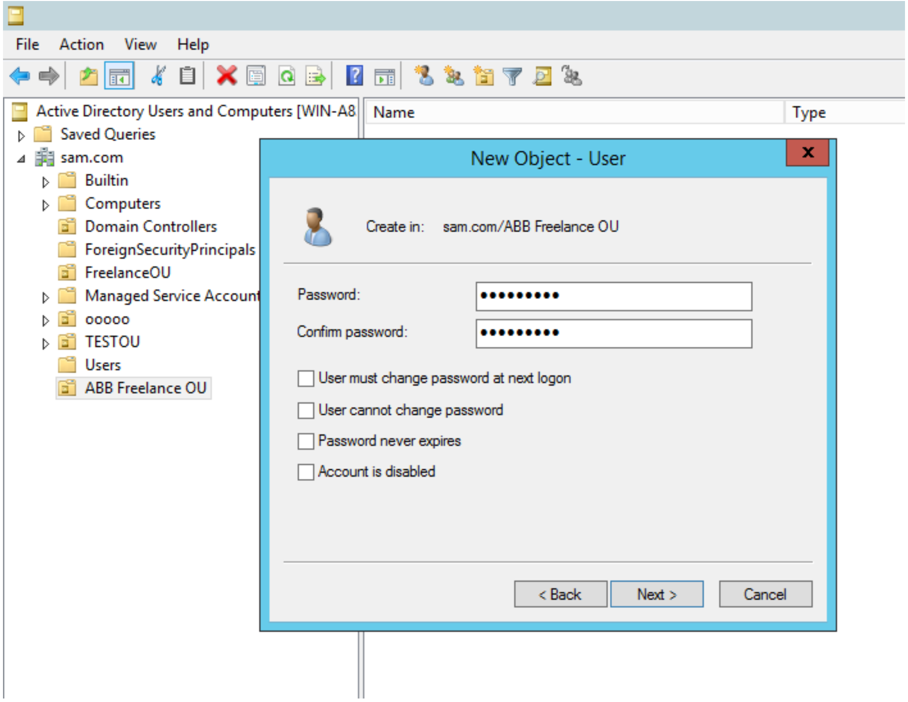
Full name: Test User 1

User logon name: Testuser1 @sam.com

User logon name (pre-Windows 2000): SAM\ Testuser1

Create User

- Configure the user password. Input the user password and confirm the password in the pop-up dialog box. The password length and complexity has to meet the requirement as you set in the group policy. Check the checkbox(es) according to the user requirement.



Create in: sam.com/ABB Freelance OU

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

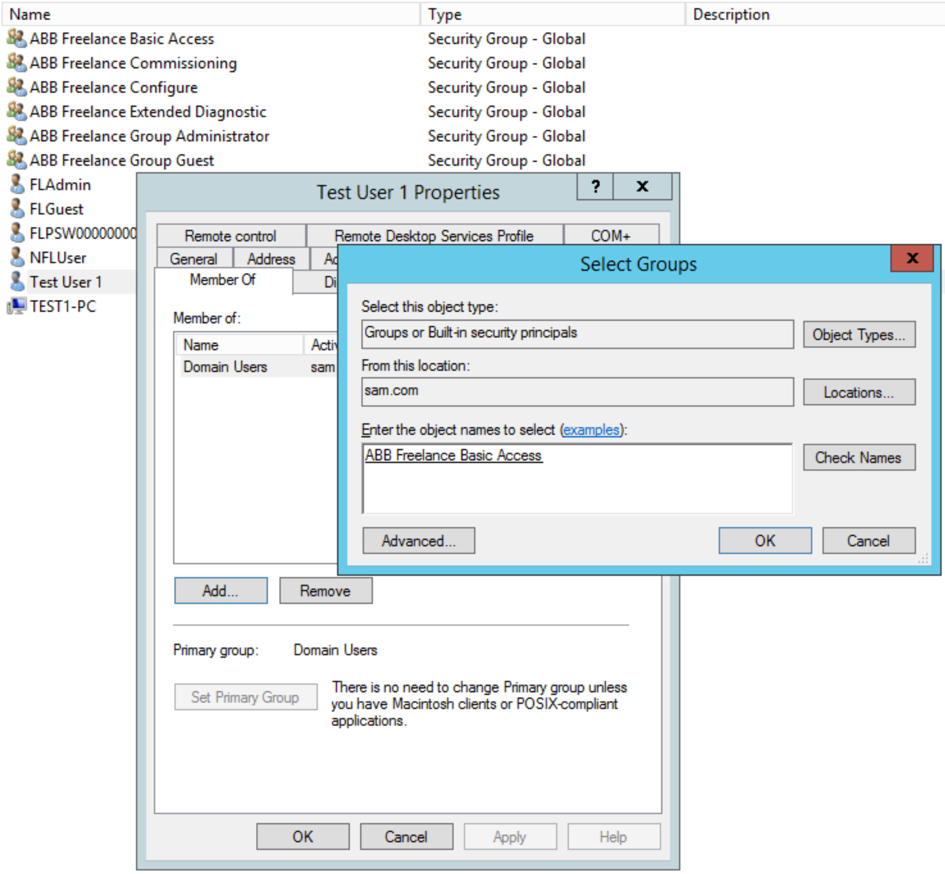
Configure User Password

Assign users to the group

- Assign the created users to the specified group. Right click on the created user, and select **Properties**.
- Go to the **Member** tab and input the group name.
- Click **Check Name**, the system will judge the group name automatically to see if the group name is correct, then click **OK** to complete.
- Add the other users by repeating the steps above.

Every user has to be added to the group of ABB Freelance Basic Access and one of the user groups.

A user shall be belong to only one customized group for the system to read and judge the user permissions clearly.



