



XHQ
System Guide




About This Guide

Overview	1
Third-party Vendors	2
XHQ Server	3
XHQ End-user Client [Applet]	4
XHQ API, IDG, BI Interfaces	5
Network	6
Personal Data Use in XHQ	7

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 DANGER
Indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
Indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
Indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
Indicates that property damage can result if proper precautions are not taken.


If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage. See the topic, [Visual Cues for Online Viewing](#), for additional XHQ-specific notices.

Qualified Personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner. For a complete list, see the [Copyright](#) topic.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Copyright © 1998-2020 Siemens AG. All rights reserved. Protected by U.S. Patents Nos. 6,700,590, 7,069,514, 7,478,128, 7,689,579, 7,698,292, 7,814,123, 7,840,607, 8,001,332, 8,078,598, 8,260,783, 8,442,938, 8,566,781, 8,700,671 and 8,700,559; Patents Pending.

Siemens Industry Software Inc.
6 Journey, Suite 200
Aliso Viejo, CA 92656-5318, USA
siemens.com/xhq

XHQ® is a registered trademark of Siemens AG in the United States. This License does not grant LICENSEE any rights to trademarks or service marks of Siemens AG.

All other company, product and service names and logos may be trademarks or service marks of their respective companies. Any rights not expressly granted herein are reserved. LICENSEE may not remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels from the Licensed Software or the Documentation.

This software is proprietary and confidential. Siemens AG or its suppliers own the title, copyright, and other intellectual property rights in the Software. The Software is licensed, not sold.

Adobe, the Adobe logo, Acrobat, the Adobe PDF logo, PostScript, and the PostScript logo, Distiller, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft, Active Directory, ActiveX, Authenticode, Developer Studio, DirectX, Microsoft, MS-DOS, Outlook, Excel, PowerPoint, Visual Basic, Visual C++, Visual C#, Visual J#, Visual SourceSafe, Visual Studio, Win32, Windows, Windows Server, WinFX, Windows 7, Windows 10, Windows Server 2012, Windows Server 2016, Windows Server 2019, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries, or both.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Oracle, Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. Oracle, or its licensor, shall at all times retain all rights, title, interest, including intellectual property rights, in Oracle Programs and media.

SAP, SAP R/3, R/3, R/3 software, mySAP, mySAP.com, xApps, xApp, ABAP, BAPI, and SAP NetWeaver are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Documentum, OpenText Documentum, OpenText and the Corporate Logo are trademarks or registered trademarks of OpenText in the United States and throughout the world.

IBM, the IBM logo, DB2, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

InstallShield® is a registered trademark and service mark of Macrovision Corporation and/or Macrovision Europe Ltd. in the United States and/or other countries. DemoShield, InstallFromTheWeb and PackageForTheWeb are service marks and registered trademarks of Macrovision Corporation and/or Macrovision Europe Ltd. in the United States and/or other countries. InstallShield Express, InstallShield for Windows Installer, InstallShield for Windows CE, Express Wizard, InstallShield Objects, WebUpdate, FastReg and NetInstall are trademarks and/or service marks of Macrovision Corporation and/or Macrovision Europe Ltd. InstallShield Software Corporation. InstallShield is a member of Macrovision Corporation.

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <https://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

For the Siemens Security Advisory, visit <https://www.siemens.com/industrialsecurity>.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>.

While every effort is made to ensure the accuracy of content, the XHQ product documentation set (which includes online help) could contain inaccuracies or out-dated material (which includes product screenshots and images) due to the large number of product enhancements being added. As such, the documentation set is subject to change at any time without notice. Refer to the README for documentation corrections and addendum. Please note, updates to the documentation set are reflected in the next general availability major release of XHQ.

Table of Contents

About This Guide	7
Conventions Used in This Guide	7
Visual Cues for Online Viewing	8
Related XHQ Product Documentation	9
Contacting Customer Support	11
General Feedback and Comments	12
1 Overview	13
Key items to consider	14
Security Information and Links	15
Holistic Approach	15
Security Management	16
2 Third-party Vendors	17
Microsoft Windows Operating System	17
IT Updates for Microsoft Windows and Oracle Java	17
Oracle Java Runtime (JRE)	18
Microsoft Windows UAC	18
Observe Microsoft and other third-party vendor security-related information	18
Secure Configuration of the Microsoft IIS Web Server	19
Preventing Malware in Leveraged Documents	19
3 XHQ Server	20
Usage of a dedicated, adequately sized XHQ Server	20
Access from the XHQ Server to the Internet	20
Use of XHQ with a Public Cloud	21
Protection of the XHQ installation media	21
XHQ README	21
Access Rights on the XHQ Server	22
XHQ Server Version	22
General server checks via Windows and XHQ log file analysis	22
XHQ Authentication Checks	22
XHQ Server Property Files	23
XHQ Import and Export files	23
Use XML files from trusted sources only	23
Server Virus Scan	24
XHQ Embedded Database	25
XHQ Backup and Recovery	25

Active Directory and Role-based Security	25
XHQ Audit Trail	26
4 XHQ End-user Client [Applet]	27
Client Java Version	27
Client Property Files	27
Administrator Rights on the XHQ Client	27
XHQ Client View Cache	28
Client Virus Scan	28
Encryption and Obfuscation	28
5 XHQ API, IDG, BI Interfaces	29
XHQ API	29
XHQ ADO.NET	29
XHQ BI Data Provider	29
Mobile Devices	30
Restricting network communication with mobile devices	30
Connecting mobile devices only to authorized workstations	30
Mobile application	30
6 Network	31
Network Login	31
XHQ Server Network Positioning	31
XHQ Server ISA-95 Positioning	31
Access to the XHQ Server from the Internet	32
Firewall Usage	32
Encryption over the Network	32
Hardening the IIS Configuration	33
About Transport Layer Security	33
LAN Manager Authentication Level	33
7 Personal Data Use in XHQ	34
Personal Data Protection	34
Audit Trail Module	35
View Statistics Module	35
XHQ Log Files and XHQ Support Utility	36
Backup XHQ	36
Layered Applications - XHQ Performance Management	36
Retention and Deletion	37
Where XHQ Stores Your Personal Data	37
Safeguarding Your Personal Information	37

About This Guide

Conventions Used in This Guide

The following formatting cues are designed to allow you to quickly locate and understand the information provided in this guide.

Formatting Conventions

Convention	Example
Acronyms are spelled out the first time they appear.	Alert Notification System (ANS)
Bold is used for menu names, command options, and dialog box names in primary task procedures.	From the XHQ Workbench , go to the Add menu and click New Component .
<i>Italic</i> is used for glossary terms.	The first step in building this model is to develop reusable software building blocks, called <i>components</i> .
A monospaced font is used for program and code examples.	The subdirectory <code>\log</code> is automatically created below the location you choose. All log files are written to this subdirectory. <code>C:\XHQ</code>
Key combinations appear in uppercase, bold. If joined with a plus sign (+), press and hold the first key while you press the remaining keys.	CTRL+B
In See Also notices, sub-chapter headings are in italics, chapter headings are in quotes, and guide titles are in bold.	For more information, go to the <i>About install.properties</i> topic located in the "Working with PROPERTIES Files" chapter of the XHQ Administrator's Guide .

Visual Cues for Online Viewing

This document uses the following styled paragraphs.

Important notices provide information that are required to completing a given task.



XHQ must run as a domain user.

Warnings tell you that failure to take or avoid a certain action could result in loss of data or application malfunction.



WARNING

Do not modify the `shutdown.dat` template file.

Notes are used to offer information that supplement important points of the main text. Tips suggest certain techniques and procedures that may help you achieve your task quickly.



