SIEMENS SIMATIC WINCC FLEXIBLE 2008 SECURITY HARDENING GUIDE

16 JUN 2013

PUBLIC BETA

TABLE OF CONTENTS

LEGAL NOTES....6
1. OS CONFIGURATION....7
1.1 Use a compatible Windows version....7
1.2 Ensure compatibility of WinCC flexible 2008 with other components and software....7
1.3 Ensure appropriate Windows language settings....7
1.4 Install the latest Windows updates....8
1.5 Disable installation of unsigned drivers and files after WinCC flexible is installed....8
1.6 Use Data Execution Prevention feature....8
1.7 Restrict membership in system groups....8
1.8 Ensure WinCC flexible rights are configured appropriately....9
1.9 Disable Windows hotkeys....9
1.10 Disable remote access to computer....10
1.11 Enable User Account Control....10
1.12 Configure Windows Firewall authorized components list....10
1.13 Disable access to external networks....10
1.14 Do not use Novell Netware....10
2. DBMS CONFIGURATION....11
2.1 Use Microsoft SQL 2005....11
2.2 Ensure installation of the latest security updates for Microsoft SQL 2005....11
2.3 Use strong system administrator password....11
2.4 Use strong password for DBMS access....11
2.5 Provide SIMATIC HMI users with SQL Server access rights....11
3. ADDITIONAL MEANS OF PROTECTION....12
3.1 Ensure the installed antivirus is compatible....12
3.2 Use up-to-date antivirus software....12
4. SIMATIC SIEMENS WINCC FLEXIBLE SYSTEM PARAMETERS....12
4.1 Ensure the latest updates are installed....12
4.2 Remove the supplementary SIMATIC ProAgent application....12
4.3 Remove the supplementary SIMATIC ProSave application....13
4.4 Configure WinCC flexible Runtime Loader....13
4.5 Ensure autostart of the WinCC flexible Start Center application and project....14
5. RUNTIME SECURITY SETTINGS....14
5.1 Configure password aging options....14

5.2 Use strong passwords 15
5.3 Restrict the number of invalid login attempts 15
5.4 Disable login using password exclusively 15
5.5 Use access group hierarchy 15
5.6 Configure the idle time before automatic forced logoff 16
5.7 Require initial administrator's password change 16
5.8 Ensure appropriate settings are configured if SIMATIC Logon is used 16
5.9 Install SSL certificates 17
5.10 Ensure SIMATIC HMI HTTP\HTTPS Protocol settings are configured appropriately 17
5.11 Apply binding your HMI device to the controller 17
6. SIMATIC SIEMENS WINCC FLEXIBLE ACCESS SETTINGS 18
6.1 Change default administrator password for the project 18
6.2 Configure forced logoff for all users 18
6.3 Change default MiniWeb password 19
6.4 Change default Sm@rtServer passwords 19
6.5 Check and change Sm@rtServer forced access password 19
6.6 Store email password in the project only 19
6.7 Ensure access privileges are configured appropriately in WinCC Internet Settings 20
7. SM@RTSERVER SECURITY SETTINGS 21
7.1 Disable or provide correct Sm@rtServer settings (Remote Server) 21
7.2 Limit remote project management 21
7.3 Limit number of users with access to the workstation 21
7.4 Grant access only with operator confirmation 21
7.5 Restrict to pass settings for applets via URL 22
7.6 Restrict to pass files remotely 22
7.7 Configure Sm@rtServer (Remote Server) disabling and enabling together with Runtime 22
7.8 Do not use Sm@rtServer as a service 22
8. MINIWEB (HTTP) SECURITY SETTINGS 23
8.1 Disable MiniWeb (Web Server), if not necessary 23
8.2 Enable authentication for tags 23
8.3 Disable remote project loading for HMI panels 23
8.4 Configure MiniWeb disabling and enabling together with Runtime 24
9. OPC SERVER SECURITY SETTINGS 24
9.1 Disable OPC server if it is not used 24

9.2 Configure DCOM access rights 24
10. WEB SERVICE (SOAP) SECURITY SETTINGS 26
10.1 Disable or provide security for Web service (SOAP) 26
11. SMTP SECURITY SETTINGS 26
11.1 Ensure that email is secure 26
11.2 Configure a secure connection for email data exchange 26
12. LOGGING 27
12.1 Enable event logging in Sm@rtServer application 27
13. PROJECT MANAGEMENT 27
13.1 Disable hot keys in user interface 27
13.2 Configure protection against unauthorized access 27
14. WEB SERVER: HTML PAGES 28
14.1 Publish necessary tags only 28

LEGAL NOTES

1. OS CONFIGURATION

1.1 Use a compatible Windows version

Description:
Install WinCC flexible 2008 on those operating systems that are supported by the vendor.

How to fix:
To verify your Windows version is compatible, use the list http://support.automation.siemens.com/WW/llisapi.dll/csfetch/22055368/22055368_WinCC_flexible_compatibility_list_e.pdf.

Links:
http://support.automation.siemens.com/WW/llisapi.dll/csfetch/22055368/22055368_WinCC_flexible_compatibility_list_e.pdf

https://support.automation.siemens.com/kompatool/pages/main/index.jsf

1.2 Ensure compatibility of WinCC flexible 2008 with other components and software

Description:

Installation of excessive or incompatible with WinCC flexible 2008 products, OS components or Siemens software is not recommended by the vendor.
Note:
Parallel installation of WinCC flexible 2008 is possible with the following SIMATIC products: WinCC Basic V11, WinCC Comfort V11, WinCC Advanced V11 и WinCC v11 Professional, STEP 7 V5.4 or V5.5, STEP 7 Micro/WIN, STEP 7 10.5, STEP 7 11, WinCC V7.0 SP2.
How to fix:
To check the state of the installed components, go to Start -> Control Panel -> Add or Remove Programs -> Add/Remove Windows Components.
Links:

http://support.automation.siemens.com/WW/llisapi.dll/csfetch/22055368/22055368_WinCC_flexible_compatibility_list_e.pdf

1.3 Ensure appropriate Windows language settings

Description:

WinCC is supported only for operating systems with the following language interfaces:

- German
- English
- French
- Italian
- Spanish
- Multilingual User Interface (MUI)*.

