SIEMENS SIMATIC WINCC 7.X

SCADA SECURITY HARDENING GUIDE
PUBLIC BETA

27 DEC 2012

CONTENTS

LEGAL NOTES....4
1. OPERATING SYSTEM CONFIGURATION....5
1.1 Use compatible Windows version....5
1.2 Ensure appropriate Windows language settings....5
1.3 Ensure the latest Windows updates are installed....5
1.4 Enable unsigned drivers installation....5
1.5 Set user interface restrictions....5
1.6 Set system parameters according to the vendor's requirements....6
1.7 Ensure control of system group membership restrictions....6
2. SYSTEM NETWORK PARAMETERS CONFIGURATION....7
2.1 Disable access to external networks....7
2.2 Do not install Novell Netware clients....7
3. DBMS CONFIGURATION....7
3.1 Ensure installation of the latest security updates for Microsoft SQL 2005....7
3.2 Use strong system administrator password....7
3.3 Provide SIMATIC HMI users with SQL access rights....7
4. ADDITIONAL SECURITY TOOLS....8
4.1 Install compatible antivirus software....8
4.2 Use up-to-date antivirus software....8
5. SIMATIC WINCC (SYSTEM PARAMETERS)....8
5.1 Do not use the WinCC DiagAgent (CCDiagAgent) application in production systems....8
5.2 Ensure WinCC Runtime launch as a system service....8
5.3 Disable WinCC Runtime autostart cancelling....8
6. SIMATIC WINCC (SIMATIC LOGON CONFIGURATIONS)....9
6.1 Set logon time-out....9
6.2 Enable password change reminder....9
7. SIMATIC WINCC (ACCESS CONFIGURATIONS)....10
7.1 Change default passwords for demonstration accounts....10
7.2 Change administrator’s default password....10
7.3 Control password strength for HMI access accounts....10
7.4 Restrict management group membership....10
7.5 Disable access via local groups....11
8. SIMATIC WINCC (EVENTS LOGGING)....11
8.1 Enable logon events logging to archive....11

8.2 Enable logon events logging to the Windows system log 11
9. SIMATIC WINCC (PROJECT CONTROL) 11
9.1 Disable interface management hotkeys 11
10. SIMATIC WINCC (WEBNAVIGATOR — SCREEN PUBLISHING) 12
10.1 Publish only necessary screens 12

LEGAL NOTES

1. OPERATING SYSTEM CONFIGURATION

1.1 Use compatible Windows version

Install WinCC on those operating systems that are supported by the vendor.

Recommendations:
To verify whether the Windows version is compatible, use the list http://cache.automation.siemens.com/dnl/zQ/zQzMjEzAAAA_21927773_FAQ/WinCC_V70_compatibility_list_e.pdf.

1.2 Ensure appropriate Windows language settings

WinCC is available 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.

Recommendations:
To make sure the OS language settings are appropriate, verify the language used in the system: Start -> Control Panel -> Regional and Language Options.

1.3 Ensure the latest Windows updates are installed

For supporting Windows up-to-date security level, it is required to check for updates regularly.

Recommendations:
Ensure that all the latest OS updates have been installed.

1.4 Enable unsigned drivers installation

For WinCC proper functioning on a Windows operating system, it is necessary to disable the default check for drivers' signatures on installation.

Recommendations:
Verify that the installation of unsigned drivers is allowed.

1.5 Set user interface restrictions

It is necessary to restrict user actions performed via Windows interface in the WinCC environment. It is required to disable such hotkeys as Ctr+Alt+Del, Alt+Esc, Alt+Tab, Ctl+Esc.

Recommendations:

To verify the status of restriction on WinCC user interface, go to WinCC Explorer -> Computer properties -> Parameters -> Disable Keys.

