Secure Deployment Guide

Proficy Historian

Proprietary Notice

Trademark Notices

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

1 Proficy Historian Overview

GE's Proficy Historian is a high-performance data archiving system designed to collect, store and retrieve time-based data from an Industrial Control System (ICS). This historical ICS data can be useful to operations to assist with monitoring and control, to planners and schedules to optimize their planning and scheduling, and to corporate users and applications to extract business intelligence and track key performance indicators. There are a wide variety and growing uses of ICS historical data, and the Proficy Historian makes that data available where it is needed.

The main purpose of this document is to provide guidance on how to make historical ICS data available where it is needed while minimizing the risk to the availability and integrity of the ICS. This involves deploying and securing the Proficy Historian Servers.

The Proficy Historian Server is one of four parts of the Proficy Historian environment.

> **Collectors** – The Proficy Historian Server collects real-time data and alarms from one or more Collectors on the ICS. GE has developed a wide range of Collectors to get data from different systems, applications and protocols commonly found in ICS. The collectors are typically deployed close to the source of data in order to minimize the loss of data on a network failure.
>
> **Clients** – Users and applications who require historical data are clients to the Proficy Historian Server. Some clients are GE products such as iFIX, CIMPLICITY, Operations Hub and other Proficy Historians. Others are third party applications such as Microsoft Excel. Custom clients or client interfaces can be developed using the Proficy Historian API.
>
> **Proficy Historian Server** – The Proficy Historian Server receives real-time data and alarms from Collectors and makes the ICS historical data available to clients. In some reference security architectures, a Proficy Historian Server may also play the role of a Collector and forward real-time data and alarms to another Proficy Historian Server, see Section 2.4.
>
> **Proficy Historian Administrator** – A client application for managing the Proficy Historian application on the Proficy Historian Server.

This Secure Deployment Guide covers the Proficy Historian Server as well as the security measures related to the connection of Collectors and clients to the Proficy Historian Server.

2 Reference Security Architecture

There are numerous ICS security guideline and standard documents including those available from IEC, ISA, governments and various sector specific groups. A primary focus of these documents is the importance of a security architecture that limits access to the control center, plant floor, SCADA field sites or other portions of the ICS involved in monitoring and control.

These same guideline and standard documents recognize the value in making historical ICS data available to users and applications on the corporate network, and increasingly even to mobile devices on the Internet. The key is to make this historical ICS data available in a way that does not put the integrity or availability of the ICS at risk.

One of the primary purposes of the Proficy Historian System is to make ICS data available to users and applications throughout the enterprise. Therefore, placing the Proficy Historian Servers in the proper security zones, and mediating communication between these zones, is an important part of a reference security architecture.

There are some basic terms and rules to guide the placement of the Proficy Historian Servers in your reference security architecture. The first set of terms define the security zones:

ICS Trusted Zone – Any zone that is used for monitoring and control is considered a trusted zone. This is typically the control center, plant floor in a DCS or field network in a SCADA system. An ICS Trusted Zone is used only for ICS purposes; email, web surfing and other corporate network activities are not allowed in an ICS Trusted Zone. In the ISA 95 / Purdue Enterprise Reference Architecture (PERA) the ICS Trusted Zones would consist of Levels 0, 1 and 2.

Untrusted Zone – The Internet and other public networks are Untrusted Zones. The corporate network is also an Untrusted Zone from an ICS reference security architecture viewpoint. The email, Internet access and large number of users on the corporate network makes it very difficult to maintain a secure environment. In the ISA 95 / PERA the Untrusted Zone would be Level 4, although some organizations have introduced it as a new Level 5.

Semi-Trusted Zone (ICS DMZ) – A Semi-Trusted Zone, also known as an ICS de-militarized zone (ICS DMZ), is deployed to mediate communication between ICS Trusted Zones and Untrusted Zones. An ICS may have one or more ICS DMZ. The ICS DMZ is sometimes considered to be ISA 95 / PERA Level 3, but it is not performing the Level 3 functions. It is more correctly defined as Level 2.5 or Level 3.5.