*For MUI systems, the OS language should be English.

Note:
Installation of WINCC flexible on operating systems with unsupported languages is possible, but in this case some issues may occur (inappropriate rendering of screen fonts or instable performance of the product itself).

How to fix:
To verify that language settings are appropriate, check the system language: Start -> Control Panel -> Regional and Language Options.

1.4 Install the latest Windows updates

Description:
For maintaining Windows up-to-date security level, it is required to regularly check for and install all the latest hotfixes, marked by Microsoft as "critical" or "important" and checked by the enterprise IT specialists.
How to fix:
Ensure that all the latest OS updates have been installed.

1.5 Disable installation of unsigned drivers and files after WinCC flexible is installed

Description:
For appropriate performance of the WinCC flexible software on the Windows system it is necessary to disable the default check for signed drivers. Once WinCC Advanced TIA Portal is installed, the check for digital signature should be enabled.
How to fix:
To disable installation of unsigned drivers and files after WinCC flexible is installed, go to Start -> Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Security Options.
Check the configuration of the security option Devices: Unsigned driver installation behavior for Windows Vista, Windows XP, and Windows Server. For this option select "Silently succeed" or "Warn, but allow installation".

1.6 Use Data Execution Prevention feature

Description:
Use Data Execution Prevention (DEP) for all applications on your Windows system. DEP is an embedded security feature which does not allow an application to execute code from memory locations marked as being non-executable. Use of this feature allows preventing some attacks during which malicious code is stored in such memory locations (for example, during buffer overflow).
How to fix:
The feature can be disabled for the time when installation, maintenance or project creation is taking place. If WinCC flexible is used on continuing basis, Data Execution Prevention should be enabled for all programs.
Start -> Settings -> Control Panel -> System -> Advanced -> Performance -> Settings -> Data Execution Prevention. Select the option Turn on DEP for all programs and services except those I select.

1.7 Restrict membership in system groups

Description:
Control restrictions on membership in the system groups Administrator, Server Operators, and Power Users.
How to fix:
Ensure appropriate restrictions are imposed on membership in the specified groups.

1.8 Ensure WinCC flexible rights are configured appropriately

Description:
Once WinCC flexible is installed, the system automatically creates the following local groups (you can view them in the groups and users management window):

- SIMATIC HMI. Members of the group can create local projects, remotely manage and launch them, and also access them. By default this group includes a user who performs WinCC flexible installation and a local administrator. Administrator can add other members manually.
- SIMATIC HMI CS. Members of the group can only perform configuration, they cannot directly change components of the execution environment. By default this group is empty and reserved for future use.
- SIMATIC HMI Viewer. Members of the group only have read access to configuration and execution environment data. The group is mainly used for web publishing services accounts, e.g. for MiniMeb or Sm@rtServer operation.

Restrict members of this group only to those local users who are allowed to access WinCC flexible.
Note:
The developers and users of the execution environment components should belong not only to the SIMATIC HMI group, but also to a Windows group. Members of the SIMATIC HMI can only access projects, but not the operating system. To create a project, a developer should be the main user and the main user and the user of the of the SIMATIC HMI group.
In distributed systems, the newly-created WinCC flexible users should be added to the same groups. Moreover, a user on all computers should have the same password.
How to fix:
For adding users to the SIMATIC HMI group, local users should first be created (domain users can be added to the SIMATIC HMI group directly).
To create local users, go to Start -> Settings -> Control Panel -> Administrative Tools -> Computer Management -> Local Users and Groups -> Users. Via the context menu, open the New User dialog box and create an account for every user, who needs access to WinCC flexible.
Then, go to Local Users and Groups -> Groups -> SIMATIC HMI. Via the pop-up menu, open the Add Member dialog box and add users as members of SIMATIC HMI.
If domain is used, an additional global domain user group may be added as a SIMATIC HMI member. To do this:

- Domain administrator should create a global domain user group.
- The administrator should add users that are allowed to access WinCC flexible to the domain.

To create domain users, go to Start -> Settings -> Control Panel -> Administrative Tools -> Computer Management-> Local Users and Groups -> Users. Via the pop-up menu, open the New User dialog box. Create a user account for the global domain user group.
Then, go to Local Users and Groups -> Groups -> SIMATIC HMI.
Via the pop-up menu, open the Add Member dialog box and add the global domain user group as a member of SIMATIC HMI.

1.9 Disable Windows hotkeys

Description:
Once hotkeys are disabled, the following combinations will also be disabled in the execution environment:
- Win+U (open Utility Manager)
- Shift five times (toggle StickyKeys on and off)
- Right Shift for eight seconds (toggle FilterKeys on and off)
- Left Alt+Left Shift+NumLock (toggle MouseKeys on and off)

- Left Alt+Left Shift+PrintScreen (toggle High Contrast on and off).

How to fix:

Hotkeys can be configured via Windows Control Panel. If hotkeys are enabled via Control Panel, they are not blocked when WinCC flexible is launched.

1.10 Disable remote access to computer

Description:

If remote access to the computer, which runs the WinCC flexible environment, is not required, disable this feature in Windows.

How to fix:

To disable remote access, go to Start -> Settings -> Control Panel -> System -> Remote.

1.11 Enable User Account Control

Description:

By default, User Account Control (UAC) is enabled on Windows Vista and Windows 7. If WinCC flexible 2008 is in use, ensure this OS setting remains enabled.

How to fix:

Ensure UAC is enabled.

1.12 Configure Windows Firewall authorized components list

Description:

Once WinCC flexible 2008 is installed, exceptions for various components will be automatically added to the firewall settings. Unused components should be excluded or reconfigured.

How to fix:

It is recommended that you reconfigure used components according to your needs and allow exceptions only for used components.