Verify the following registry key values:

For 64-bit Windows systems:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Siemens\WinCC\Winlogon\Permissions]
"AllowShutdown"=dword:00000001
"AllowLogout"=dword:00000001
"AllowCtlAltDel"=dword:00000001
"AllowAltEsc"=dword:00000000
"AllowAltTab"=dword:00000001
"AllowCtlEsc"=dword:00000000
```

For 64-bit Windows systems:

```
[HKEY_LOCAL_MACHINE\SOFTWARE \Siemens\WinCC\Winlogon\Permissions]
"AllowShutdown"=dword:00000001
"AllowLogout"=dword:00000001
"AllowCtlAltDel"=dword:00000001
"AllowAltEsc"=dword:00000000
"AllowAltTab"=dword:00000001
"AllowCtlEsc"=dword:00000000
```

1.6 Set system parameters according to the vendor's requirements

For WinCC proper functioning on a Windows operating system, it is necessary to configure the operating system according to the vendor's requirements. Configure following parameters:

- User group
- Registry settings and rights
- Firewall settings
- DCOM settings
- File system rights

Recommendations:
Ensure that the system parameters are set according to the vendor's requirements. You can use SIMATIC Security Control (SecurityController.exe) tool to automate configuration process.

1.7 Ensure control of system group membership restrictions

It is required to ensure control over the membership restrictions of such system groups as Administrator, Server Operators, and Power Users.

Recommendations:
Ensure that membership restrictions set for the specified system groups are correct.

2. SYSTEM NETWORK PARAMETERS CONFIGURATION

2.1 Disable access to external networks

For maximum security, it is necessary to divide networks by 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.

Recommendations:
To verify external networks availability, use the **netstat** application with the **-rn** parameters.

2.2 Do not install Novell Netware clients

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.

Recommendations:
Ensure that the Netware client's software or Microsoft client for Netware are not used.

3. DBMS CONFIGURATION

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

For supporting up-to-date security level of SQL Server, it is required to check for updates regularly.

Recommendations:
Ensure that all the latest SQL Server updates have been installed.

3.2 Use strong system administrator password

Only the ASCII characters can be used for the password of the SQL Server system administrator. The password should contain at least 14 characters.

Recommendations:
Ensure that a strong password is used for the system administrator account.

3.3 Provide SIMATIC HMI users with SQL access rights

To receive access to WinCC in Microsoft SQL Server 2005, the SIMATIC HMI group members should have appropriate rights. For provision of the access rights, it is required to add users to the group SQLServer2005MSSQLUser$<COMPUTERNAME>$WINCC.

Recommendations:
Verify that SIMATIC HMI users have been provided with SQL Server access rights.

4. ADDITIONAL SECURITY TOOLS

4.1 Install compatible antivirus software

It is recommended to install only that antivirus software which is compatible with the WinCC software installed on your operating system.

Recommendations:
To ensure that the installed antivirus software is compatible, use the list http://cache.automation.siemens.com/dnl/zQ/zQzMjEzAAAA_21927773_FAQ/WinCC_V70_compatibility_list_e.pdf.

4.2 Use up-to-date antivirus software

The antivirus software should be active and should use an up-to-date database.

Recommendations:
Verify that antivirus software is active. To ensure that the antivirus software database is up-to-date, use recommendations of antivirus software vendor.

5. SIMATIC WINCC (SYSTEM PARAMETERS)

5.1 Do not use the WinCC DiagAgent (CCDiagAgent) application in production systems

WinCC DiagAgent (CCDiagAgent) is used to control and diagnose Simatic WinCC, operating system, and DBMS. By default, the application does not require authorization, which may allow a remote attacker to alter system configuration and execute arbitrary code. Ensure that this application has been removed or is not running on production systems.

Recommendations:
To ensure the application is not used in production systems, it is required to regularly check that there is no **CCDiagAgent.exe** among the processes running on the operating system. Use SIMATIC Diagnostics Tool or the SIMATIC Analyser. http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-223158.pdf

5.2 Ensure WinCC Runtime launch as a system service

It is required to ensure that WinCC Runtime is launched as a system service.

Recommendations:
To ensure that WinCC Runtime is launched as a system service, verify service settings available here: Project properties -> Operation mode -> Service.

5.3 Disable WinCC Runtime autostart cancelling

If autostart is configured for the WinCC project, it is required to ensure that the *Allow "Cancel" during activation* option of the AutoStart Configuration application is disabled.

Recommendations:

To ensure the specified option is disabled, verify which settings are enabled by launching the AutoStart Configuration application available here: Program Files\Siemens\WinCC\bin\AutoStartRT.exe.