There is not one, single correct reference security architecture for sharing ICS historical data among all zones using the Proficy Historian System. There is a set of rules that should be followed in creating your reference security architecture:

Rule 1 – No direct access from an Untrusted Zone to an ICS Trusted Zone

Do not allow a user or application on the Untrusted Zone to access a Proficy Historian Server or any other system on the ICS Trusted Zone. An adversary may have compromised the Untrusted Zone and this access could allow the adversary a direct attack path to the ICS.

Rule 2 – No direct access from an ICS Trusted Zone to an Untrusted Zone

Less obvious than Rule 1 but still important. An application or user in the ICS Trusted Zone should not connect to a system on the corporate network. An attacker could use this connection to attack the originating system in the ICS Trusted Zone.

Note: Rules 1 and 2 are the reason one or more ICS DMZ are required. The ICS DMZ mediates the communication between the ICS Trusted Zone and Untrusted Zone that is necessary for operation or business purposes. This includes making historical ICS data available on the corporate network.

Rule 3 – Push data from the more sensitive zone to the less sensitive zone when possible

Rules 1 and 2 prohibit direct connection between an ICS Trusted Zone and an Untrusted Zone, and therefore require the use of an ICS DMZ to share historical ICS data with Untrusted Zones. It is still possible for an attacker to compromise a system on the ICS DMZ from an Untrusted Zone and then use the compromised system on the ICS DMZ to attack the ICS Trusted Zone.

To make this more difficult, TCP connections should be initiated from the more trusted zone when possible.

The Proficy Historian data flow supports Rule 3 for the loading of real-time data and alarms in the Proficy Historian Server. A Collector always initiates the connection to the Proficy Historian Server (TCP/14000) to send, or push, the real-time data to the Proficy Historian Server. This is also true when one Proficy Historian Server is playing the role of a Collector and sending (pushing) data to another Proficy Historian Server.

The following subsections describe three reference security architectures that could be considered to share historical ICS data outside an ICS Trusted Zone.

2.1. Single Proficy Historian Server in the ICS DMZ

This is the simplest reference security architecture as it only has one Proficy Historian Server that is placed in an ICS DMZ, see Figure 1. ICS data is pushed/sent from Proficy Collectors on an ICS Trusted Zone to the Proficy Historian Server in the ICS DMZ. Users and applications on the Corporate Network initiate a connection to the Proficy Historian to access the historical ICS data. The user and applications initiating access from the less sensitive Corporate Network violates Rule 3 in this section, but this may be an acceptable risk because compromise of the Proficy Historian Server would only provide access to the ICS DMZ.