To configure the list of allowed components use the following register key:
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List]

1.13 Disable access to external networks

Description:

For maximum security, it is necessary to divide networks into the following categories: networks for management, for data transmission, and main purpose networks. So, if an attacker penetrates into one of the networks, system compromise may be avoided.

How to fix:

To verify external networks availability, use the **netstat** application with the **-rn** parameters. For checking, enter netstat –rn command in the command line.

1.14 Do not use Novell Netware

Description:

Avoid installing WinCC on the system together with the Novell client's software.

Such an installation may result in failure to log into the Novell system or to lock the keyboard in the execution environment.

How to fix:

Do not use Netware client software (using Microsoft client for Netware is possible).

2. DBMS CONFIGURATION

2.1 Use Microsoft SQL 2005

Description:
By default, use of Microsoft SQL 2005 in WinCC flexible is an additional feature logging events and issues on the system. If the project is not configured to use Microsoft SQL 2005, logging will be performed into the files (CVS, RDB, TXT), stored on the system disk (by default, C:\Logs). Data stored in the formats specified above may be compromised.
How to fix:
Ensure Microsoft SQL 2005 is used.

2.2 Ensure installation of the latest security updates for Microsoft SQL 2005

Description:
It is recommended that you install all the latest SQL Server updates and patches. In environments with multiple SQL Server instances, updates should be applied to every instance.
Latest updates and patches are available on the vendor's website.
How to fix:
Ensure that all the latest SQL Server updates and service packs have been installed.

2.3 Use strong system administrator password

Description:
Only the ASCII characters can be used for the password of the SQL Server system administrator. The password should contain at least 14 characters.
How to fix:
Ensure that a strong password is used for the system administrator account.

2.4 Use strong password for DBMS access

Description:
Only the ASCII characters can be used for the SQL Server access. The password should contain at least 14 characters.
How to fix:
Ensure that a strong password is used for DBMS access.

2.5 Provide SIMATIC HMI users with SQL Server access rights

Description:
To access WinCC flexible in Microsoft SQL Server 2005, SIMATIC HMI members should be granted appropriate access rights. For granting rights, add the users to the group SQLServer2005MSSQLUser$<COMPUTERNAME>$WINCCFLEXEXPRESS.
How to fix:
To grant SQL Server rights to users, add them to the group SQLServer2005MSSQLUser$<COMPUTERNAME>$WINCCFLEXEXPRESS.

3. ADDITIONAL MEANS OF PROTECTION

3.1 Ensure the installed antivirus is compatible

Description:

It is recommended that only compatible antivirus software is used on OS with WinCC flexible installed.

How to fix:
Check the compatibility of the antivirus software via the following list:

http://cache.automation.siemens.com/dnl/DE/DE4ODIzAAAA_22055368_FAQ/22055368_WinCC_flexible_compatibility_list_e.pdf

Links:

http://cache.automation.siemens.com/dnl/DE/DE4ODIzAAAA_22055368_FAQ/22055368_WinCC_flexible_compatibility_list_e.pdf

3.2 Use up-to-date antivirus software

Description:

The antivirus software should be active and should use the latest database.

How to fix:
Ensure that the antivirus software is active and that the latest database is used.

Links:

http://cache.automation.siemens.com/dnl/DE/DE4ODIzAAAA_22055368_FAQ/22055368_WinCC_flexible_compatibility_list_e.pdf

4. SIMATIC SIEMENS WINCC FLEXIBLE SYSTEM PARAMETERS

4.1 Ensure the latest updates are installed

Description:
Before service packs or updates are officially released, Siemens often issues various official fixes for specific WinCC flexible 2008 components. It is recommended that you install all the latest WinCC flexible 2008 updates and patches.
Ensure that all the latest WinCC flexible 2008 updates and service packs have been installed.
Latest updates and patches are available on the Siemens official website.
How to fix:
To check for the latest updates, use the following link:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&siteid=cseus&aktprim=0&extranet=standard&viewreg=WW&objid=16502685&treeLang=en
Links:

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&siteid=cseus&aktprim=0&extranet=standard&viewreg=WW&objid=16502685&treeLang=en

4.2 Remove the supplementary SIMATIC ProAgent application

Description:

As a rule, the diagnostic application ProAgent is not installed by default. The application may be installed only separately. If the application is installed on the system with the execution environment, it allows accessing directly to the process via the diagram of changes, which also supports errors correction. Moreover, the application allows gaining excessive diagnostic data.

How to fix:

ProAgent is not necessary for the operation of a workstation or an HMI panel, it is advisable to remove the application from the system.

Check if the application is installed on the system:

[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\WinCCflexibleSetup]

"ProAgent"=sz:Off

[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\WinCC flexible 2008]

"ProAgent"=dword:00000000

Ensure the running ProAgent.exe application is absent in the list of OS processes.

4.3 Remove the supplementary SIMATIC ProSave application

Description:

The ProSave application is used for performing services functions for HMI panels. By default the application does not require authorization and may be used for reconfiguration, data backupping\restoring, and OS updating on HMI panels. If the program is used inappropriately, the project can potentially be damaged or unauthorized data modification can occur on HMI panels. The application should be used by competent staff members only.

How to fix:

ProSave is unnecessary for the work of a station with the execution environment, although it is installed together with WinCC flexible by default. If the application is not needed, it is advisable that you remove it from the system and create backups from a separate workstation (separately installing ProSave there).

Go to Start -> Settings -> Control Panel -> Add or Remove Programs -> SIMATIC ProSave V9.x.

Ensure the component is removed and the keys are absent:

[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\ProSave]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PTProSave.ProSaveAutomationEx]

Ensure the running ProSave.exe application is absent in the list of OS processes.

4.4 Configure WinCC flexible Runtime Loader

Description:

The WinCC flexible Runtime Loader allows transferring execution environment data via various interfaces.

The application may be misused, so restrict the use of the Runtime Loader to competent staff members only.

Previously discovered application vulnerabilities are: SIEMENS-SSA-460621, ICSA-11-244-01, and CVE-2011-4877.

How to fix:

Ensure the running HMiLoad.exe application is absent in the list of OS processes. Check the TCP port 2308.