Depending on your network configuration, include domain information only if the domains are different.

See Also notices provide you with additional references to similar topics and/or concepts within the documentation set. Sub-chapter headings are in italics, chapter headings are in quotes, and guide titles are in bold.



For more information, go to the About the Options Menu topic located in the "Working with PROPERTIES Files" chapter of the **XHQ Administrator's Guide**.

Tips provide additional hints to help you use the product more efficiently.



Use the `NavbarWestVerticalOffset` property to make fine adjustments in pixels. The upper, left-hand corner is the origin. The positive horizontal direction moves to the right and the positive vertical direction moves down.

Web References point you to external web sites that give additional information on the given topic.



Refer to Microsoft support information with regards to the various server settings for application performance and network utilization.

<http://support.microsoft.com>

Related XHQ Product Documentation

The XHQ documentation set includes the following titles.

XHQ Documentation Set

Title	Target Audience
XHQ Administrator's Guide Provides the steps required to begin administering XHQ. It also covers security and access, property settings, redundancy, and localization.	Administrators
XHQ ANS User's Guide Learn how to use and administer the XHQ Alert Notification System (XHQ ANS).	ANS Users, Administrators
XHQ Backup and Recovery Guide Learn how to properly backup XHQ.	Administrators
XHQ Connection Guide Provides information on injecting an XHQ-supported connector type and configuring the connection.	Connector Developers
XHQ Developer's Guide Introduces the XHQ Development Client (Workbench and Solution Builder) user interface and provides information on how to set-up XHQ, develop reusable components, create views, and build a solution hierarchy.	Content and Solution Developers
XHQ Getting Started Gives you step-by-step instruction on how to set up your model and solution.	Content, Connector, and Solution Developers
XHQ Installation Guide Provides the system requirements, installation instructions, and upgrade information for the current release of the XHQ System.	Administrators
XHQ Integrated Data Gateway Guide Includes information on the ADO.NET and the XHQ OPC UA Server.	Application Engineers, Integrators
XHQ Performance Analytics Guide Learn how to use the Engineering Environment to enable the generation of the processes necessary to extract and transform data for source systems, and populate the XHQ Data Store and Data Mart.	Solution Developers/Users, Analysts
XHQ Performance Management Guide Learn how to use Target Management to monitor performance indicators and eLogs to create shift reports.	Administrators, End Users
XHQ Reference Guide Lists the functions and methods used in XHQ, and provides examples,	Content and Solution Developers

Title	Target Audience
usage notes, and parameter descriptions.	
XHQ Reporting Services Guide	Application Engineers, End Users
Introduces the XHQ Reporting Services and provides instruction on how to connect to an XHQ data source.	
XHQ SDK Reference Guide	Application Engineers, Integrators
Provides a set of development tools that allows you to create applications that extend XHQ. Includes information on the Client API and Web Services.	
XHQ Solution Design and Architecture	Solution Architects
Provides best-practice examples for XHQ solution design. Includes information on tag synchronization.	
XHQ Solution Viewer User's Guide	All End Users
Gives you step-by-step instruction on how to access your solution through a browser client and set browser preferences.	
XHQ System Guide	Administrators, Application Engineers, Integrators
Contains information regarding secure handling of an XHQ implementation.	
XHQ Trend Viewer User's Guide	All End Users
Learn how to use the XHQ Trend Viewer to view both real-time and historical data.	

Contacting Customer Support

XHQ Customer Support is a second-level customer support offering, that is, it does not provide XHQ end users with direct support. XHQ end users are to contact their local company help desk or internal application support staff and, in turn, those representatives contact the XHQ Customer Support Team. These representatives are expected to have attended basic product administrative training or possess comparable skills with XHQ, and know and support the specific XHQ customer solution in use.

If the details or response times noted below deviate from those specified in a specific customer contract, the customer contract always takes precedence.

For general XHQ product support or related questions, pre-registered customer or partner support staff with a valid XHQ customer support agreement may contact the XHQ Customer Support Team using any of the following means:

Web Portal

The support portal leverages a system called GTAC (Global Technical Access Center). GTAC provides one common support entry point for many Siemens products. It is available via this URL:

<https://www.siemens.com/gtac>

Customers must be pre-registered to be able to use the web portal. A log-in can be requested at any time by self-registering in the GTAC portal. Note, the end-user "sold to" identifier is needed in order to register.

Use of the support portal is the preferred means to report incidents to the XHQ Customer Support Team unless immediate interactive telephone assistance is required. The support portal is available twenty four hours per day/seven days per week ("24/7").

E-mail

support.xhq@siemens.com

Phone Support and Hours of Coverage

International: +1 (949) 448-7463

U.S. only: +1 (877) 700-4639

The following paid support levels are available:

Bronze Support: 9/5

9 x 5 hours support. 9 hours per day, 5 days per week, Monday to Friday. Daylight Saving Time is honored.

Choice of one coverage zone out of the following options (the default is Americas):

- Americas (7 am - 6 pm PST; 11 hours coverage due to PST/CST/EST time zone coverage overlap)
- South Central Asia (9:30 am - 6 pm IST; 9 hours coverage)

Excludes national holidays as defined by the following countries for the related coverage zone:

- USA/California (Americas)
- India/Pune (South Central Asia)

Example Americas zone: *Implies coverage from 7:00 AM to 6:00 PM, Pacific Time, Monday to Friday, excluding US national holidays.*

Silver Support

Ability to leverage both support coverage zones **Americas** and **South Central Asia** as defined in Bronze for extended daily coverage hours.

The weekly start/end times of coverage follow the local times of the following coverage zone:

- California/USA (Americas)

This implies weekday coverage from 7 am until 6 pm Pacific Time, Monday to Friday, as in the Americas support coverage zone but with the ability to additionally leverage the South-central Asia coverage zone for additional coverage hours.

Gold Support: 24/7

Silver Support coverage plus 24 hours per day, 7 days per week emergency support for Severity One incidents.

Postal Mail

Siemens Industry Software Inc.
XHQ Operations Intelligence
Attn: XHQ Customer Support Department
6 Journey, Suite 200
Aliso Viejo, CA 92656, USA

General Feedback and Comments

Please send an e-mail to:

info.xhq@siemens.com

Siemens Industry Software Inc. and affiliated Siemens Industry Software companies (collectively referred to as "SISW") are committed to working with our customers. Your comments, suggestions, and ideas for improvements are very important to us. Thank you for taking the time to send us your feedback.

1 | Overview

XHQ is enterprise software that runs on a server machine connecting to various backend data sources and allows connections by many different client processes from remote machines. Some of these clients open multiple communication channels when they connect.

This document contains information regarding more secure handling of a customer XHQ implementation.

By default, XHQ undergoes a threat and risk analysis for every release. In this process, measures for improving the standard product are identified and implemented as a matter of course.

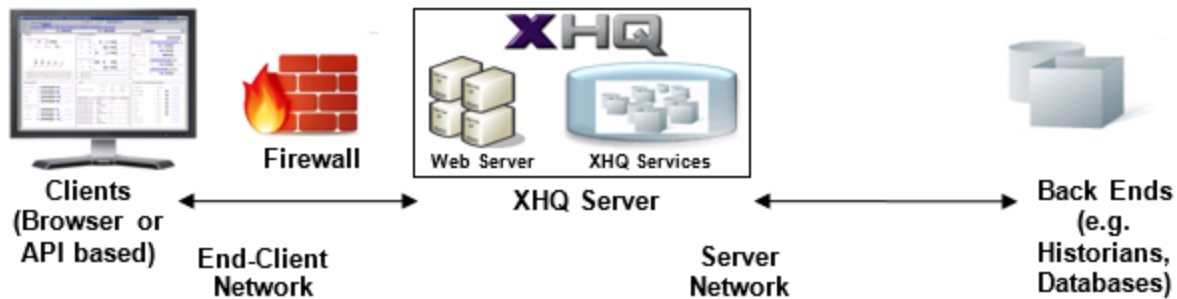
You will find suggestions and recommendations for general technical and organizational security measures at www.siemens.com/industrialsecurity.