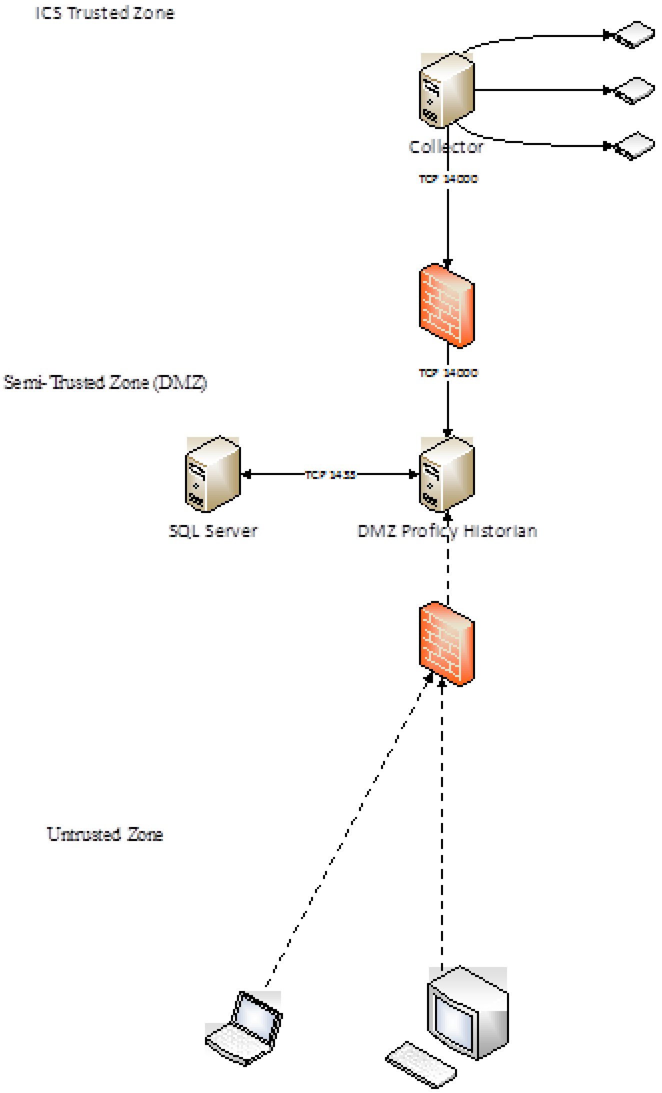


Figure 1 - Single Proficy Historian in the ICS DMZ

This reference security architecture is not recommended if the ICS operators or applications in the ICS Trusted Zone need to access the Proficy Historian Server. Given its exposure to the Corporate Network it should not be relied on by operations to provide data for monitoring and control.

2.2. Proficy Historian Servers in the ICS Trusted Zone and the ICS DMZ

This reference security architecture adds one or more Proficy Historian Servers into the ICS Trusted Zone, see Figure 2. Collectors send the ICS data to a Proficy Historian Server in the ICS Trusted Zone, and this Proficy Historian Server sends the historical ICS data to the Proficy Historian Server in the ICS DMZ.

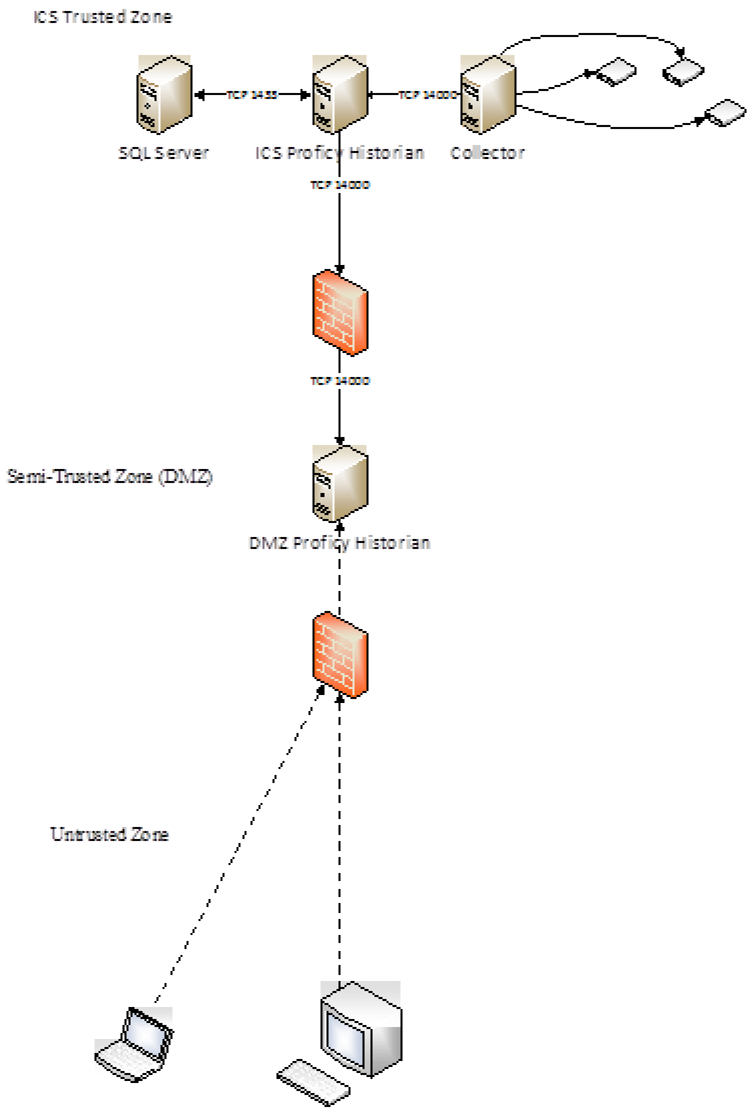


Figure 2 – Proficy Historian Servers in the ICS Trusted Zone and the ICS DMZ

Users and applications in the Corporate Network would connect to the Proficy Historian Server in the ICS DMZ, as in the single Proficy Historian Server reference security architecture in Section 2.1. The users and applications in the ICS Trusted Zone can access ICS data on the Proficy Historian Server in the ICS Trusted Zone without leaving the ICS Trusted Zone. This data can be relied on by operators and engineers as input to control decisions.