For checking disabled parameters for all possible interfaces:

Start -> Programs -> Siemens Automation -> Runtime Systems -> WinCC flexible Runtime 2008 -> WinCC Runtime Loader

[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\CoRtHmiRTm\Loader]

"ChannelStatus"=dword:00000000 (all interfaces and remote access are disabled)

"Channel_2"=dword:00000001 (selection of COM interface in Runtime Loader)

"EnableSmartStart"=sz:C:\Program Files\Siemens\Automation \SIMATIC WinCC flexible\ WinCC flexible 2008 Runtime\HmiRtm.exe (the path to the execution environment autostart file)
"Timeout"=dword:00000003 (timeout before the execution environment start)
"FWX_Path"=sz: (the path to the configuration file)
"PDZ_Path"=sz: (the path to the backup file)
"ComPort"=sz:COM1 (selected COM port on the first interface)
Values with the enabled interfaces "ChannelStatus"=dword:
00000100 (first interface is enabled)
00000001 (second interface is enabled)
00001100 (first interface and remote access to it are enabled)
00000011 (second interface and remote access to it are enabled)
00001111 (both interfaces and remote access to all the interfaces are enabled)
Links:

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=29054993

4.5 Ensure autostart of the WinCC flexible Start Center application and project

Description:
Verify that WinCC flexible Start Center autostart is configured and WinCC flexible Runtime starts together with the system.
How to fix:
Ensure the running HmiSmartStart.exe application is present in the list of OS processes.
Ensure the SIMATIC WinCC flexible Auto Start setting is enabled in WinCC flexible Start Center.
[HKEY_CURRENT_USER\Software\SIEMENS\SIMATIC WinCC flexible]
"EnableSmartStart"=dword:00000001
Note:
Ready and compiled project is stored in the .fwc file. To make it launch together with the Windows system start, create the link to the project file and add it to the Autostart folder. Autostart also can be configured via WinCC flexible Runtime Loader (HmiLoad.exe).
Start -> Programs -> Siemens Automation -> Runtime Systems -> WinCC flexible Runtime 2008 -> WinCC Flexible Runtime Loader -> Settings.
For checking or configuring the project autostart, use the following link:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=32813727
Links:

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=32813727

5. RUNTIME SECURITY SETTINGS

5.1 Configure password aging options

Description:
If default authorization is used for WinCC Flexible 2008 project, it is necessary to enable password aging.
How to fix:
The number of days for which the user will be notified about the password expiration should not be greater than 7, the password should be valid for not more than 60 days, and the number of consecutive invalid login attempts should remain default — not more than 3.

For checking or configuring the settings in the project, go to: WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings -> Password aging.
To ensure Password aging values are appropriately configured for each tab in groups, go to: WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Groups.
Note:
Do not use windows with forced password change in the execution environment. If the project involves the use of such windows, access to them should be granted only to the administrator account and a complicated authorization scheme should be applied.

5.2 Use strong passwords

Description:
If default authorization is used for WinCC Flexible 2008 project, it is necessary to use complex passwords.
How to fix:
Require the use of numbers and special characters for passwords. Password length should be at least 14. For checking or configuring the settings in the project, use the following link: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings (enable the options "The password must contain at least one special character" and "The password must contain at least one number", the value of the option "Min. length of password" should be at least 14 characters).

5.3 Restrict the number of invalid login attempts

Description:
Restrict the number of invalid login attempts up to 3 attempts.
How to fix:
To restrict the number of invalid login attempts, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings -> Password aging. Set the Invalid login attempts option to 3.

5.4 Disable login using password exclusively

Description:
Do not allow login using password exclusively (without providing user name). The requirement of providing user name together with the password makes the authorization scheme more complex and makes it securer.
How to fix:
For checking or configuring the settings in the project, go to: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings -> Password security -> Login using password exclusively (the option should be disabled).

5.5 Use access group hierarchy

Description:
WinCC flexible 2008 provides access group hierarchy. The smaller is the number of a group, the higher are its access level permissions. The administrative group is assigned number 1, the users group is assigned number 9 by default. Administrator of the group which was assigned number 5 can manage

only those users whose group number is less than or equal to 5. This means that such an administrator can add users into groups which number is less than or equal to 5.

How to fix:

To activate group hierarchy in the project, go to: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings -> Group Administration -> Group number hierarchy.

To configure group numbers and access permissions, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Groups.

5.6 Configure the idle time before automatic forced logoff

Description:

Configure forced logoff when an operator has not been using the execution environment for a long time. You can configure logoff time in the project in the access groups' settings.

How to fix:

To configure this feature, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings -> Runtime Services -> Logoff time.

To configure access time, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Groups.

5.7 Require initial administrator's password change

Description:

Configure the requirement of initial administrator's password change.

How to fix:

To enable this feature, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings -> Runtime Services -> Initial password change.

5.8 Ensure appropriate settings are configured if SIMATIC Logon is used

Description:

WinCC flexible provides SIMATIC Logon remote access. SIMATIC Logon is not a free product and requires a license.

When SIMATIC Logon is used, it is required that on the server (central station) you activate the feature of automatic logoff after a specified time, configure the logoff time and enable password aging. Encryption should be used for data transferred to the server.

How to fix:

To enable and appropriately configure SIMATIC Logon in the project, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Runtime Security Settings. Enable Encrypted transfer to apply data encryption. Verify the SIMATIC Logon settings are configured appropriately in the configuration file on the server: C:\Documents and Settings*{All Users\Documents}*\Siemens\SIMATICLogon\settings\slsettings.ini.