Security-relevant settings and recommendations are described in detail in the chapters below and a brief checklist of some key items is also included directly below for convenience.

The key components of XHQ referenced in this document are summarized below:

Key Components	Notes (purpose, location)
XHQ Server Processes: Enterprise (model) Server, Solution Server, Web Server, and, if licensed, Alert Notification Server and/or Application Server	Processes that run on the Windows server host and that execute the functions of the XHQ application (solution).
XHQ Database	Embedded database used internally on the XHQ Server to persist XHQ Solution configurations and information from the layered web applications (e.g., ANS, TM, eLogs).
XHQ Cache Database	Embedded database used internally on the XHQ Server to cache data from customer data sources.
XHQ Data Recorder	Embedded database used to store time series values of customer data. Most common example is: Targets (including future targets).
XHQ Solution Viewer	Web-based client displaying the solution content to end-users.
XHQ Web Applications	Specialized applications with user runtime and administration screens that are accessible via a web browser.
XHQ Developer Tools	Thick client (Windows applications) tools that can be used to manage the system configuration. Note, using these tools does not necessarily require Administration privileges on the client machine.
XHQ IDG / Connector Framework	The Connector Framework uses "intelligent" connection processes to perform data retrieval for specific backend systems such as Historians or Databases. Additional interfaces such as ADO.NET, Web Services, Client API, and OPC are also available.

The typical solution architecture (simplified) is as follows:



Key items to consider

- Periodically review and validate the XHQ Server logs, XHQ Audit Trail, and the Windows event logs and related operating system logging. Validate if the logs are as expected and without any unexplained issues (performance, security, and so forth).
- Ensure the production server has adequate sizing especially CPU cores, fast disks, and memory assigned. Refer to the [XHQ Installation Guide](#) for recommendations.
- The production server should run the latest general availability (GA) XHQ version, which also ensures the most current baseline of security fixes and updates available. Apply any later published updates that were flagged as relevant for security-related topics.
- XHQ configuration setting changes to the property files should be reviewed to ensure they conform to the XHQ version in use and that any unnecessary or outdated settings are removed.
- Check and/or update the Virus Scan exclusions on the server if in conformance with local policies on exclusions and additional means of threat protection are in place.
- Check and/or update the Virus Scan exclusions on the client if in conformance with local policies on exclusions and additional means of threat protection are in place.
- Ensure the XHQ Server is exclusive to XHQ and no unrelated software is installed or running especially no external databases (other than a local Microsoft Access data source possibly) and no external or custom web applications.
- Run the XHQ Server in a suitable and protected (server) network that is separated (with a firewall) from general client(s) network traffic with restricted remote access.
- To access XHQ from outside the corporate network, use the corporate network VPN to obtain intranet access to XHQ, unless XHQ is specifically being used as part of a public cloud solution. In this case, see the topic relating to [public cloud](#) use.
- The traffic to and from the XHQ Server would ideally be monitored for threats in real time by a suitable agent or network solution.

Security Information and Links

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (for example. use of firewalls and network segmentation) in place.

Additionally, guidance from Siemens on appropriate security measures should be taken into account. For more information about industrial security, please visit

<http://www.siemens.com/industrialsecurity>

Siemens products and solutions undergo continuous development to make them more secure. Siemens strongly recommends you apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

<http://www.siemens.com/industrialsecurity>.

To stay informed about general product updates as they occur you can also sign up for a product-specific newsletter. For more information, visit <https://support.automation.siemens.com>.

Holistic Approach

Industrial security solutions require a holistic approach based on different protection levels.

Plant Security

- Protection against access by unauthorized persons
- Physical access protection for critical components

Network Security

- Controlled interfaces between the office and plant networks, e.g. using firewalls
- Additional segmentation of the plant network

System Integrity

- Use of anti-virus software
- Maintenance and update processes
- User authentication for machine or plant operators
- Integrated access protection mechanisms in automation components

Security Management

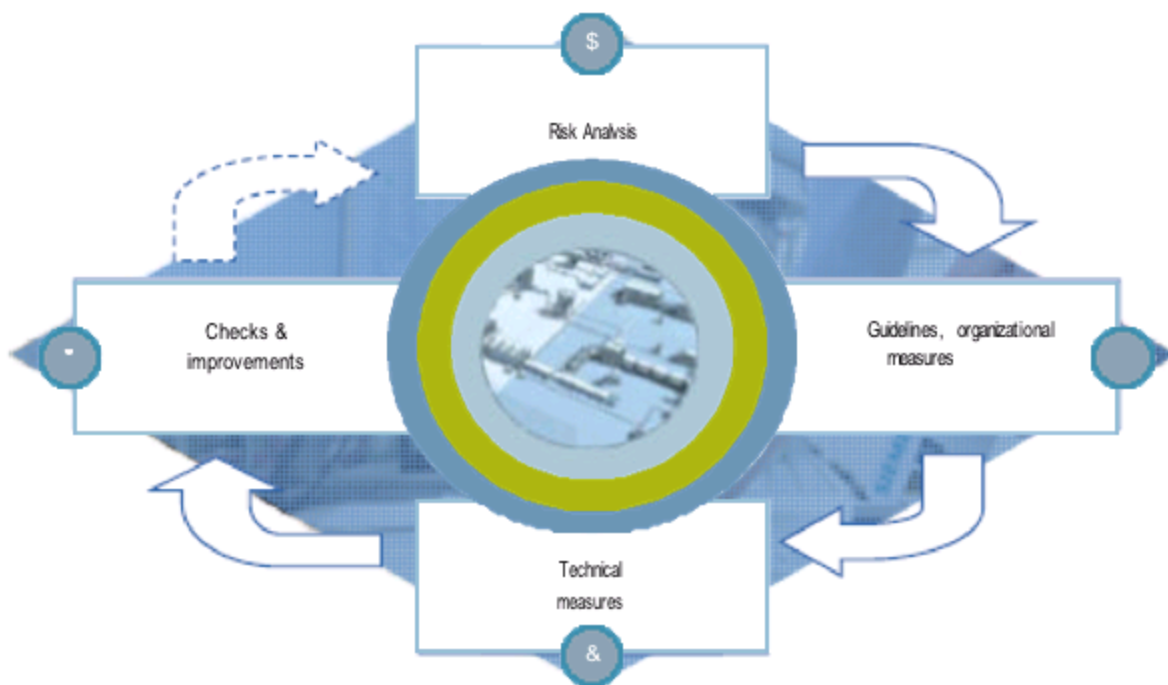
Continuously check security measures and adjust them to your individual requirements.

Security management is an essential component of any industrial security concept. Define security measures to fit your individual plant based on the identified hazards and risks.

A continuous security management process is needed to achieve and maintain a required security level:

- Risk analysis including evaluation of current threats and definition of countermeasures for reducing the risk to an acceptable level
- Agreed-upon organizational and technical measures
- Periodic / event-driven repetition

Products, plants, and processes must meet applicable duty-of-care requirements based on laws, standards, internal guidelines, and the state of the art.



Security Management Process

2 | Third-party Vendors

This section covers some general and third-party vendor related topics. For the third-party vendors such as Microsoft, refer to their security related information directly from their web sites or their published information – the topics below are a cross section representing the most critical areas but the specific guidance can change over time and the direct vendor information should be leveraged since it will be the most current over time.