Name	Type	Description
ABB Freelance Basic Access	Security Group - Global	
ABB Freelance Commissioning	Security Group - Global	
ABB Freelance Configure	Security Group - Global	
ABB Freelance Extended Diagnostic	Security Group - Global	
ABB Freelance Group Administrator	Security Group - Global	
ABB Freelance Group Guest	Security Group - Global	
FLAdmin		
FLGuest		
FLPSW00000000		
NFLUser		
Test User 1		
TEST1-PC		

Test User 1 Properties

Member of:

Name	Acti
Domain Users	sam

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Select Groups

Select this object type: Groups or Built-in security principals

From this location: sam.com

Enter the object names to select (examples): ABB Freelance Basic Access

Add User to Group

After completing the allocation of created users to the desired groups, users are now able to login to the Freelance Engineering and Freelance Operations with the domain accounts.

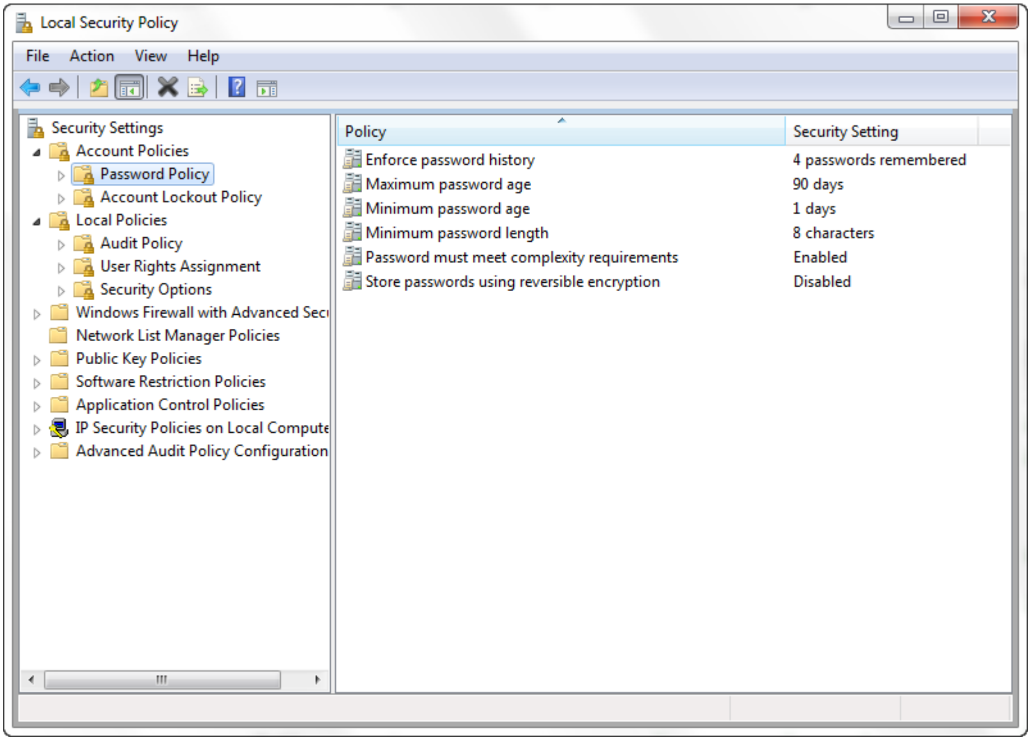
If a user is added to both ABB Freelance Basic Access group and Windows Administrator group, it is suggested that user reboot the PC before login.

2.2.3 Use local account

If the user does not want to use the domain, or user's computer is not configured as a domain computer, user can select to login to Freelance Engineering or Freelance Operations with a local account. Logging in with a local account, the central password management function is invalid, user needs to configure the password requirement via the local security policy editor in the local computer for better data security.

Configure local security policy

- Log on to the computer with administrative rights.
- Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy** to open the console.
- (Optional) Or user can just simply click **Start**, and type "gpedit.msc" in the search field of the Windows start menu to find the local group policy editor console. Then go to **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Account Policies**.
- Go to **Account Policies** > **Password Policy**, and configure the password requirements according to your demand, including password age, password length, password complexity requirements, etc.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
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	4 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Local Security Policy

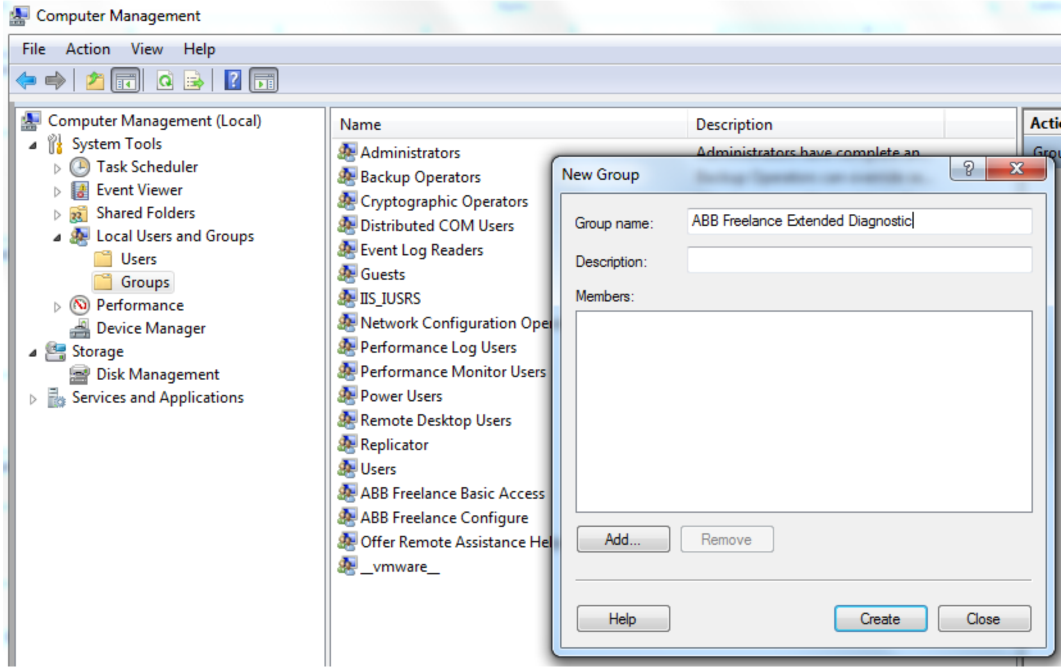
- Complete the password settings and close the local security console.