Control parameters of the configuration file on the server (parameters can change depending on your needs, but still they should be configured appropriately):

[Screensaver]

UseScreensaver=0 — Used SIMATIC Logon automatic logoff

WaitTime=3000 — Delay Time in Seconds

TimeToLogout=30 — Time until automatic logoff

[Config]
Reminder=0 — Days for reminder of password expiration
[LogonService]
ClientWatchTimeOut=2000 — Delay Time in Seconds
Timeout4ControlClients=1000 — Delay Time in Seconds

5.9 Install SSL certificates

Description:
For secure data transfer via SSL (Secure Sockets Layer), install the certificates on the WinCC flexible workstations and clients. The certificates are required for server authentication. Such a certificate guarantees that the server, with which the connection will be established, is the very server specified in the certificate.
How to fix:
Initially HTTPS server created a certificate and saves it to the file Cert.cer. The file is available:
• on a Windows PC/panel PC: in a folder containing the WinCC flexible Runtime environment
• on Windows CE devices in the folder \SystemRoot\SSL\cacert.pem (on HTTPS client the file cacert.pem should be stored on a media from which the file can be launched by double-clicking on its name).
To install the certificate in the Windows client system, connect the media containing cacert.pem to the device or open the folder containing cacert.pem. Double-click on the filename and follow the instructions in the Windows dialog box.
Links:
http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC%20Flex/WinCC_flexible_2005_Kommunication1_r.pdf (p. 3-11)

5.10 Ensure SIMATIC HMI HTTP\HTTPS Protocol settings are configured appropriately

Description:
If the project uses SIMATIC HMI HTTP Protocol connections, use SSL protocol for secure data transfer. In the WinCC flexible connections editor define the protocol type (https://) and specify how an HTTPS client should check the server certificate properties and react to errors.
How to fix:
To check or change the settings in the project, go to: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Communication -> Connections.
If the HTTPS is configured, disable the following features (if possible): Allow invalid computer names for certificates, Allow expired certificates, and Allow certificates signed by unknown authorities.
Links:
http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC%20Flex/WinCC_flexible_2005_Kommunication1_r.pdf (p. 3—5)

5.11 Apply binding your HMI device to the controller

Description:
On the execution mode start, there is a possibility to verify if your HMI device is connected to an appropriate controller. It is especially important when several HMI devices are in use or in case of attempts to add date from an unknown device (controller). Your HMI checks if the value stored on the controller matches the value specified in the project data. This procedure ensures the compatibility of project data with the controller program. If they are incompatible, a due notification appears on the HMI device and the project execution is stopped.
How to fix:

Specify the project version. The range of possible values is from 1 up to 65535. In the project, enter the version into the Project ID field, which is available in the device settings editor in the Device settings window: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings.
On the controller, in the connections editor select Communication -> Connections, and enter the address in the Address field.

6. SIMATIC SIEMENS WINCC FLEXIBLE ACCESS SETTINGS

6.1 Change default administrator password for the project

Description:
Change empty or default WinCC flexible administrator password (Administrator/100).
How to fix:
To check users list and passwords in the project, go to
WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Groups or Users.
All password data are stored in the project file and separate file.
Note:
The password is stored in a separate file in the folder containing the project. By default, WinCC flexible suggests saving files in user's documents (C:\Documents and Settings\User\My Documents). You can find the location of the project file by its extension (.hmi). The compiled execution environment (RT) file has the .fwx extension. Passwords are usually stored in a separate .pwx file in the folder that contains the HMI file. After the start of the execution environment (RT) the file changes its extension to .pwl or .pwl1 without any modification of its contents (provided the password was not changed before that).
Password storing is not performed automatically after its change in the project or project's compilation or saving. A new password is stored only after execution environment (RT) start. Nor the project, nor the execution environment is not bound to the password file and can operate without the file in case it is removed. After every compilation of the project, the password file is created again using the settings data in the project file. However, on the execution environment start, the password file is analyzed and applied.
Siemens proprietary encryption algorithm is used for the passwords.
For HMI passwords on Windows CE, the password file is called pdata.pwl and is stored in the folder \Flash\simatic\. File with passwords can be copied or changed to another one.
Links:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=21778862

6.2 Configure forced logoff for all users

Description:
Configure forced logoff after a specified time of idleness for all users.
How to fix:
Verify forced logoff is configured for every user. By default, this setting is always enabled (5 minutes), however administrators often disable it. Do not disable this feature absolutely but specify an optimal logoff time for all users.
WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Runtime User Administration -> Users -> (select user) -> General –> Settings -> Logoff time

6.3 Change default MiniWeb password

Description:
Change empty or default WinCC flexible MiniWeb password (Administrator/100).
How to fix:
To change MiniWeb (Web Server) passwords, go to Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server -> User Administration.C:\Documents and Settings\All Users\Application Data\Siemens\HmiRTm\MiniWeb1.4.0\SystemRoot\UserDataBase.xml.
- <USER NAME="Administrator" PASSWORD="f899139df5e1059396431415e770c6dd">
In this case the default MD5 password (100) is used.

6.4 Change default Sm@rtServer passwords

Description:
Change empty or default WinCC flexible Sm@rtServer passwords (be default, one password is used for read and write access — 100).
How to fix:
To change Sm@rtServer passwords, go to Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings -> Server.
[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm\Sm@rtServer]
"Password"=binary:11 20 00 00 00 00 00 00 73 61 71 9c 6e fd 76 76
"Password2"=binary:11 20 00 00 00 00 00 00 73 61 71 9c 6e fd 76 76
In this case default passwords (100) are used.
The reversible encryption algorithm VNC is used for the passwords.
Links:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=45815365

6.5 Check and change Sm@rtServer forced access password

Description:
Forced access password is required for login in emergency cases. The password should be changed to contain less than 14 characters. The password should not match the old passwords.
How to fix:
To configure forced access password, go to Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings -> Administration -> Forced Write Access.
[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm\Sm@rtServer]
"FWAPasswordNeeded"=dword:00000001
"Password"=binary:11 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
In this case default password (xhPMr) is used. The reversible encryption algorithm VNC is used for the password.
If the password is disabled, any operator will be able to use forced access to the data by holding the Shift key for a long time or by using four consecutive clicks (for HMI panels — 4 taps).
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings -> Administration -> Forced Write Access -> Password needed
"FWAPasswordNeeded"=dword:00000001

6.6 Store email password in the project only

Description:

Do not store email authentication data in WinCC flexible Internet Settings, store this data in the project only.