The required and authorized connections between the ICS Trusted Zone and ICS DMZ are also reduced in this reference security architecture as compared to the single Proficy Historian architecture in Section 2.1. The only connection required is between a Proficy Historian on the ICS Trusted Zone and a Proficy Historian Server on the ICS DMZ. This compares to each Collector in the ICS Trusted Zone requiring access to the Proficy Historian Server in the ICS DMZ in the single Proficy Historian reference security architecture.

2.3. Proficy Historian Servers in the ICS Trusted Zone, ICS DMZ and Corporate Network

The most secure reference security architecture discussed in this Guide is shown in Figure 3. One or more Proficy Historian Servers are added to Corporate Network. Users and applications on the Corporate Network no longer are allowed to access the ICS DMZ as they can get the historical ICS data from a Proficy Historian Server on the Corporate Network.

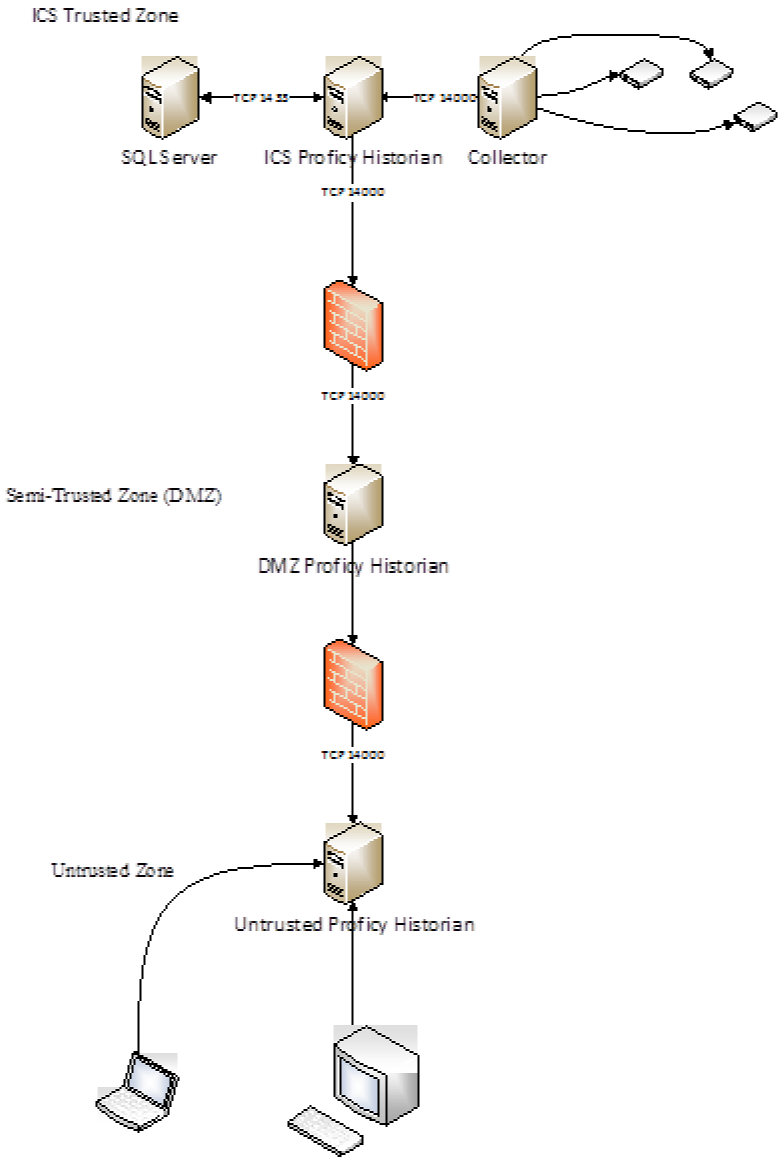


Figure 3 – Proficy Historian Servers in the ICS Trusted Zone, ICS DMZ and Corporate Network

In this reference security architecture, the Proficy Historian Server in the ICS DMZ initiates a connection to the Proficy Historian Server in the Corporate Network and pushes the historical ICS data to the Corporate Network.