Microsoft Windows Operating System

The recommended Windows operating server versions are documented in the [XHQ Installation Guide](#).

For this XHQ release, the following are the version recommendations:

- Microsoft Windows Server 2019 is the desired server operating system today from a security and performance perspective. It is understood that not all enterprises are ready for this version, so XHQ also supports Microsoft Windows Server 2016 for those use cases.
- Microsoft Windows 10 is the desired client operating system today from a security and performance perspective.

IT Updates for Microsoft Windows and Oracle Java

Windows should be kept current in terms of Microsoft general and security related patches. These do not require special approval from Siemens before being applied. Changes to the operating system at the level of a new version (for example, Windows Server 2012 R2 compared to Windows Server 2012 or Windows Server 2016) or new service packs do require prior approval, as well as any changes to the documented XHQ prerequisites on the server.

Validation of the latest XHQ release against any new Microsoft Windows service pack is targeted to complete within 60 days of the official market release of such a service pack. Validation of new Microsoft Windows service packs with non-current XHQ versions may take longer or require customers to upgrade XHQ to a newer XHQ version in order to get XHQ support with the new Microsoft Windows service pack.

For the life cycle of the operating system, refer to the Microsoft End-of-Life documentations as out-of-date software may contain security gaps through which malware can be introduced or sensitive data can be spied on.

The supported Windows operating system releases, Visual Studio version, SQL Server version, and browsers are documented in the [XHQ Installation Guide](#). In general, changes in Windows releases (such as version releases or Service Pack versions) or architectures (32-bit or 64-bit, and so forth) require explicit approval for XHQ Systems. However, Windows fixes that are provided as part of a Windows update (such as security fixes) do not require explicit approval for XHQ Systems.

The XHQ development or test environments are recommended to be kept up to date with the latest Windows updates. When applying patches, a pre-validation using an XHQ development or test server is recommended. Although these patches may be acceptable for XHQ, they could still have issues in your IT environment.

Oracle Java Runtime (JRE)

XHQ has provided an HTML5-based runtime client since XHQ version 5.1 onwards. Prior XHQ versions exclusively offered a Java applet-based runtime client. Use of the XHQ solution with the Java applet-based runtime client is *no longer recommended* due to the availability of the HTML5 option, which also has security advantages.



If the Java applet is still required, then Oracle Java version 8 must be installed on the client machines. In this case, the installed Java version should be kept current to the latest version confirmed supported by XHQ until such time that the solution exclusively uses the HTML5-based runtime.

Microsoft Windows UAC

The Windows default is to enable UAC (User Account Control) and this should not be changed or disabled for security reasons.

Observe Microsoft and other third-party vendor security-related information

During installation, configuration, and operation of Microsoft Windows and any other third-party vendor software used on the XHQ Server, observe the security information of the vendor. If not observed, sensitive data may reach unauthorized persons and the integrity of user data may be harmed.

The machine on which the web server is operated should be subject to additional measures for closing potential security gaps (server hardening). For example, deactivate all unneeded user accounts and services.

You can find more information for securing Windows Servers and Clients on the Microsoft Technet and general Microsoft web sites.

You can also refer to the numerous respected web sites dedicated to security topics, such as:

<https://www.us-cert.gov/>

Secure Configuration of the Microsoft IIS Web Server

Comply with the recommendations of the manufacturer regarding security when configuring the web server. For example, you can find more information about secure IIS 8 configuration at:

[https://technet.microsoft.com/en-us/library/jj635855\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj635855(v=ws.11).aspx).

Incorrect configuration produces security gaps that can result in introduction of malware, stealing of sensitive data, and harm to the data integrity.

A specific example of a desirable security configuration is noted below – specifically to counteract clickjacking in this case:

- This requires setting up site-specific information and updating it in the case that the server name is changed or the DNS name is changed, and so forth.
- It is possible to remediate clickjacking by adding CSP header frame-ancestor.
- This can be done by using the HTTP Response Headers GUI in IIS Manager or by adding the following to the web.config.

```
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <add name="Content-Security-Policy" value="frame-ancestors https://site1.com
https://site2.com" />
    </customHeaders>
  </httpProtocol>
</system.webServer>
```

Default IIS installation files are already removed by the XHQ installer, as a best practice. The purpose of these pages is to verify connectivity to the IIS server when first installing and enabling the web server. Default IIS installation files, if available, can be used by attackers to gain valuable information about the infrastructure used and its configuration. Furthermore, default IIS installation files may contain vulnerabilities themselves allowing attackers to compromise the system.

Preventing Malware in Leveraged Documents

Documents that might be leveraged by XHQ (Excel, XML) can contain malicious code. Use an anti-virus program on all XHQ servers and clients.

Only import files from trusted sources. When files are exchanged via e-mail, verify the identity of the sender.

Encrypt and sign e-mails. For exchange via a file system, restrict write permission to those parties who actually need it.

Imported XML files pose a potential risk. Besides the security gaps in software components that process these files, the files can contain incorrect parameters that could cause a production outage. Make sure adequate privileges and rights are assigned to XHQ.

3 | XHQ Server

XHQ Server security depends on a number of factors, the most critical being the following areas.

Usage of a dedicated, adequately sized XHQ Server

Ensure the physical (or virtual) hardware is carefully selected for adequate performance based off the specific customer solution in question and future growth profile (data, users, solution expansion, and so forth).

Multiple applications on one server access the same resources and can cause interference to one another.

Operation of an additional web server and/or database server, for example, on the same computer increases the security risk. This is because when the web server is compromised, the customer data in the database are also at risk.

XHQ must be operated on a dedicated server on which no other applications are run and that is separate from other applications such as databases other than the XHQ embedded database which is expected to be run on the XHQ Server directly.

The XHQ Server recommendations are documented in the XHQ documentation in the [XHQ Installation Guide](#) prerequisites as needing to be exclusive to XHQ. That is, other applications should not run on the XHQ Server or share resources on the actual machine.

Applications, such as IIS, that are either installed or used with the XHQ are exclusive to XHQ and are not available for use by other applications. In addition, such third-party applications are known in some cases to interfere with the XHQ Web Service and indirectly with the ability of the XHQ Server to shut down and start-up automatically.

In addition, there should be no other applications and/or databases installed on the XHQ Server (except the ones required by XHQ, such as third-party clients used for connectivity, or the ones explicitly mentioned in the XHQ product guides) because they can interfere with the operation of the XHQ System by competing for the CPU and memory usage or by installing conflicting versions of required system files or by accessing/locking needed files/resources.

Access from the XHQ Server to the Internet

A server that has direct access to the Internet has a higher risk of being exploited, for example, by an unauthorized program that transfers information about the server or data from the server to an external location.

Protect your XHQ and related web server from direct access to the Internet. It should generally not be possible. In general, it should not be possible to directly access an XHQ Server from the Internet unless XHQ is being used as part of an explicit public cloud solution. In this case, see the topic relating to [public cloud](#) use.

Use of XHQ with a Public Cloud

As noted, a server that has direct access to the Internet has a higher risk of being exploited. Due to this, the first choice is to always place a solution like XHQ within the intranet and have users access via the corporate VPN to ensure one access point that is well monitored and maintained is in use.

If this is not possible (due to use cases requiring public cloud access to the XHQ solution), there are additional safeguards and considerations to be taken into account. The main items are noted below.

Consider if this needs to be the *complete* XHQ solution as is used in the intranet, or only a *subset*. In the subset case, the extranet XHQ Server can be connected to the intranet XHQ Server via the XHQ Connector, for example, to allow a subset of information to be replicated to the extranet. This reduces the attack vector and maximal information loss or access if there is a corporate breach.