Create local groups

- Right click **My Computer** and select **Manage**.
- Click **Local Users** and **Groups** in the left panel.
- Click **Groups** and right click on the right panel to select New Group...
- Input the group name in the group name field and click **Create to complete**.

During the installation of Freelance, the system creates the ABB Freelance Basic Access group automatically. Except for this one, the other privilege group needs to be created as the steps above, and the privilege group names for local are same with the ones for the domain, which are ABB Freelance Configure, ABB Freelance

Commissioning, and ABB Freelance Extended Diagnostic. And the user group name shall also follows the pattern of ABB Freelance Group <name of group>.



Group name: ABB Freelance Extended Diagnostic

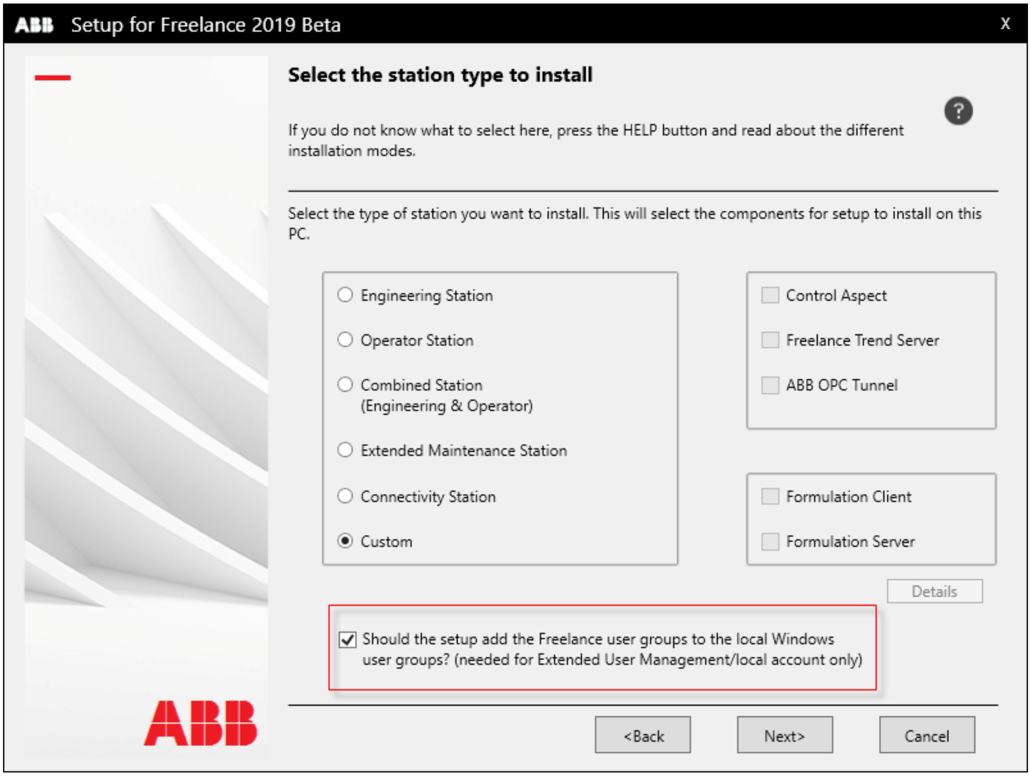
Description:

Members:

Create Local Group

If user enables the option of “Should the setup add the Freelance user groups to the local Windows user groups (needed for Extended User Management /local account only)” during the Freelance installation, the system creates the groups automatically, including ABB Freelance Basic Access, ABB Freelance Commissioning, ABB Freelance Configure, ABB Freelance Extended Diagnostic, and ABB Freelance Group GUEST.

Local group privilege



Setup for Freelance 2019 Beta

Select the station type to install

If you do not know what to select here, press the HELP button and read about the different installation modes.

Select the type of station you want to install. This will select the components for setup to install on this PC.

- ○ Engineering Station
- ○ Operator Station
- ○ Combined Station (Engineering & Operator)
- ○ Extended Maintenance Station
- ○ Connectivity Station
- ● Custom

- □ Control Aspect
- □ Freelance Trend Server
- □ ABB OPC Tunnel

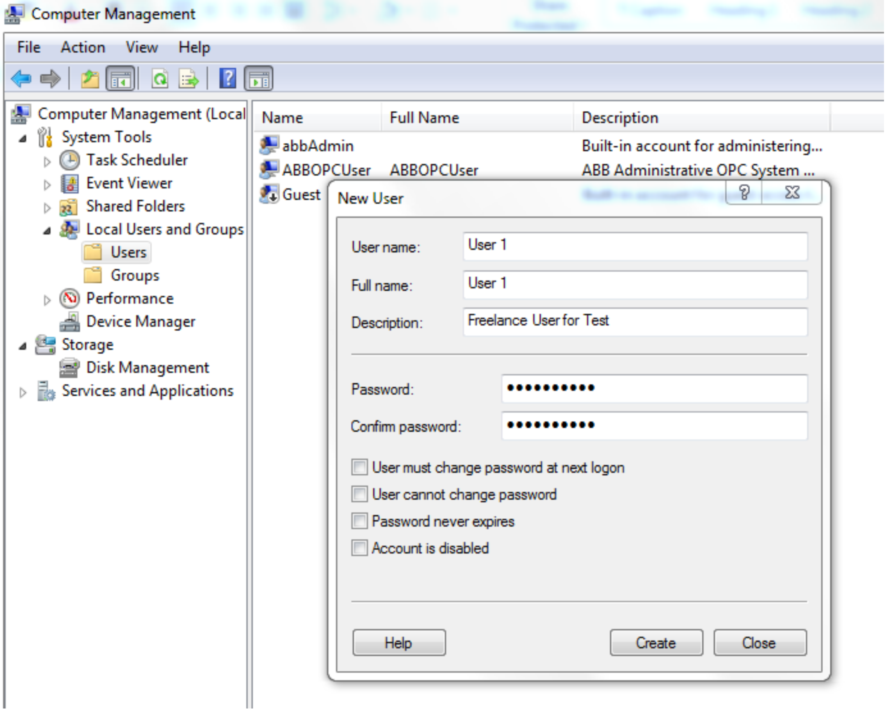
- □ Formulation Client
- □ Formulation Server

☑ Should the setup add the Freelance user groups to the local Windows user groups? (needed for Extended User Management/local account only)

The local group privilege is the same as the group privilege in domain, please refer to Group Privilege on Page 16 for details.