This reference architecture is most appropriate when many users and applications on the Corporate Network or other Untrusted Zones require access to ICS historical data. If there is no Proficy Historian Server on the Corporate Network, the firewall would be required to allow many IP addresses on the Corporate Network, possibly the entire Corporate Network subnet, to access the Proficy Historian Server in the ICS DMZ.

2.4. Proficy Historian Server to Proficy Historian Server Communication

The Security Reference Architectures in Figures 2 and 3 show a Proficy Historian Server in a more trusted zone pushing ICS historical data to a Proficy Historian Server in a less trusted zone. This is an important ICS security concept that can provide ICS historical data to users in less secure zones with a low risk to the integrity and availability of the ICS.

There are two methods to push this data from one Proficy Historian Server to another.

1. Server-to-Server Collector

   The Proficy Historian Server that is pushing the ICS historical data from the more trusted zone functions as a Collector. The Server-to-Server Collector initiates a TCP session with the Proficy Historian Server in the less trusted zone on TCP 14000, similar to any other Proficy Collector.

   While the Server-to-Server Collector initiates the communication, the Proficy Historian Server in the less trusted zone determines what data is pushed to it. There is a risk that a compromised Proficy Historian Server in the less trusted zone, or compromised administrator credentials or computer, could request data that was not authorized for the less trusted zone. This is an issue of ICS historical data confidentiality, not an issue that could affect the availability or integrity of the ICS.

2. Server-to-Server Distributor

   The Server-to-Server Distributor is another option to push ICS historical data from one Proficy Historian Server to another Proficy Historian Server. Either Proficy Historian Server involved in the Distributor server-to-server communication can configure what points are pushed out to the receiving server.

   There is a security benefit to having the Proficy Historian Server in the more secure zone determine what points are pushed to less secure zone. However, the Proficy Historian Server receiving the data also has the ability to determine what points it receives, so the security benefit of using the Server-to-Server Distributor is minimized.

If the confidentiality of the ICS historical data is important, asset owners should consider the reference security architecture in Figure 3. The Proficy Historian Server in the ICS DMZ can determine what points are sent to it, and therefore what points would be available to the Proficy Historian Server in the Untrusted Zone. Even if the Proficy Historian Server in the Untrusted Zone was compromised, it would not be able to access data from the Proficy Historian Server in the ICS Trusted Zone that was not pushed to the ICS DMZ.

2.5. SQL Server Database

The Proficy Historian stores alarms in a Microsoft SQL Server database. This database can be installed on the Proficy Historian Server or on a separate server for improved performance.

The reference security architectures in Figures 1 – 3 show the SQL Server Database being deployed on a separate server in the most trusted zone, usually the ICS Trusted Zone. Alarms are often used only by the Operations Group and not replicated outside the ICS Trusted Zone. This however is expected to change as alarm and other historical ICS data is increasingly being used in advanced analysis.

The choice of whether the database is on the Proficy Historian Server is primarily a performance decision. The following are some factors that might warrant deploying a separate SQL Server:

- A large number of alarms
- Longer term alarm data being available in the Proficy Historian Server
- A large number of Proficy Clients accessing alarm data

If a separate SQL Server is deployed, the Historian Alarm Archiver service on the Proficy Historian Server must be allowed to login to the SQL Server via Windows Authentication.

The Proficy Historian Server installation process installs the SQL Server application in Mixed Authentication Mode. After installation the authentication mode should be changed to Windows Authentication mode to eliminate SQL Server Authentication.

2.6. Security Perimeter Firewall Rulesets

Historical ICS data is sent (pushed) from a Collector to a Proficy Historian Server on TCP/14000. This is also true when a Proficy Historian Server acts as a Collector and pushes data to another Proficy Historian Server in a less trusted zone. The ability to push data combined with the need to only allow one TCP port through the firewall supports the good practice security reference architecture described in Section 2. The firewall rules required per reference security architecture are:

Section 2.1 - Single Proficy Historian Server in the ICS DMZ

Source	Destination	Destination Port
All Collectors in ICS Trusted Zone	Proficy Historian Server in ICS DMZ	TCP/14000
Client on Corporate Network	Proficy Historian Server in ICS DMZ	TCP/14000