The external access needs to be very restrictively firewalled. Siemens recommends only exposing the solution by default via HTTPS (443) for end-user use only, and only through HTML5 for security reasons.

In addition, the latest XHQ version should be deployed and kept current with regard to any vendor updates relating to security. And ensure the underlying operating system is maintained in a secure and current version.

Development and administration use cases should be limited to the intranet access path for added security.

The XHQ Server logs, the Windows logs, and the XHQ Audit Trail need to be part of the general monitoring for the solution to ensure any abnormalities are identified quickly. Ideally, an intrusion detection system and other best practices would also be deployed to identify and notify potential threats and risks.

If Siemens is taking care of the public cloud solution infrastructure, this would be covered by Siemens either as part of an offering like PlantSight or a managed service offering.

If the cloud server only needs to be connected to the corporate network and does not require end-user direct access, a suitable VPN should be deployed to protect against public access. And this use case would then be a private cloud use case and would align more with the intranet use case.

Protection of the XHQ installation media

Inadequate protection of the XHQ installation media can result with it being manipulated.

Always scan the XHQ installation media before usage with a current virus scan.

Make sure that only the server and application administrators and no other users have access to the server on which XHQ is installed.

The relevant MD5 checksum for the current XHQ installation media can be requested from the [XHQ Customer Support Team](#). It is also provided with the uploaded install media by the XHQ Customer Support Team.

XHQ README

Prior to installing XHQ, it is critical to refer to the associated README, which is located at the root directory of the XHQ installation media, for a list of possible installation, upgrade, or migration issues and/or known security related issues.

Access Rights on the XHQ Server

Do not grant end-user accounts access to the XHQ Server.

With access rights, it would be easier for malicious end-users to infiltrate the server with malware.

XHQ itself requires a local administrator account for the XHQ Service and general administration.

XHQ Server Version

XHQ undergoes extensive security checks and intrusion detection scans as part of internal validation. Identified issues are resolved as discovered but the nature of security in this area implies that leveraging the most current XHQ release will always be the most secure version available. From a security perspective alone, aside from bug fixes or enhancements, it is always recommended to adopt the latest release when available.

XHQ patches and updates should be applied when available to ensure the highest security of the system is in place.

Use of the most current XHQ Server version is preferred due to additional system hardening.

General server checks via Windows and XHQ log file analysis

XHQ Server logs and the XHQ Audit Trail must be periodically checked for issues relating to server operation or security. Ideally, this would be done via an automated approach that triggers events on anomalies but it must still be augmented by manual spot checks to ensure the configuration is not tampered with and that use cases that were not considered in the automated monitoring are also identified.

XHQ Authentication Checks

XHQ leverages Windows authentication by default for connection to XHQ (see [XHQ product documentation](#)).

This means each XHQ user is authenticated individually for access to the system. The minimum rights that each user is receives is based on the roles the user is mapped to in the system.

Additional server logging can be temporarily enabled to allow a check if the server authentication is working as expected. This should be checked during the initial project implementation and during any subsequent security audits of the system.

A System Environment Variable must be added:

- `REP_DEBUG_FUNCS=*`

Add/Change the following in `modelsettings.properties`:

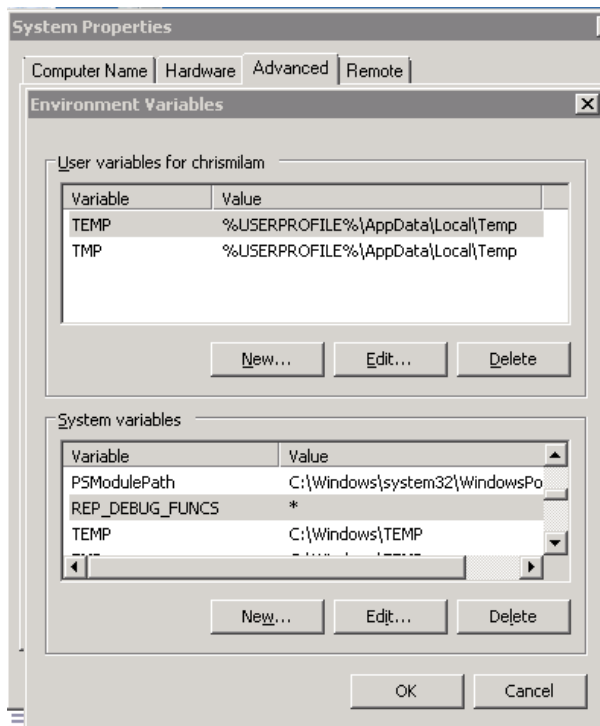
- `net.indx.util.syslog.maxlogsize=500`
- `net.indx.util.syslog.serversystem=4100`

The change to the system environment variable requires a restart of XHQ Service to pick it up.

After restart there will be copious debug messages in `modellog.out` similar to the output of `rep_ugroups util` on the server. Open an XHQ Shell (Run As Administrator) then use the following to get a sense of what the debug looks like:

```
rep_ugroups network\<username>
```

Example of property setting:



XHQ Server Property Files

Disable any unused XHQ subsystems (for example, XHQ ANS, eLogs, XHQ Performance Analytics, Target Management, XHQ Reporting Services, XHQ Data Recorder, and so forth) per the official procedures defined in the [XHQ product documentation](#) or ask the [XHQ Customer Support Team](#) for guidance if in doubt as to the correct and supported manner to accomplish this.

XHQ Import and Export files

Files that are created during an export from XHQ or are imported into XHQ can include sensitive information.

This includes, for example, the XHQ export created files or database exports.

Take the necessary precautions to protect these files from unauthorized access or misuse.

Make sure that the files are protected from theft and manipulation during storage or transfer.

Suitable measures include saving the files to encrypted data storage media or to encrypted file containers as well as sending the data by means of encrypted emails only.

Use XML files from trusted sources only

When you import XML files to XHQ, make sure that the data originates from a trusted source.

XML files could contain manipulated or corrupt contents that could result in a faulty data import and the loss of confidential information.

Server Virus Scan

The following notes apply to virus scanners in general.

The following are the XHQ processes that would ideally be excluded from the virus scan on the server if included in on-access type scanning to improve performance assuming additional processes are in place e.g. to detect malicious content in the network traffic to and from the server and/or by usage of virus scanners that check the server holistically separate to an on-access scan.

In all cases, any installation or upgrade activity on the server should result in a comprehensive scan of the server as should any provided media be scanned before any usage occurs.

xhq_service.exe	xhq_info.exe	xhq_test.exe	xhq_vu.exe
xhq_appserver.exe	xhq_ip21.exe	xhq_routend.exe	xhq_ws.exe
xhq_appsrvend.exe	xhq_ip21w.exe	xhq_router.exe	xhq_webserver.exe
xhq_aserver.exe	xhq_jdbc.exe	xhq_saccess.exe	xhq_websrvend.exe
xhq_asrvend.exe	xhq_mysql.exe	xhq_sacon.exe	xhq_xhq.exe
xhq_auditserver.exe	xhq_native.exe	xhq_sadmin.exe	xhq_xhqci.exe
xhq_auditsrvend.exe	xhq_nativew.exe	xhq_sap.exe	xhq_xhqci_s.exe
xhq_boot.exe	xhq_odbc.exe	xhq_sap3.exe	xhq_xhqci_scon.exe
xhq_catalog.exe	xhq_opc.exe	xhq_sbcon.exe	xhq_xhqdr.exe
xhq_catcon.exe	xhq_opco.exe	xhq_sbuid.exe	xhq_xhqdrcon.exe
xhq_concon.exe	xhq_opcw.exe	xhq_sim.exe	xhq_xhqeci.exe
xhq_connect.exe	xhq_ora.exe	xhq_sith.exe	xhq_xhqecicon.exe
xhq_csrvend.exe	xhq_phd.exe	xhq_sithw.exe	xhq_xhqtestconnect.exe
xhq_dbhist.exe	xhq_phdv.exe	xhq_smck.exe	xhq_xml.exe
xhq_dbhistend.exe	xhq_phdvw.exe	xhq_snmp.exe	launcher.exe
xhq_dde.exe	xhq_phdw.exe	xhq_solcon.exe	
xhq_doc.exe	xhq_pi.exe	xhq_spawn.exe	
xhq_epw.exe	xhq_pisdk.exe	xhq_sserver.exe	
xhq_eserver.exe	xhq_pisdkw.exe	xhq_ssopt.exe	
xhq_esrvend.exe	xhq_piwi.exe	xhq_trigger.exe	
xhq_hostinfo.exe	xhq_ssrvend.exe	xhq_version.exe	