Create local users

- Right click **My Computer** and select **Manage**.
- Click **Local Users** and **Groups** in the left panel.
- Click **Users** and right click on the right panel to select **New User....**
- Input the user customized password, click **Create** to complete. Please note that the password has to meet the password requirement configured in the Local Security Policy.



Name	Full Name	Description
abbAdmin		Built-in account for administering...
ABBOPCUser	ABBOPCUser	ABB Administrative OPC System ...
Guest		

User name: User 1

Full name: User 1

Description: Freelance User for Test

Password: •••••••••••

Confirm password: •••••••••••

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

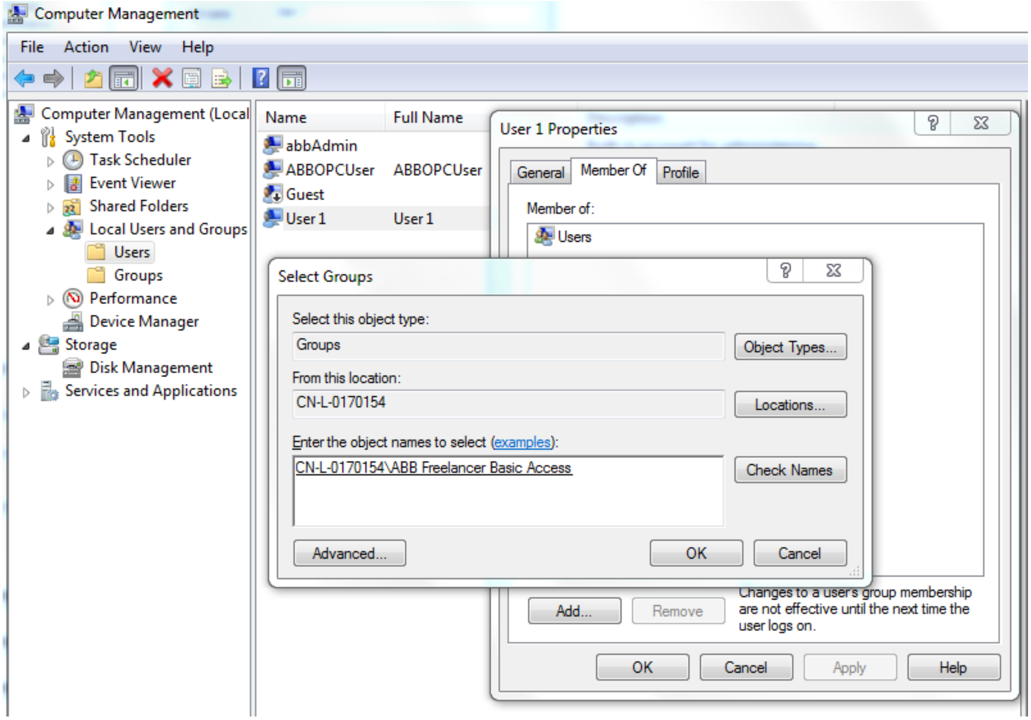
Create Local User

Assign user to the group

- Right click on the user and select **Properties**.
- Click **Member of tab** and go to **Add**.
- Input the Group Name and click **Check Name**, the system will judge the group name automatically to see if the group name is correct, and click **OK** to complete.

Every user has to be added to the group of ABB Freelance Basic Access.

A user shall belong to only one customized group.



Select this object type: Groups

From this location: CN-L-0170154

Enter the object names to select (examples): CN-L-0170154\ABB Freelancer Basic Access

Changes to a user's group membership are not effective until the next time the user logs on.

Assign Local User to Group

- Add the other users by repeating the steps above.

After the local accounts are successfully configured, users are able to login to the FO/FE with the local accounts.

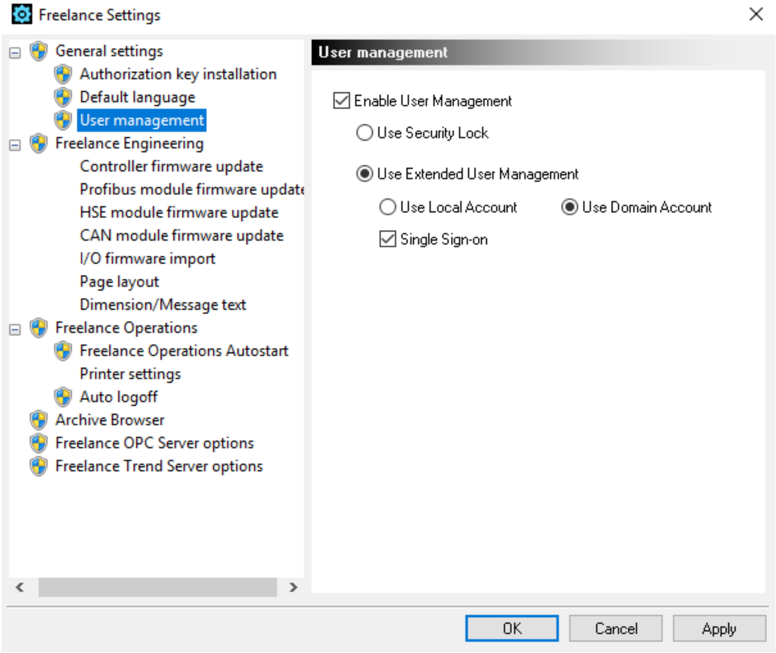
If you would like the created user has configuration rights in Freelance Settings, you have to add the user to the Administrator group.