How to fix:

Use authentication data stored in the project:

Start -> Setting -> Control Panel -> WinCC flexible Internet Settings -> Advanced -> Authentication -> Use the default or the project file

[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]

"Smtp_Login"=sz: (empty)

"Smtp_Password"=sz: (empty)

Note:

Password is stored in Windows registry if you try to save authentication data in WinCC flexible Internet Settings (Use panel settings for authentication).

[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]

"Smtp_Password"=sz:zfzM/Mz8 (no default password, password example — 100)

Embedded encryption algorithm is used for the password. The password is empty by default.

6.7 Ensure access privileges are configured appropriately in WinCC Internet Settings

Description:

WinCC Internet Settings allows you to create new accounts and configure access control (UserDataBase-Edit) in case you have administrator credentials.

How to fix:

We recommend creating a special user with limited privileges for these purposes. We also recommend assigning access privileges for administrator account.

Use the following directions to change the settings: Start -> Setting -> Control Panel -> WinCC Flexible Internet Settings -> Web Server -> User Administration -> *Enter Password* -> Authorizations.

The user configuration file for a computer is available here: C:\Documents and Settings\All Users\Application Data\Siemens\HmiRTm\MiniWeb1.4.0\SystemRoot\UserDataBase.xml.

The user configuration file for HMI panels is available here: C:\Documents and Settings\All Users\Application Data\Siemens\HmiRTm\MiniWeb1.3.2\SystemRoot\UserDataBase.xml.

Every item is a possible access privileges (all items mean a full access):

<GROUP NAME="Default"/> — default;

<GROUP NAME="RuntimeAccess"/> — start and stop the run-time environment;

<GROUP NAME="RTCommunication"/> — rights to use HMI HTTP server;

<GROUP NAME="Engineering"/> — rights to transfer data from the development system to the device

<GROUP NAME="SoapUser"/> — access via SOAP with read/write privileges;

<GROUP NAME="UserData"/> — user access;

<GROUP NAME="UserAdministration"/> — administrator access;

<GROUP NAME="FileBrowserUser"/> — limited access and file management via Web;

<GROUP NAME="FileBrowserAdministrator"/> - full access and file management via Web.

If all items are available for every account in the file, it means that all users have full privileges.

Links:

http://cache.automation.siemens.com/dnl/jk/jkyMTI1MQAA_48955975_Tools/48955975_WinCCflexible_HTML_Site_en.pdf (page 73)

7. SM@RTSERVER SECURITY SETTINGS

7.1 Disable or provide correct Sm@rtServer settings (Remote Server)

Description:
If remote access to Sm@rtServer is not necessary, we recommend you to disable it in the project.
If the application is necessary, we recommend you to ensure that it is correctly and securely configured.
How to fix:
Web Client VNC or Sm@rtClient settings are available on the server in the following registry key:
[HKEY_CURRENT_USER\Software\SIEMENS\Sm@rtClient].
Server stores the settings provided by the connected client. You are unable to block these settings. The client can modify the settings in every connection.
Use the following directions to enable or disable access via Sm@rtServer:
WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> Sm@rtAccess or Service: Start up Sm@rtServer.
Ensure the running SmartServer.exe application is absent in the list of OS processes.
Check the default ports: 5800 and 5900.
If the application is not used (loaded) at least once, the registry does not include stored settings.
Use the following directions to change Sm@rtServer settings: Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings.

7.2 Limit remote project management

Description:
Sm@rtServer is based on TightVNC technology. You can use third-party clients such as VNC Viewer developed by RealVNC to remotely access Windows functionality. In this case, you can view the project but unable to manage it.
How to fix:
You can fully block the data input for clients in the following way:
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings: -> Server -> Incoming connection -> (Password 1: -> View only) and(Password 2: -> View only).
[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HmiRTm\Sm@rtServer]
"InputsEnabled"=dword:00000000
"InputsEnabled2"=dword:00000000

7.3 Limit number of users with access to the workstation

Description:
If an operator does not need to use the workstation, we recommend you to disable HMI access and enable access for remote clients only.
How to fix:
Use the following directions: Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings: ->Server -> No local input during client session.
[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HmiRTm\Sm@rtServer]
"LocalInputsDisabled"=dword:00000001

7.4 Grant access only with operator confirmation

Description:

We recommend you to restrict incoming connection, and make the operator to enable remote access on his own.

How to fix:

Enable the operator confirmation request:

Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings: -> Query -> Query console on incoming connection -> Query console on incoming connections

Default action: Refuse, Allow option to accept without authentication setting is disabled

[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HmiRTm\Sm@rtServer]

"QuerySetting"=dword:00000004

7.5 Restrict to pass settings for applets via URL

Description:

We recommend you to disable a possibility to configure settings for applets via URL.

How to fix:

Use the following directions to disable this feature: Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings -> Administration -> HTTP server -> Enable applet params in URLs.

[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HmiRTm\Sm@rtServer]

"EnableURLParams"=dword:00000000

7.6 Restrict to pass files remotely

Description:

Sm@rtServer does not allow you to restrict to send files but you can do it via the registry. The feature makes it possible to send files via a remote connection. We recommend you to disable this feature.

How to fix:

Use regedit registry editor to disable the feature:

[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HmiRTm\Sm@rtServer]

"EnableFileTransfers"=dword:00000000

7.7 Configure Sm@rtServer (Remote Server) disabling and enabling together with Runtime

Description:

Sm@rtServer enabling and disabling should be done together with WinCE flexible Runtime 2008 start and stop to make it impossible for users to access Windows features in case the run-time environment is disabled.

How to fix:

Use the following directions:

Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server: -> Close with Runtime

[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\HmiRTm\Sm@rtServer]

"StopVnc"=dword:00000001

7.8 Do not use Sm@rtServer as a service

Description:

If Sm@rtServer enabling and disabling is done together with WinCC flexible Runtime start and stop, but Sm@rtServer is started as a service, then Sm@rtServer is started every time with the operating system instead of other settings. This feature should be disabled to rule out any possibility to access Windows features in case the run-time environment is not started.