Section 2.2 - Proficy Historian Servers in the ICS Trusted Zone and the ICS DMZ

Source	Destination	Destination Port
Proficy Historian Server in ICS Trusted Zone	Proficy Historian Server in ICS DMZ	TCP/14000
Client on Corporate Network	Proficy Historian Server in ICS DMZ	TCP/14000

Section 2.3 - Proficy Historian Servers in the ICS Trusted Zone, ICS DMZ and Corporate Network

Source	Destination	Destination Port
Proficy Historian Server in ICS Trusted Zone	Proficy Historian Server in ICS DMZ	TCP/14000
Proficy Historian Server in ICS DMZ	Proficy Historian Server in Corporate Network	TCP/14000

3 Securing the Proficy Historian Server Platform

3.1. Redundancy

The Proficy Historian offers numerous possible redundancy solutions to ensure historical ICS data is not lost or temporarily unavailable due to one or more components in the Proficy Historian being unavailable.

Redundancy benefits begin with the Collectors, which can store data for a period of time if the Proficy Historian Server is unavailable to receive the data. Once the Proficy Historian Server is available the recorded data will be sent to the Proficy Historian Server. Collectors also have Recovery Modes that regenerate calculations as required and send them to the recovered Proficy Historian Server.

The redundancy benefits of the Collectors are limited to preventing the loss of the historical ICS data. Redundant Proficy Historian Servers should be considered for high availability requirements related to the historical ICS data. For example, if operators in the control room require access to historical ICS data for operational decisions, high availability of the Proficy Historian Server in the ICS Trusted Zone may be required.

The Proficy Historian Server can be deployed with high availability using Microsoft's Cluster Server. If the primary node in the cluster is unavailable, another node in the cluster assumes the role of primary node.

The Proficy Historian Server can be deployed with high availability, improved read performance using "Historian Mirroring Server Setup". For high availability mirror nodes serve the client requirements if primary server went down.

Proficy Historian Servers in different security zones should generally not be considered as redundancy for the availability of the historical ICS data.

3.2. Operating System Selection

The Proficy Historian Server runs on many versions of Microsoft Server operating system (OS). The key is to install and maintain the Proficy Historian Server on an OS that is supported by Microsoft so that security patches will be available for published vulnerabilities. Microsoft typically provides extended support for ten or more years after the initial release of an OS, and Microsoft provides at least five years notice of when extended support for a Microsoft Server OS will end.

Proficy Historian Server users should insure there is a plan to upgrade the Microsoft Server OS before extended support and security patches ends. This likely will require updating the OS with a service pack periodically since Microsoft typically supports the current and previous service pack for each OS.

3.3. Minimize Attack Surface

Every listening port, running service and installed application is something that could have a software vulnerability. By limiting what is on the Proficy Historian Server to what is required for operation, organizations will be limiting the attack surface --- what is available for an attacker to potentially compromise. A secondary benefit of minimizing the attack surface is it reduces the security patching burden.

The information in Sections 3.3.1 – 3.3.3 identify what software, running services and listening ports are necessary for the Proficy Historian Server to operate. If an organization is using the same server for other applications additional installed software, running services and listening ports may be necessary. This is not necessarily a security issue as long as the attack surface is minimized and the other software installed is for a purpose appropriate for the security zone the Proficy Historian Server is located in.

3.3.1. Software

The following software applications are required on a Proficy Historian Server.

- M4 Common Licensing (GE-IP Software Licensing Service)
- Microsoft .NET Framework
- Microsoft Application Error Reporting
- Microsoft SQL Server (May be deployed on separate server, see Section 2.4)
- Microsoft Visual C++ Redistributable
- OPC Core Components
- Proficy Alarm and Event Database
- Proficy Historian

Software on a Proficy Historian Server that is not on the above list should be evaluated to determine if it is required for operation. If it is not necessary, remove the software from the Proficy Historian Server.

All software should be running a version that is supported by the software vendor and should be added to the ICS inventory and the ICS security patching program.

3.3.2. Running Services

The list of running services required by the Proficy Historian Server are listed in the table below. Any additional services should be investigated to determine if they are required for operation and added to the inventory as appropriate.