If a user is added to both ABB Freelance Basic Access group and Windows Administrator group, it is suggested that user reboot the PC before login.

2.2.4 Single Sign-on

The Single Sign-on function provides to the user an option to login to the system automatically after you launch Freelance Engineering, Freelance Operations, or

Formulation. The user can find the Single Sign-on available by selecting **User Management > Enable User Management** in Freelance Settings.


Freelance Settings
General settings
Authorization key installation
Default language
User management
Freelance Engineering
Controller firmware update
Profibus module firmware update
HSE module firmware update
CAN module firmware update
I/O firmware import
Page layout
Dimension/Message text
Freelance Operations
Freelance Operations Autostart
Printer settings
Auto logoff
Archive Browser
Freelance OPC Server options
Freelance Trend Server options
OK
Cancel
Apply

User management

☑ Enable User Management

○ Use Security Lock

● Use Extended User Management

○ Use Local Account ● Use Domain Account

☑ Single Sign-on

Enable Single Sign-on

After Single Sign-on is enabled, it works only when the selected login account is consistent with the Windows login account. Example: If the user selects **Use Domain Account** in Freelance Settings, the user has to use the domain account to login the Windows system for Single Sign-on to take effect.

Here is a list of lists several situations which the user can refer to.

Use Local Account	Use Domain Account	Single Sign-on Enabled	Windows Login Account	FE/FO/Formulation User Status
√	-	√	Local Account	Login FE/FO/Formulation automatically
√	-	√	Domain Account	Auto login failed because of the account conflicts

Use Local Account	Use Domain Account	Single Sign-on Enabled	Windows Login Account	FE/FO/Formulation User Status
-	√	√	Domain Account	Login FE/FO/Formulation automatically
-	√	√	Local Account	Auto login failed because of the account conflicts.

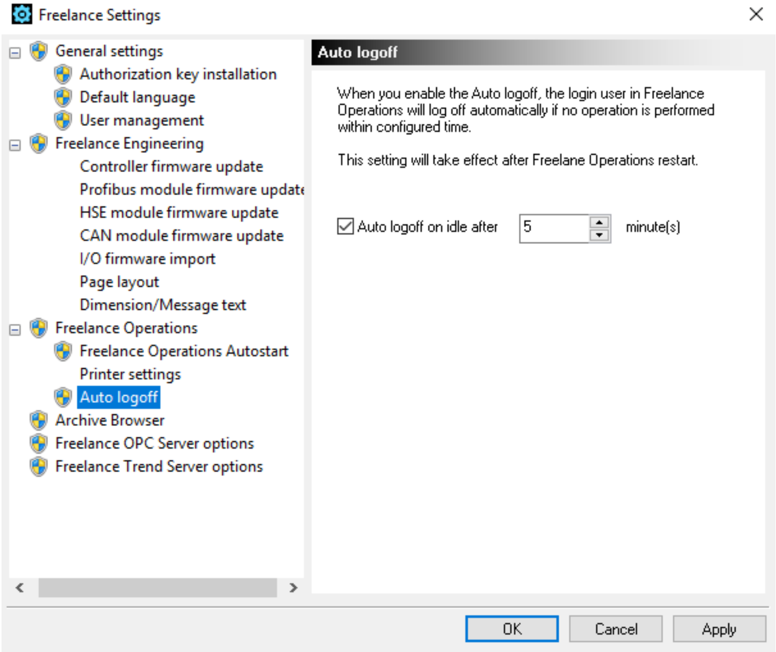
2.2.5 Auto Logoff

The check(√) symbol in the table stands for using the current account, and the hyphen(-) stands for current account is not selected.

Auto Logoff function is also a part of the User Management. With Auto Logoff enabled, a logged-in user will be logged over to a read-only state in Freelance Operations if the user was inactive for a configured time.

Auto Logoff configuration

- Launch FreelanceSettings and click the left node Freelance Operations.
- Check the checkbox to enable the function.
- Configure the Auto Logoff time, which by default is 5 minutes. The value ranges from 1 minute to 180 minutes.
- Click **Apply** to save the settings.


Freelance Settings
General settings
Authorization key installation
Default language
User management
Freelance Engineering
Controller firmware update
Profibus module firmware update
HSE module firmware update
CAN module firmware update
I/O firmware import
Page layout
Dimension/Message text
Freelance Operations
Freelance Operations Autostart
Printer settings
Auto logoff
Archive Browser
Freelance OPC Server options
Freelance Trend Server options
OK
Cancel
Apply

Auto logoff

When you enable the Auto logoff, the login user in Freelance Operations will log off automatically if no operation is performed within configured time.

This setting will take effect after Freelane Operations restart.

☑ Auto logoff on idle after 5 minute(s)

Auto Logoff

Re-login after Logoff

If Freelance Operations detects that the current idle time is greater than the configured idle time, the user will be logged over to a read-only user. All the popup windows will be closed, but the current view will remain. The user has to re-login to gain the rights to operate the system.

2.2.6 Forbidden cross-credential login

With Extended User Management enabled, the user may come across the situation of using different credentials to login to the computer and the system. Considering the software working principles, the system will read the logged-in accounts, and deploy the permissions according to the settings in Freelance Settings.

Assuming the user is in a domain environment, there are two accounts available: Sam (Domain), and Sam (Local); the user can refer to the table below for a better understanding of the cross-credential login./

Use Local Account	Use Domain Account	Single Sign-on	Logged in Windows Account	Freelance Permission
√	-	-	Sam (Local)	Permission fetched from local
√	-	-	Sam (Domain)	Permission fetched from local
√	-	√	Sam (Local)	Permission fetched from local
√	-	√	Sam (Domain)	Auto login failed because the current windows account is not a local account
-	√	-	Sam (Local)	Permission fetched from domain
-	√	-	Sam (Domain)	Permission fetched from domain
-	√	√	Sam (Local)	Auto login failed because the current windows account is not a domain account
-	√	√	Sam (Domain)	Permission fetched from domain

The check(√) symbol in the table stands for using the current account, and the hyphen(-) stands for current account is not selected.