How to fix:
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server: -> Start automatically after booting
Ensure that the whole branch with settings is absent:
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\smartserver]
"ImagePatch"=" "C:\Program Files\Siemens\SIMATIC WinCC flexible\WinCC flexible 2008 Runtime\SmartServer.exe" -service
"Start"=dword:00000002
…

8. MINIWEB (HTTP) SECURITY SETTINGS

8.1 Disable MiniWeb (Web Server), if not necessary

Description:
If MiniWeb (Web Server) is not necessary, we recommend you to disable it in the project.
How to fix:
Ensure the running Miniweb.exe application is absent in the list of OS processes.
Check the default ports: 80 or 443.
If the application is not used (loaded) at least once, the registry does not include stored settings.
Use the following directions to configure MiniWeb:
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server
Enabling/disabling in the project:
WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> Sm@rtService: HTML pages
WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> Sm@rtAccess: SIMATIC HMI HTTP Server — access to tags via HMI runtime environment.

8.2 Enable authentication for tags

Description:
We recommend you to enable authentication for tags in the project, at the same time the possibility to modify or view tags without authorization would be disabled (Connection -> HMI HTTP Protocol).
How to fix:
Tag authenticate -> Authentication required
Restrict the data input (for projects that use displaying only).
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server: -> Tag access -> Read only
[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]
"TagAccess"=dword:00000002
(If No authenticate and Read only, then "TagAccess"=dword:00000000)
(If No authenticate and Read/write, then "TagAccess"=dword:00000001)
(If Authentication required and Read/write, then "TagAccess"=dword:00000003)

8.3 Disable remote project loading for HMI panels

Description:
We recommend you to disable remote loading of a project file (mostly used for HMI panels).
How to fix:

Use the following directions to disable remote management of project loading:
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server: -> Enable Remote-Transfer (Project)
[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]
"MiniwebRemoteControl"=dword:00000000

8.4 Configure MiniWeb disabling and enabling together with Runtime

Description:
MiniWeb enabling and disabling should be done together with WinCC flexible Runtime 2008 start and stop to make it impossible for users to access and modify data in case the run-time environment is disabled.
How to fix:
Use the following directions:
Start -> Setting -> Control Panel -> WinCC Internet Setting -> Web Server: -> Close with Runtime
[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]
"StopMiniweb"=dword:00000001

9. OPC SERVER SECURITY SETTINGS

9.1 Disable OPC server if it is not used

Description:
OPC server provides data to other applications. These applications can be run on the same system or other systems in the same network. This means that process data can be viewed, for example, in Microsoft Excel. If you do not need OPC server, we recommend you to disable it in the project.
How to fix:
Ensure the running OPCDAServer.exe application is absent in the list of OS processes.
Start -> Setting -> Control Panel -> WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> Runtime services Act as OPC server
Enabling and disabling communication settings for the project is available here: WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Communication -> Connection -> OPC.
Links:
http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC%20Flex/WinCC_flexible_2005_Kommunication1_r.pdf (p. 4-1)

9.2 Configure DCOM access rights

Description:
Data exchange between OPC DA server and OPC client is done via DCOM interface. You should grant DCOM start and access privileges before the data exchange process is run.
How to fix:
Grant DCOM start and access privileges before a OPC client is able to start OPC DA server and establish connection for data exchange:
Start -> Settings -> Control Panel -> Administrative tools -> Component services -> Component Services -> Console Root\Component\Services\Computers\My Computer\DCOM Configuration
Open OPC.SimaticHMI.HmiRT context menu and choose Properties. You can see OPC.SimaticHMI.HmiRTm properties dialog window.

Add (Administrator and Network) to Access Permissions and Configuration Permissions and grant access (Allow Access\Type Allow) only for necessary users.

Links:

http://iadt.siemens.ru/assets/files/infocenter/Documetations/Automation_systems/HMI/WinCC%20Flex/WinCC_flexible_2005_Kommunication1_r.pdf p. 4-16

10. WEB SERVICE (SOAP) SECURITY SETTINGS

10.1 Disable or provide security for Web service (SOAP)

Description:
If the service is enabled, users are able to read and write tags with usual applications (for example, MS Excel). Communication is possible by the use of a script added into the application based on SOAP (Simple Object Access Protocol) HTTP protocols. If the service is not necessary, disable it. If the service is necessary, take appropriate measures to provide the application's security.
How to fix:
Use the following directions to enable or disable the service: WinCC Flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> Sm@rtAccess: Web service (SOAP).
The service is mostly used together with VBA in MS Excel. In this case authorization is made in the following way:

```
Set objRuntime = CreateObject("MSSOAP.SoapClient")
objRuntime.mssoapinit "HTTP://servername/soap/RuntimeAccess?wsdl"
objRuntime.ConnectorProperty("AuthUser") = "Administrator"
objRuntime.ConnectorProperty("AuthPassword") = "100"
```

Surely, you should encrypt Excel file. The file password should contain at least 14 characters. By default MS Office uses extended 128 bit encryption based on AES algorithm for files.
We also recommend you to use a secure connection to transfer data via the network.
Links:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=28970872
http://www.electricalmanuals.net/files/PLC/SIEMENS/WINCC/ONLINE-HELP-1.pdf (p.3-17)

11. SMTP SECURITY SETTINGS

11.1 Ensure that email is secure

Description:
Use settings stored in the project only to send email. All settings are copied and stored in Windows registry if WinCC flexible Internet Settings is used.
How to fix:
Settings in the project: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> SMTP settings
Use authorization settings from the project file:
WinCC flexible Internet Settings -> Advanced -> Authentication -> Use the default or the project file
If the application is not used (loaded) at least once, the registry does not include stored settings.
We recommend you to use SMTP server that is assigned and configured in the project file.
Start -> Setting -> Control Panel -> WinCC flexible Internet Settings -> SMTP server -> Use the default or the project file
[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]
"Smtp_Server"=sz:
"Smtp_SenderName"=sz:
"Smtp_AuthenticationName"=sz:

11.2 Configure a secure connection for email data exchange

Description:

Ensure that email data exchange is performed via a secure channel (SSL).