Additionally, verify the EnableBreak value in the Windows registry.

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Siemens\WinCC\AutoStartWinCC]
"ProjectName"="C:\\Users\\Public\\Documents\\Siemens\\WinCCProjects\\123\\123.MCP"
"Activate"=dword:00000000 (Activate project at startup)
"EnableBreak"=dword:00000001.
"AllUsers"=dword:00000000 (available for all users)
"NCGM"=dword:00000000
"RedProject"=dword:00000000
"RedProjectName"=""
"StartInServiceMode"=dword:00000000

6. SIMATIC WINCC (SIMATIC LOGON CONFIGURATIONS)

6.1 Set logon time-out

If the SIMATIC LOGON application is used, it is necessary to activate the automatic logoff function and set a logon time-out.

Recommendations:
To ensure the logon time-out is set, verify the SIMATIC LOGON settings using the following configuration file: C:\Documents and Settings***{All Users\Documents}*** \Siemens\SIMATICLogon\settings\slsettings.ini.

Configuration file control parameters:
[Screensaver]
UseScreensaver=1 — Used SIMATIC Logon automatic logoff
WaitTime=46620 — Delay Time in Seconds
TimeToLogout=30 — Time until automatic logoff

6.2 Enable password change reminder

If the SIMATIC LOGON application is used, it is necessary to activate the function of the password change reminder. The relevant option should be configured in such a way so that the reminder appears not earlier than two months prior to the password change.

Recommendations:
To ensure the password change reminder is enabled, verify the SIMATIC LOGON parameters using the following configuration file: C:\Documents and Settings***{All Users\Documents}***
\Siemens\SIMATICLogon\settings\slsettings.ini.

Configuration file control parameters:
[Config]
Reminder=0 — Days for reminder of password expiration

7. SIMATIC WINCC (ACCESS CONFIGURATIONS)

7.1 Change default passwords for demonstration accounts

It is required to change the following default passwords for the WinCC demo accounts:

- winccd/winccpass
- wincce/winccpass
- DMUser/Data&Pass

Recommendations:
Ensure the default passwords for the demo accounts have been changed. It's recommended to delete this accounts in production environment

Links:
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=45027800&caller=view

7.2 Change administrator's default password

It is required to change the following WinCC administrator password created by default: Administrator/Administrator.

Recommendations:
To ensure the default password is not used for the administrator account, verify the WinCC user list via the following database query:

SELECT * FROM ***{database_name}***.dbo.PW_USER

Use automatic tools to control password complexity.

7.3 Control password strength for HMI access accounts

It is necessary to control password strength for group members possessing the rights to change such system parameters as:

- User administration
- Value input
- Process controlling

Recommendations:
To verify WinCC user rights, use the following database query:

SELECT * FROM ***{database_name}***.dbo.PW_USER

Use automatic tools to control password complexity.

7.4 Restrict management group membership

Control membership in the groups possessing the rights to change such system parameters as:

- User administration

- Value input
- Process controlling

Recommendations:
To verify WinCC user rights, use User Administrator (PassCS.exe) tool.

7.5 Disable access via local groups

A server with installed WebNavigator should be available only for groups of the same domain.

Recommendations:
To ensure that access via local groups is disabled, verify the following option configuration: WinCC Web Settings -> Session Logon/Logoff -> Disable local groups of SIMATIC Logon.

8. SIMATIC WINCC (EVENTS LOGGING)

8.1 Enable logon events logging to archive

WebNavigator Client logon and logoff successful attempts should be logged (logging of the system messages No. 1012400 or 1012401).

Recommendations:
To ensure that the event logging is enabled, verify the following option configuration: WinCC Web Settings -> Session Logon/Logoff -> Enable WinCC system messages.

8.2 Enable logon events logging to the Windows system log

It is required to log successful logon sessions to the Windows system log.

Recommendations:
To ensure that the event logging is enabled, verify the following option configuration: WinCC Web Settings -> Session Logon/Logoff -> Enable event log messages.

9. SIMATIC WINCC (PROJECT CONTROL)

9.1 Disable interface management hotkeys

Interface management shortcut keys should be disabled for each project.
Hotkeys (Alt+F4, Resize, Move, Minimize, Maximize, etc.) for windows management should be disabled in the WinCC project settings.

Recommendations:
To verify the status of WinCC user interface restrictions, go to WinCC Explorer -> Computer properties -> Graphics Runtime.

10. SIMATIC WINCC (WEBNAVIGATOR — SCREEN PUBLISHING)

10.1 Publish only necessary screens

It is required to control project screens published via WebNavigator.

Recommendations:
To verify only necessary screens are published, go to WinCCExplorer -> WebNavigator -> WinCC Web Publishing Wizard -> Select pictures.