The following file types and locations should be excluded from a virus scan on the server:

```
%XHQ_SERVER_DATA%\mlc\*.dat
%XHQ_SERVER_DATA%\repos\*.dat
%XHQ_SERVER_DATA%\repos\*.properties

%XHQ_DBMS_HOME%\%XHQ_DBMS_VERSION%\*.ctl

%XHQ_CORE_DB_DATA%\*.ctl
%XHQ_CORE_DB_DATA%\*.dbf
%XHQ_CORE_DB_DATA%\*.log
```



```
%XHQ_CACHE_DB_DATA%\*.ctl  
%XHQ_CACHE_DB_DATA%\*.dbf  
%XHQ_CACHE_DB_DATA%\*.log  
  
%XHQ_DR_DB_DATA%\*.ctl  
%XHQ_DR_DB_DATA%\*.dbf  
%XHQ_DR_DB_DATA%\*.log
```

XHQ Embedded Database

The XHQ embedded database is, by default, not accessible via the network. The XHQ installation makes the embedded database only accessible to the XHQ Server locally. This is a very important security setting and should not be changed. If the database were exposed to the network, this would provide more potential entry points for malicious attackers.

The embedded database may not be manipulated or changed or directly accessed by customers. The database is exclusive to XHQ and is exclusively managed by XHQ and any customer provided interfaces or scripts in XHQ.

Updates to the embedded database will be provided as part of general XHQ updates.

Embedded database properties should be configured only via the provided and documented product interfaces and configuration files to avoid errors that might accidentally modify the database configuration incorrectly and to avoid license violations.

The embedded database password is managed by XHQ and can be changed via provided scripts that are documented in the [XHQ Administrator's Guide](#).

XHQ Backup and Recovery

Refer to the XHQ Backup and Recovery Guide for details on how to backup or recover an XHQ System.

The backup files created by the backup commands must be secured in the same manner as the XHQ System against unauthorized access or misuse.

Active Directory and Role-based Security

XHQ supports Microsoft Active Directory for authentication.

The Windows Domain Controllers in the network must be, at the minimum, running Windows Server. This is needed for XHQ to accurately query the group membership of a user.

It is also possible to run all Windows Domain Controllers on Windows Server. Refer to the [XHQ Installation Guide](#) for supported Windows Server.

XHQ roles are mapped to Active Directory groups and are used for defining security access within XHQ to data. XHQ roles are used to restrict access to data at runtime. Due to the mapping of these roles to Active Directory groups it is easy for customers to manage security in a consistent manner within Active Directory groups that are generally defined and used for this purpose with other applications as well.

This approach also reduces XHQ maintenance and the risk of overlooking to change or remove a person that has changed their role or access needs.

XHQ supports the various account types used in Active Directory (domain universal, domain global, domain local) as well as cross-domain authentication. Refer to the [XHQ Administrator's Guide](#) for details.

XHQ Audit Trail

XHQ contains an audit trail that contains a record of all change requests (write, update, delete) and the user that requested the change.

This audit trail should be monitored on a regular basis for any unexpected or suspicious behavior or patterns. The standard Windows audit trail of the server should also be checked in a similar manner and with a similar frequency.

This current release of XHQ provides a comfortable UI where the audit trail can be viewed by a user that has suitable permissions.

XHQ also contains View Statistics, which is a complementary source of data for a general system usage assessment.



Refer to the *XHQ Administrator's Guide* for details.

4 | XHQ End-user Client [Applet]

Client Java Version

For security reasons, the most recent client JRE version (that is supported by the XHQ version in use) should be deployed in the case when the applet-based runtime is in use. The latest supported version can be provided by the XHQ Customer Support Team. Older versions of Java have known bugs, so the most recent versions are strongly recommended.



Refer to the topic, "XHQ Solution Viewer," located in the *XHQ Installation Guide* for supported JRE version(s).

Versions of the Oracle JRE or Internet Explorer require explicit approval for XHQ for applet usage. If the desired version is not documented in the XHQ product guides or the README, a clarification of support can be requested through the XHQ Customer Support Team. For example, if you desire to move to a newer Oracle JRE on the client (common due to security updates), the XHQ Customer Support Team can inform you as to the latest supported version.

Client Property Files

The client-side configuration files should be checked to ensure the technique used to initialize JavaScript is not an older method that is no longer supported. The recommended and supported initialization technique is set forth in the Migration/Statistics section of the README.

Changes to the way the Oracle JRE 1.6 (and higher) initializes the applet has changed the timing of the initialization of JavaScript in the applet. This is seen most commonly in the initialization of client variables. In prior XHQ releases, this was done through the `OnAppletInitListener()` callback method. However, due to the updated initialization of the applet to align with Java 1.6 changes, the supported method of initializing these variables is through the properties file, `clientvariablessettings.properties`. The initialization of the variables can be directly copied to the `clientvariablessettings.properties` file. The references in the `clientvariables.properties` file do not require double quotes for the variable value.

Modify the client files to match the XHQ documentation where specific call-outs need to be made.

Administrator Rights on the XHQ Client

Do not grant end-users Windows administrator rights to end-users on client computers where avoidable.

With administrator rights, it can be easier for users to infiltrate the computer with malware, which damages sensitive data.

Do not grant end-user accounts direct access to the XHQ Server.

XHQ Client View Cache

The XHQ cache location should be in %APPDATA%\IndX and this location should be in the Virus Scan exclusion list respectively the files with the expected endings that exist in the cache should be in the exclusion list.

This location should only be accessible to the related end-user account.

Client Virus Scan

The following notes apply to virus scanners in general. The following locations and/or specific files should be generally excluded from the client virus scan.

The exclusion list of the client should be reviewed to ensure it is current for the latest XHQ version.

The complete client list for XHQ is as follows.

Location:

```
APPDATA\Roaming\IndX
```

Files:

```
**\APPDATA\Roaming\IndX\**\*.iclass  
**\APPDATA\Roaming\IndX\**\*.imagelist  
**\APPDATA\Roaming\IndX\**\*.iobject  
**\APPDATA\Roaming\IndX\**\*.objectid  
**\APPDATA\Roaming\IndX\**\*.oinfo  
**\APPDATA\Roaming\IndX\**\*.rsinfo  
**\APPDATA\Roaming\IndX\**\*.revid  
**\APPDATA\Roaming\IndX\**\*.valueid  
**\APPDATA\Roaming\IndX\**\*.vdata  
**\APPDATA\Roaming\IndX\**\*.viewtableID
```

Encryption and Obfuscation

The Java-based XHQ Solution Viewer (Java applet) uses an encrypted connection to the server to avoid network eavesdropping on the client – server traffic.

The XHQ product code is also encrypted or obfuscated to avoid reverse compilation which would allow a malicious third-party to check for weaknesses or attack vectors.