How to fix:

Use the following directions to configure a secure connection:

WinCC flexible Internet Settings -> Advanced -> Use secure connection -> Enable SSL

If the application is not used (loaded) at least once, the registry does not include stored settings.

[HKEY_LOCAL_MACHINE\SOFTWARE\SIEMENS\HmiRTm]

"Smtp_SecureAUTHMethod"=dword:00000100

Enable his server requires a secure connection (SSL) setting in email configuration. Then, go to WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings -> SMTP settings.

12. LOGGING

12.1 Enable event logging in Sm@rtServer application

Description:

We recommend you to use event logging. Events should be stored in Sm@rtServer application logs.

How to fix:

Use the following directions to modify the settings: Start -> Setting -> Control Panel -> WinCC Internet Setting -> Remote -> Change settings -> Administration -> Logging -> Log information to SmartServer.log.

13. PROJECT MANAGEMENT

13.1 Disable hot keys in user interface

Description:

Restrict actions performed via Windows user interface in the WinCC flexible environment. We recommend you to disable hot keys (Ctrl+Alt+Del, Alt+Esc, Alt+Tab, Ctrl+Esc, Resize, Move, Minimize, Maximize, etc.) for the computer project. We also recommend you to enable soft keyboard only (if possible). We also recommend you to enable soft keyboard only (if possible), configure full-screen project window and block a possibility to switch windows.

How to fix:

Go to the following project settings to check user interface restrictions in WinCC flexible: WinCC flexible 2008 -> Project -> Project Name -> Device Name (WinCC flexible Runtime) -> Device Settings -> Device Settings.

Ensure that the following settings are enabled: Use on-screen keyboard, Lock task switching, Full-screen mode и Disable function keys on modal dialogs.

13.2 Configure protection against unauthorized access

Description:

Every important project's object or element should be protected against unauthorized access. The critical project elements are the data that can be sent from WinCC flexible to a controller directly.

How to fix:

You are able to configure protection against unauthorized access for a number of objects in WinCC flexible (input/output field, graphic input/output field, symbol input/output field, button, switch, graphic windows, message windows, message answerback, etc.). You should try to view and edit the project to ensure that protection against unauthorized access is enabled for all important elements

(Enabled is on and access level is chosen in Properties -> Security). Then, an unauthorized user has to enter a password to use the object.
Additionally, logoff element should be located so that it is easy to use. A operator should logoff as all necessary changes are made.

14. WEB SERVER: HTML PAGES

14.1 Publish necessary tags only

Description:
If own HTML pages are used, you should provide access only to necessary tags published via MiniWeb (Web Server). You also should bind every published tag to the default authorization. Otherwise all tags are available without authorization.
How to fix:
Ensure that every important published tag is bound to an authorization (ShareRealm). In this case, tag data input/output is blocked until a user is not authorized.
Here is an example how to use scripts without authorization:
Read tag's value:
<MWSL><!-- write(GetVar("Tag_1")); --></MWSL>
Write the tag with '1' parameter:
<MWSL><!-- SetVar("Tag_1", "1"); --></MWSL>
Here is an example how to use scripts with authorization:
Read tag's value:
<MWSL><!-- if (ShareRealm("ANY_REALM")){write(GetVar("Tag_1"));} --></MWSL>
Write the tag with '1' parameter:
<MWSL><!-- if (ShareRealm("ANY_REALM")){SetVar("Tag_1", "1");} --></MWSL>
Show authorization status:
I/0 access= <MWSL> if (ShareRealm("NO_REALM")){write("disabled");}else{write("enabled");}</MWSL>
It is possible to check if user's pages or modified default pages exist with the initial structure and default files' properties:
C:\Documents and Settings\All Users\Application Data\Siemens\HmiRTm\MiniWeb1.4.0\WebContent
Links:
http://cache.automation.siemens.com/dnl/jk/jkyMTI1MQAA_48955975_Tools/48955975_WinCCflexible_HTML_Site_en.pdf

Additional materials:
Ports for different services:

SIMATIC product	Application	Service			Port
WinCC flexible RT	Web Server	Access to internal HTML pages (HTTP)			80
		Access to internal HTML pages (HTTPS / SSL)			443
	Sm@rt Server	Connection to the **Sm@rtServer**			5800
		Connection to the **Sm@rtServer**			5900
	OPC	OPC via DCOM	Server	Connection establishment	135
				Communication	dyn.
			Client	Communication	dyn.
		OPC via XML (client <=> server)			80
		OPC UA (binary protocol)		Communication	4840
	Archiving	Archiving on a server		UDP	137, 138
				TCP	139
	Other	**Transfer** via Ethernet		Configuration PC	dyn.
				Panel	2308 or 50523
		Communication between		S7 controller	102
				Panel	dyn.
		PROFINET IO communication			34964
		E-mail (SMTP server)			25
		Modicon controller (Modicon channel MODBUS TCP/IP)			502

Typical services for data exchange

Licenses:

[HKEY_CURRENT_USER\SOFTWARE\SIEMENS\SWS\LicenseManager\Explorer]
"LastDrive"=sz:C:\
C:\AX NF ZZ (hidden folder)
*.EKB files
The following registry key is widely used to display license details:
HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\SWS\LicenseManager\FixedViews\5211
"Columns"=sz: licenses are enumerated by internal numbers possibly.

References to Siemens recommendations on SCADA security:

SIMATIC Process Control System PCS 7 Security concept PCS 7 & WinCC (Basic):
http://support.automation.siemens.com/WW/llisapi.dll/csfetch/60119725/Main_de_Sicherheitskonzept_SIMATIC_en_en-US.pdf
Security for PC-based Automation Systems with Windows Embedded Operating Systems:
http://cache.automation.siemens.com/dnl/TU/TU2MDQ5MQAA_55390879_Tools/55390879_Security_Leitfaden_PCBased_WE_en.pdf