3 Security Lock

3.1 Security Lock – General description

Security Lock is an **auxiliary program** for the control system Freelance. It provides access control for **configuration** with Freelance Engineering and for **operation and observation** with Freelance Operations. The access control system can be implemented for an entire Freelance system with a single Security lock license.

It is possible, even **without Security lock**, to specify during configuration with Freelance Engineering application whether or not the operator at an operator station is allowed, for example, to alter a controller set-point. This specification influences the access rights for each operator on the operator station.

In contrast to this general specification, **with Security lock,** it is possible to give operator A permission to operate a controller but not operator B. A prerequisite is that the set-point has been marked with operator access in the controller parameter mask. Then with appropriate entries in the tag list, permission to operate the controller is given to operator A and denied to operator B.

In a system with Security Lock installed, users are required to **login** before using Freelance Engineering or Freelance Operations.

Security Lock is installed on each PC which is used in the Freelance. The installation is carried out by default when you run the Freelance installation package. User can enable Security Lock in Freelance Settings.

Technical limitations

After the installation of Security lock, the user GUEST is logged in Freelance components.

User GUEST has no rights, that means:

- User GUEST is not able to configure for Freelance Engineering

Up to 16 user access groups and up to 1000 users can be created in the system. The different access rights like Configuration, Commissioning, Security Lock configuration and Extended diagnostic are assigned to the groups. Each user can be assigned to one of the access groups.

Number of access groups (user profiles)	maximum 16
Number of users	maximum 1000

3.2 Security Lock operations

3.2.1 On the Engineering station

- Launch Security lock on the Engineering station (PC with Freelance Engineering).
- Define user groups and specify their rights with Security Lock on the Engineering station.
- Create users and assign them to the groups.
- Save the Security lock data. The data are stored in the file **<windows dir>\DIGIMAT.UID**, a backup copy can be stored at any location as **<name>.UID**.
- Assign groups to a project with Freelance Engineering (**Project Tree** > **Edit** > **User groups**).
- Use Freelance Engineering application to specify for all elements of the Freelance operator stations, which access groups have the rights to observe and/or operate on it. This can be done for all elements in the project tree and

tag list separately or on more global level. Details are described in the following chapters.

3.2.2 On the Operator stations

- Launch Security Lock on all operator stations (PCs with Freelance Operations).
- Transfer the Security Lock configuration for Groups, Users and Access rights to the Freelance Operations PCs. Copy the default file **<Windows>/DIGIMAT.UID** or the user specific file **xxx.UID** to all operator station PCs.

The target file at all operator stations must be **<windows dir>\DIGIMAT.UID**, otherwise an error message appears when Freelance Operations is started.

3.2.3 Call-up of Security Lock

There are three possibilities to call up Security Lock:

Call-up from Freelance Engineering

Freelance Engineering > **Options** > **Run Security Lock**

Precondition: The user logged in to Freelance Engineering application must be authorized to configure Security Lock.

Call-up from Freelance Operations

Freelance Operations > **Tools** > **Run Security Lock**

Precondition: The user logged in to Freelance Operations must be authorized to configure Security Lock.

Call-up from the Windows start menu

Windows 7:
Start > **All Programs** > **ABB** > **Freelance <version>** > **Security Lock**

Windows 10:
Start > **ABB** > **Security Lock**

3.2.4 Security Lock password

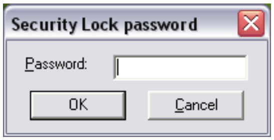
Initial password

When the program is first run, the initial password is requested; is password should be changed.

The Initial password required to run Security Lock for the first time after installation is: **admin**

General note on Security Lock password

The password must be given each time the Security Lock configuration dialog is started.



di4006uk.bmp

The password is masked using ******* to prevent it from being compromised.

Changing the Security Lock password

The password of the Security Lock application can be changed at any time:

Security lock > **File** > **Password**

In order to set a new password, the old password must be re-entered. The new password must then be typed in twice identically. Clicking **OK** stores the new password immediately; it must then be used for future starts of the Security Lock configuration dialog.

If you forget the password, please contact our technical service personnel.

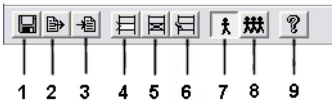
3.2.5 User interface

Menu overview Security lock

File	Save	Save the current data to file
	Backup	Create backup file of the current data
	Restore	Restore data from backup file
	Password	Change the password of security lock
	Exit	Exit security lock
Edit	Add	Add a new entry (User or Group)
	Delete	Delete the selected entry (User or Group)
	Modify	Modify the selected entry (User or Group)
	Rename	Rename the selected entry (User or Group)
	Set password	Change user password
View	Users	Show user data
	Group	Show group data
	Toolbar	Show/Hide the toolbar
	Status bar	Show/Hide the status bar

Description of the toolbar

All important functions are represented by buttons in the toolbar.



option in security lock window.png

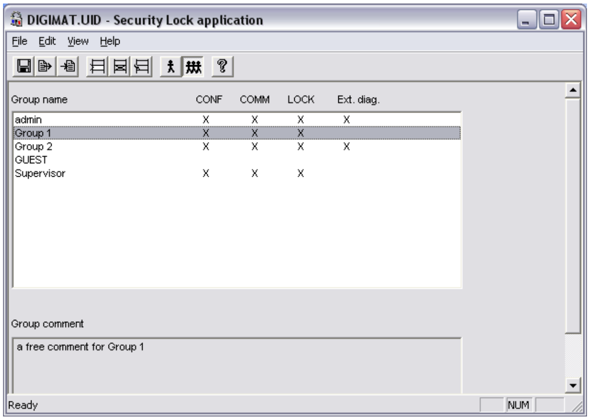
Item	Description
1	Save the active document
2	Make a backup of the current file

Item	Description
3	Restore the current file
4	Add a new entry
5	Delete the selected entry
6	Edit the selected entry
7	Display user data
8	Display group data
9	Information on Security lock

3.2.6 Configuring groups and users

Group data and system rights

Security Lock > **View** > **Groups**



Group name	CONF	COMM	LOCK	Ext. diag.
admin	X	X	X	X
Group 1	X	X	X	
Group 2	X	X	X	X
GUEST				
Supervisor	X	X	X	

Group comment

a free comment for Group 1

Ready NUM

di4009uk.bmp

Group name Defined by the Security Lock user.