HTTPS (SSL) should be enabled and used for the web server (IIS) used with XHQ to encrypt that traffic. This is not enabled out of the box in XHQ. See the topic, [Using SSL \(HTTPS\)](#), for information on how to enable SSL by default.

5 | XHQ API, IDG, BI Interfaces

All XHQ interfaces require authorization in order to be used and some additionally require a license key.

Consult the [XHQ product documentation](#) for general use information.

XHQ API

Enable and use HTTPS (SSL), for the web server (IIS) used with XHQ, to encrypt the traffic.

XHQ ADO.NET

XHQ ADO.NET includes standard ADO.NET interfaces for connecting to XHQ data, executing SQL-like queries, and retrieving results. XHQ ADO.NET data provider uses the information provided in connection string to connect to XHQ Server. Connection string can include username and password in plain text. Avoid using username and password fields in connection strings to force the XHQ ADO.NET data provider to use integrated Windows authentication to connect to the XHQ Server.

XHQ BI Data Provider

The XHQ BI Data Provider provides read-only access to XHQ collection data via Open Data Protocol (OData). Web clients and BI tools that can consume OData feed can connect to the XHQ BI Data Provider web service using simple HTTP messages. The guidelines listed in the [XHQ Administrator's Guide](#) section, "Security, Access, and Privileges", apply to XHQ BI Data Provider. HTTPS (SSL) should be enabled and used for the web server (IIS) used with XHQ to encrypt the traffic.

Mobile Devices

Restricting network communication with mobile devices

Devices connected directly to the Internet may have security gaps in their operating system and other installed applications via which malware can be introduced.

For mobile devices, avoid connecting to untrusted networks, for example, many public Wi-Fi hot spots.

Connecting mobile devices only to authorized workstations

Mobile devices could become infected with malware through connection to compromised workstations. Under certain circumstances, sensitive information could be taken from the mobile device in this way.

Connect mobile devices for synchronizing only to trusted workstations that have been designated for synchronization and that comply with the usual security guidelines.

Mobile application

To prevent unauthorized use of the XHQ application, always assign a PIN or equivalent log in protection to the mobile device home screen.

This measure provides additional protection against unauthorized access and use over and above the XHQ authentication of the application e.g. in the event of device loss or theft.

6 | Network

Network Login

Set up a specific and dedicated domain user for XHQ local server administrative usage and grant this user local administration rights on the XHQ Server.



Refer to the [XHQ Administrator's Guide](#) for details.

XHQ Server Network Positioning

The machine, to which you are installing XHQ, must be connected to the network. That is, XHQ must be configured and running on the network with a suitable active LAN connection.

The XHQ Server(s) should be placed in a network segment designed for the express use of IT critical backend servers.

This is typically a network segregated from the general client PC network, with suitable infrastructure (firewalls, and so forth) to improve security and reduce broadcast traffic or interference from the client network(s). It is good IT and security practice to segregate backend servers from end-user clients, ideally with a firewall, to reduce the accessible ports to the clients and the server exposure to the typically noisy broadcasts on the client network, which is a small but not needed load of network traffic that needs to be processed.

Protect XHQ and related web server from direct access to the Internet, unless XHQ is being used as part of an explicit public cloud solution. In this case, see the topic relating to [public cloud](#) use.

This also allows separate rules and policies to be easier applied and to monitor traffic to the server and to ensure the server is only being accessed from desired networks and clients and some traffic can be blocked up front.

This therefore provides an initial protection and hurdle to any bad actor on a client machine or misbehaving client machine.

XHQ Server ISA-95 Positioning

XHQ is generally placed at level 4 in terms of the ISA-95 model hierarchy. XHQ is generally given firewalled access to Plant Historians and other data sources that reside at level 3. Having the bulk of users requiring informational access to operational data go to XHQ instead of to level 3 based systems is a significant improvement in the security of the operational systems since it can reduce the number of users requiring access directly to level 3 based systems and also reduce load on those critical systems since XHQ can multiplex and cache available data efficiently.

Access to the XHQ Server from the Internet

A server that is directly accessible from the Internet has a high risk of being attacked, especially by denial-of-service or hacking.

Protect your XHQ and related web server from direct access from the Internet. It should generally not be possible to directly access an XHQ Server from the Internet unless XHQ is being used as part of an explicit public cloud solution. In this case, see the topic relating to [public cloud](#) use.

If remote access from laptops or mobile devices is needed, access only using a company provided VPN connection since this generally provides encryption, additional authentication, and ensures that only devices and user accounts allowed in the corporate network are used. With VPN, an authentication between the end device and the VPN access server takes place before the start of a session, which enables access to XHQ via a browser or application only after successful log on.

Firewall Usage

The usage of a firewall between the XHQ Server network and the client network(s) is strongly recommended.

For an XHQ Server, client or backend access can be limited to the ports that are noted in the product documentation as being used by XHQ, which removes a large server attack footprint and provides risk mitigation. These are documented in the topic, "Securing XHQ Communication," which is located in the "Security, Access, and Privileges" section of the [XHQ Administrator's Guide](#).

Encryption over the Network

The following topics are noted for completeness:

XHQ encrypts client – server traffic between the applet and the XHQ Server. Passwords are only stored in encrypted fashion and XHQ relies on Active Directory for authentication.

For web applications, XHQ supports HTTPS and recommends the customer install a client certificate and enable HTTPS if layered applications are in use (like ANS).

XHQ has a number of changes in each release that address security related concerns or hardening of the platform. If the customer has an internal department that specializes in validating vendor applications from a security perspective then Siemens is able to work with them and has done this for many other customers in the past which has resulted in many product updates.

The main security risk to the XHQ application is an attacker who gains unauthorized administrator access to the XHQ Server through a security hole. Protecting the XHQ Server from unauthorized access, ensuring all security updates are in place in a timely manner, and vetting all users with administrative access to the server are the most critical security related activities.

Hardening the IIS Configuration

When data are transmitted using the unencrypted HTTP protocol, sensitive customer data can be intercepted and manipulated by third parties. The authentication information (for example, session ID) can also be intercepted and misused.

Configure the web server in such a way that XHQ can be reached only using Hypertext Transfer Protocol Secure (HTTPS). Configure the firewall appropriately so that only incoming connections to TCP/443 are allowed as well as any additional ports documented in the XHQ product guides, depending on the final system configuration and modules. You can find more information on this topic in the [XHQ Administrator's Guide](#), keyword "HTTPS" or "SSL".

In addition, you must import an existing certificate or create a self-signed certificate, and then bind this certificate to the site being used. Again, the site must be secure with a URL prefixed by `https://`. The process of importing the certificate is covered in the [XHQ Administrator's Guide](#). For more information, refer to existing Microsoft documentation on importing/creating certificates.

If you use SSL and query data via HTTPS, you reduce the risk of losing confidential information.

HTTPS (SSL) should be enabled and used for the web server (IIS) used with XHQ to encrypt that traffic. This is not enabled out of the box. It can be enabled in these releases by following the steps covered in the [XHQ Administrator's Guide](#), in the section, "Security, Access, and Privileges".

The customer should obtain and install a suitable certificate for their specific organization to ensure the highest security is in place.

In addition to enabling HTTPS, we recommend applying the IIS headers settings covered in the [XHQ Administrator's Guide](#) > "Security, Access, and Privileges" > "XHQ Web Server Architecture and Security" > "Removing Headers" topic.

About Transport Layer Security

To optimize the effectiveness of using Transport Layer Security (TLS) to protect data in transport, we recommend that you only use modern, secure TLS protocols, such as TLS 1.2. In addition, all clients in the application network environment must also support TLS 1.2.

Support for older protocols, like TLS 1.1 and TLS 1.0 (due to, for example, a business need), must be based on a thorough risk assessment. Policies, compliance, and regulation may restrict the use of the less secure protocols such as TLS 1.0.