CONF Members of the group are allowed to enter the configuration mode in Freelance Engineering and edit the project configuration.

COMM Members of the group are allowed to enter the commissioning mode in Freelance Engineering and, for example, establish connection to process stations and download configuration.

LOCK Members of the group are allowed to start Security Lock.

Ext. diag. Members of the groups are allowed to enter the Extended diagnostic mode in Freelance Operations and, for example, operate device parameters and launch DTMs on Freelance Operations.

Group entries can be modified, deleted or created with the **Edit** menu or with the appropriate tool from the toolbar.

The group GUEST is always available and cannot be deleted.

Add a new group

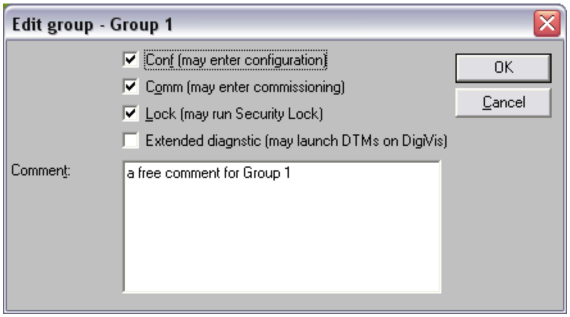
Select view mode **Group** > **Edit** > **Add** > Enter the name of the new group

Delete a group

Select view mode **Group** > **Edit** > **Delete** > Accept the message box

Modify group entries

Select view mode **Group** > **Edit** > **Modify**


Edit group - Group 1

☑ Conf (may enter configuration)
☑ Comm (may enter commissioning)
☑ Lock (may run Security Lock)
□ Extended diagnstic (may launch DTMs on DigiVis)

Comment: a free comment for Group 1

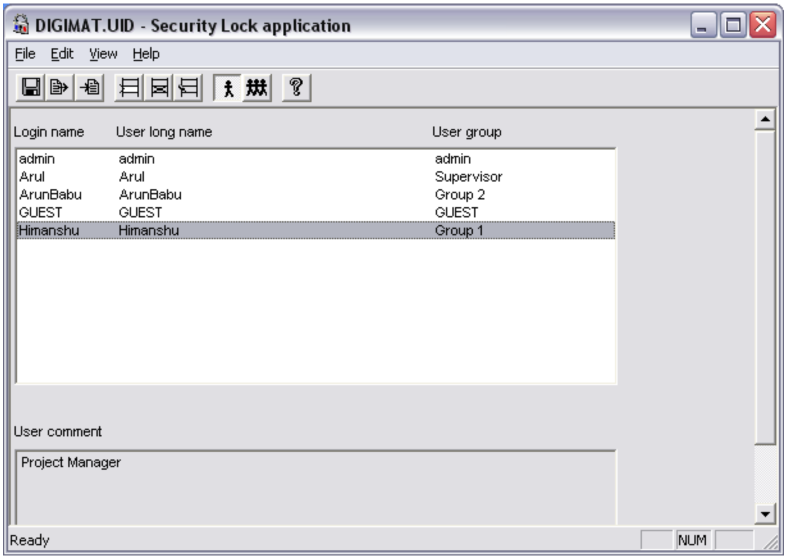
di4015uk.bmp

Edit the access rights by clicking the check boxes.

Enter text to comment and describe the group specification (optional).

User data

Security Lock > **View** > **Users**



Login name	User long name	User group
admin	admin	admin
Arul	Arul	Supervisor
ArunBabu	ArunBabu	Group 2
GUEST	GUEST	GUEST
Himanshu	Himanshu	Group 1

User comment

Project Manager

di4010uk.bmp

User entries can be edited, deleted or created with the **Edit** menu or with the appropriate tool from the tool bar.

The user GUEST is always available and cannot be deleted.

A user obtains the system rights of the group assigned to him/her.

Login name Name of the user, to be used for logging in into system; up to 8 characters.

User long name
Arbitrary text; preferably the exact identification of the user.

User group Name of the group the user is assigned.

Each user can be assigned to one group only.

Add a new user

Edit > **Add** > Enter a new user

Delete an user

Select user entry > **Edit** > **Delete**

Modify user entries

Select user entry > **Edit** > **Modify**

Change user password

Default **User password** is initially set to the corresponding login name. The password can be changed here in Security Lock application and also by the user itself, either in Freelance Operations or in Freelance Engineering.

If a user changes his password, the new password is not changed for all PCs in the Freelance system. The user has to change his password on each PC in the Freelance system, if he wants to have the same password everywhere as the configuration of Security Lock is stored locally. See also Security Lock and several PCs on Page 47.

If necessary the supervisor can set a new password for a user in Security Lock:.

Security Lock > **Edit** > **Set password**

3.2.7 Security Lock on Operator station

Group and user data must available on each operator station. Instead of repeating the Security Lock configuration work on each PC, the configuration data can be transferred by copying the dat file:

Copy the file **<windows dir>\DIGIMAT.UID** from the Freelance Engineering PC to all operator stations. See also Security Lock and several PCs on Page 47.