To **disable** other protocols, refer to the site:

<https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat>

LAN Manager Authentication Level

We recommend you set the LAN Manager authentication level to the **Send NTLMv2 response only. Refuse LM & NTLM** security setting from the **Local Security Policy** window (Security Settings > Local Policies > Security Options).



Refer to existing Microsoft documentation on setting the Local Security Policy and the following link for more information.

<https://msdn.microsoft.com/en-us/library/ms814176.aspx>

7 | Personal Data Use in XHQ

Personal Data is information that relates, directly or indirectly, to a Data Subject, including without limitation, names, email addresses, postal addresses, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

In the context of this section and XHQ specific usage, Personal Data is defined to be any information that relates, directly or indirectly, to an individual user of XHQ, and includes only such Personal Data entered by an end-user directly or by any authorized entity into or derived from the use of XHQ. Personal Data is a sub-set of XHQ content. It can include without limitation, user names, email addresses, identification numbers, location data, user specific time zone, online identifiers, or a computer's IP address or host name.

Pseudonymisation is a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information.

Personal Data Protection

XHQ is designed to comply with general personal data protection regulations including the General Data Protection Regulation (GDPR) (EU) 2016/679, which is a regulation in EU law on data protection and privacy for all individuals within the European Union.

The following section provides general guidance on the processing and handling of Personal Data within XHQ for information purposes only. For formal regulations and legally binding agreements, refer to the legal agreements in place related to the XHQ platform licensing.

XHQ is primarily a data integration platform for integrating, contextualizing, and visualizing customer operations data and business data.

Due to the nature of XHQ usage in business and operations processes (and typically due to compliance and security reasons), customers generally have a business need to capture and track some limited Personal Data in XHQ.

There are two delineated aspects to XHQ deployment and usage:

1. The XHQ core platform as delivered by Siemens, including the associated product modules, which is the focus of this section, and
2. The implemented and configured XHQ customer-specific solution, which is typically defined and managed by the customer (although Siemens or a partner may implement it for the customer).

With regard to the second item, an XHQ solution is typically managed by the end customer and the solution and related data collected from customer IT systems lies in the responsibility of the customer. Such data can also be a potential source of Personal Data, if Personal Data would be configured to be explicitly retrieved from backend customer systems by customers. This means that customers need to periodically evaluate their XHQ solution and content for compliance with applicable Data Protection guidelines based on their specific usage and data sets since this lies outside the influence of the Siemens core product. Such data may also be visualized by XHQ but the core XHQ product in this case has no implicit understanding of the data itself.

The remainder of this section therefore focuses on the first item noted, the XHQ core platform (that is, the XHQ product), and its associated capabilities as they relate to the storage of Personal Data in the platform as licensed from Siemens to the customer.

The XHQ core platform and modules can contain the following Personal Data if such data is explicitly entered by end-users or bulk imported by a customer or authorized entity:

- User Name
- Domain and User Log in-related information (for example, Windows Log in)
- Email Address
- User preferred Time Zone

The tracking of a user name (where permissible) and the associated data is of importance in a business process to understand and track changes to operations which is often legally required or for compliance purposes. In locations where tracking of user names is not desired or permissible, XHQ provides an option for [pseudonymisation](#) (which is the case, for example, within the general View Statistics and Audit Trail modules).

The following sections describe the various XHQ modules where Personal Data may be managed or leveraged.

Audit Trail Module

The Audit Trail module provides historical tracking of XHQ solution changes, typically for compliance or security-related purposes. Access to the data of this module is limited to a specific subset of users with added privileges, such as an Administrator or a user with explicitly enabled rights to view such statistics.

It is possible to disable the tracking of a user name in these modules ([pseudonymisation](#)) by usage of a system property but, unless this is enabled, the following data can be available:

- User Name, unless pseudonymisation is enabled.
- Domain and User Log in-related information (for example, Windows Log in), unless pseudonymisation is enabled.
- Timestamp, server name, and operation carried out that resulted in a solution change (update/modify/delete).
- Client machine name or IP address.

Important Things to Note

- Read operations are not recorded.
- Records can be purged by an Administrator.

View Statistics Module

The View Statistics module is intended to provide historical tracking of XHQ view usage, typically for security purposes or to provide usage information that allows customers to prioritize view maintenance (for example, improve and optimize heavily used views), remove or rework infrequently used views, assess system load over time to allow performance optimizations, and so forth. Access to the data of this module is limited to a specific subset of users with added privileges, such as an Administrator or a user with explicitly enabled rights to view such statistics.

It is possible to disable the tracking of a user name in these modules ([pseudonymisation](#)) by usage of a system property but, unless this is enabled, the following data can be available:

- User Name, unless pseudonymisation is enabled.
- Domain and User Log in-related information (for example, Windows Log in), unless pseudonymisation is enabled.
- View Name viewed, including View Path and Timestamp (Start and End Dates).
- Client machine name or IP address.

Important Things to Note

- Reports are available that summarize the average and peak number of XHQ view accesses by specific XHQ users over time, including view usage statistics.
- User-related view statistics are unavailable if pseudonymisation is enabled.
- Records can be purged by an Administrator.

XHQ Log Files and XHQ Support Utility

The XHQ log files are intended to be used by system administrators or the XHQ Customer Support Team to primarily analyze and diagnose system problems or performance. Internal system information are logged, including general operation logging and also warnings, errors, or installation-related information.

XHQ log files, depending on the log level chosen, may include the following information as an incidental consequence of the system operation logging:

- Domain and User Name
- Client machine name or IP address

The XHQ Support Utility, by default, contains the XHQ log files since this information is required by the XHQ Customer Support Team to analyze product incident reports. The XHQ Support Utility must be run by a customer and the resulting output is typically reviewed by the customer and then shared with the XHQ Customer Support Team as part of a customer support incident report.

Backup XHQ

An XHQ system backup includes all the noted information for the [Audit Trail module](#), the [View Statistics module](#), and the [XHQ log files](#). Backups are configured, scheduled, and managed by the customer IT organization and need to be managed by the customer in accordance with suitable guidelines to protect access to the included information.

Layered Applications - XHQ Performance Management

The XHQ Performance Management modules provide added functionality such as eLogs, Shift Reports, Alert Notifications, Lost Opportunity, Target Management, and so forth.

The following data is stored related to the module, if provided:

- Email Address
- User preferred Time Zone

Important Things to Note

- The email address is required for end-users to be able to receive email-based alerts or notifications.
- The time zone assists with the calculation of items, such as shift periods.

Retention and Deletion

XHQ defers to the customer organization for data retention and deletion policies and their related implementation, due to the nature of the XHQ platform. XHQ itself will not delete any data without external customer initiation.

There is one exception since, by default, the XHQ log files function as a ring buffer with a fixed (configurable) size and therefore do not retain long term information beyond the configured log file size limits. This typically means that the log files will typically not contain data for more than a few hours to a few days depending on log file defined limits and log level configured. Such log data may, however, be available longer term in customer data backups.

Where XHQ Stores Your Personal Data

All information you provide to XHQ is stored within the XHQ application or associated databases. In many cases, data protection depends on the security of the user account used to authenticate against XHQ, so it is very important to follow corporate and best practice guidelines on protecting your account and log in from unauthorized access, and keeping any related passwords or equivalent credentials confidential.

Safeguarding Your Personal Information

XHQ endeavors to use appropriate security measures at all times to protect your data. The XHQ product has security measures in place to mitigate against the loss, misuse and alteration of the information under the control of the XHQ product. These security measures include SSL certificates to ensure encrypted data is received as it was sent, cookies, and so forth.