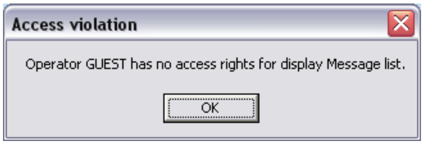
On the Freelance operator station, the operator sees the following from Security lock:

- Each user must log in before being allowed to perform any operations.
- The user name always appears in the status line.
- Entries or operator actions recorded in the signal sequence log can include the login name.

Standard user names

NOLOCK	No Security Lock license
GUEST	No user logged in, for example, just after start of Freelance Operations
SYSTEM	System-initiated operation events (may appear in the signal sequence log

When a user without proper authorization attempts to operate a display, the following message box will pop up:



Access violation

Operator GUEST has no access rights for display Message list.

di4014uk.bmp

Additionally each display and faceplate will indicate whether or not the logged-in user has operating rights for this display - by means of an open or a closed padlock.

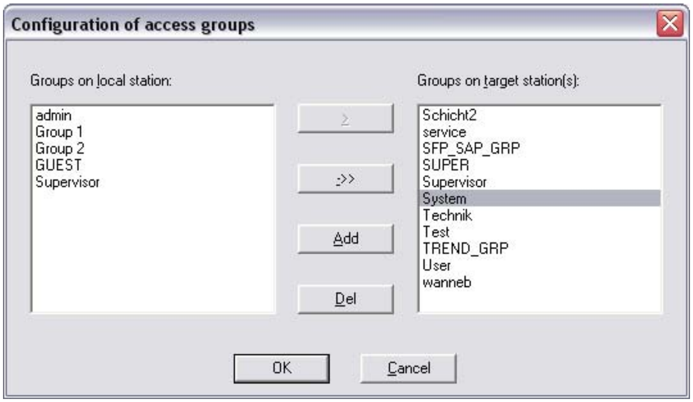
3.2.8 Access rights configuration for the project

Assign user groups to the project

Different user groups can be defined in Security lock. In a first step, the user groups must be assigned to the project.

The project tree has a submenu for configuration of access groups.

Edit > User Groups



Configuration of access groups

Groups on local station:

admin
Group 1
Group 2
GUEST
Supervisor

Groups on target station(s):

Schicht2
service
SFP_SAP_GRP
SUPER
Supervisor
System
Technik
Test
TREND_GRP
User
wanneb

di4005uk.bmp

On the left side the locally configured groups are listed, the right side shows the groups which are used in the project.

>	The selected local groups are added to this project.
>>	All local groups are added to this project.
ADD	Add a new access group to this project. For adding user to this new group, this group must be configured in Security lock application again.
DEL	Delete a user group from the project.

Assign access rights to tags

For each element of an operator station, the access rights of the project user groups can be configured.

Access rights for faceplates are specified in the tag list of Freelance Engineering.

Project tree in configuration mode > **System** > **Tag list**

Select one or more tags by dragging the mouse over them (with the mouse button pressed)

Edit > **Access rights**

Assign access rights to system display, message list and hint list

Access rights to **system displays**, **message list** or **hint list** are specified in the project tree of Freelance Engineering:

Project tree in configuration mode

Select Operator Station node or elements under Operator Station node in Project tree

Edit > **Access rights**

Assign access rights to displays and logs

Access rights to **displays and logs or whole operator stations** are specified in the project tree of Freelance Engineering:

Project tree in configuration mode

Select one or more elements in the Project tree

Edit > **Access rights**

Inheritance hierarchy of access rights

On inserting a new object, this object will obtain the access rights of its next-higher project tree node (parent node) as a default entry.

The following inheritance hierarchy has been established in order to simplify the configuration:

- On inserting a new object, this object will obtain the access rights of its next-higher project tree node (parent node) as a default entry.

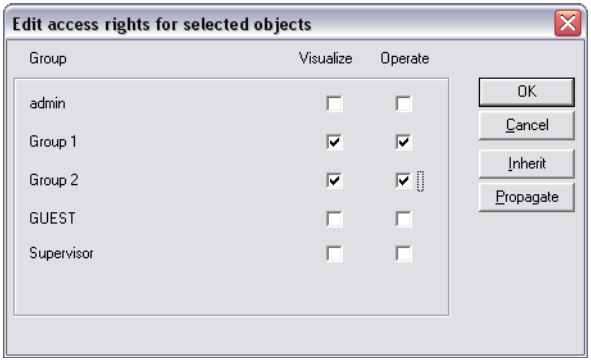
- An existing object has to get the access rights that applies to its next-higher project tree node (parent node):

Select an object > **Edit** > **Access rights** > **INHERIT**

- The rights currently applying to a project tree node can be forcibly assigned to all of the objects under it (it’s children):

Select an object > **Edit** > **Access rights** > **PROPAGATE**

When an object is moved or copied, its rights (or those of the copy), remain unchanged.


Edit access rights for selected objects

Group	Visualize	Operate
admin	□	□
Group 1	☑	☑
Group 2	☑	☑
GUEST	□	□
Supervisor	□	□

di4012uk.bmp

✓ Access right applies to all selected objects (displays or tags)

▨ Access right applies to only some of the selected objects.

□ Access right does not apply to any of the selected objects (displays or tags).

INHERIT Set the rights of the selected objects to those of the project tree node above it.

PROPAGATE Force the currently configured access rights applying to the selected project tree node to apply to all of the objects below it (child objects).

3.2.9 Security Lock and several PCs

If a user changes his password on a PC, the new password is not changed for all PCs in the Freelance system. The configuration of Security lock (user names, passwords and the assigned user groups) is stored in a file called DIGIMAT.UID in the Windows directory.

The user has to change his password on every PC in the Freelance system, if he wants to have the same password everywhere.

Alternatively copying the file DIGIMAT.UID to the other PCs will change the password. This is however not possible if the operator station is active.

The configuration of **Security Lock** is local.

Index

—

www.abb.com/freelance
www.abb.com/controlsystems

—

We reserve the right to make technical changes to the products or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not assume any responsibility for any errors or incomplete information in this document.