Caption	Command Line
System Idle Process	
System	
smss.exe	\SystemRoot\System32\smss.exe

Caption	Command Line
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024
wininit.exe	wininit.exe
winlogon.exe	winlogon.exe
services.exe	C:\Windows\system32\services.exe
lsass.exe	C:\Windows\system32\lsass.exe
lsm.exe	C:\Windows\system32\lsm.exe
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService
svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
spoolsv.exe	C:\Windows\System32\spoolsv.exe
CCFLIC0.exe	C:\Program Files (x86)\Proficy\Proficy Common\M4 Common Licensing\CCFLIC0.exe
ihAlarmArchiver.exe	C:\Program Files (x86)\Proficy\Proficy Historian\Server\ihAlarmArchiver.exe
ihDataArchiver_x64.exe	C:\Program Files (x86)\Proficy\Proficy Historian\x64\Server\ihDataArchiver_x64.exe
ihClientManager_x64.exe	C:\Program Files (x86)\Proficy\Proficy Historian\x64\Server\ihClientManager_x64.exe
ihConfigManager_x64.exe	C:\Program Files (x86)\Proficy\Proficy Historian\x64\Server\ihConfigManager_x64.exe
ihFileCollector.exe	C:\Program Files\Proficy\Proficy Historian\x86\Server\ihFileCollector.exe

Caption	Command Line
ihSimulationCollector.exe	C:\Program Files\Proficy\Proficy Historian\x86\Server\ihSimulationCollector.exe
iLicenseSvc.exe	C:\Program Files (x86)\M1 Licensing\iLicenseSvc.exe
sqlservr.exe	c:\Program Files (x86)\Microsoft SQL Server\MSSQL10.PROFICYHIST\MSSQL\Binn\sqlservr.exe -sPROFICYHIST
svchost.exe	C:\Windows\system32\svchost.exe -k regsvc
sqlbrowser.exe	c:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe
sqlwriter.exe	c:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe
wlms.exe	C:\Windows\system32\wlms\wlms.exe
sppsvc.exe	C:\Windows\system32\sppsvc.exe
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
dllhost.exe	C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
msdtc.exe	C:\Windows\System32\msdtc.exe
taskhost.exe	taskhost.exe
dwm.exe	C:\Windows\system32\Dwm.exe
conhost.exe	\??\C:\Windows\system32\conhost.exe "-11467990541255728412528426061104247236180477918812586391227224969941685062095
explorer.exe	C:\Windows\Explorer.EXE
TrustedInstaller.exe	C:\Windows\servicing\TrustedInstaller.exe
cmd.exe	C:\Windows\system32\cmd.exe
conhost.exe	\??\C:\Windows\system32\conhost.exe "-1246894368-965463825-1302456613-8015155911396530-905067131-478455922-1017161488
wuauclt.exe	C:\Windows\system32\wuauclt.exe
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe

Caption	Command Line
msiexec.exe	C:\Windows\system32\msiexec.exe /V
WMIADAP.exe	wmiadap.exe /F /T /R
WMIC.exe	wmic process get /format:csv

3.3.3. Listening Ports

Listening TCP and UDP ports are the means in which a remote adversary can attack the Proficy Historian Server.

Listening Port	Application / Protocol
TCP/135	Windows / DCE Endpoint Resolution
UDP/137	Windows / NETBIOS
UDP/138	Windows / NETBIOS
TCP/139	Windows / NETBIOS
TCP/445	Windows / CIFS
TCP/1433	SQL Server (if separate SQL Server is deployed)
UDP/1434	SQL Server / MSSQL
UDP/5355	Windows
TCP/8008	Proficy Historian / Data Archiver Client Service
TCP/13000	Proficy Historian / Data Archiver Client Service
TCP/14000	Proficy Historian / Data Archiver (Standard)
TCP/14000	Proficy Historian / Client Manager (Enterprise)
TCP/14001	Proficy Historian / Data Archiver (Enterprise)
TCP/14002	Proficy Historian /Config Manager (Enterprise)
TCP/14003	Proficy Historian / Diagnostics Manager (Enterprise)

Additional software of functionality can open additional ports. For example, if IPSEC is deployed it is likely that UDP/500 and UDP/4500 will be listening.

In additional Microsoft services will open short lived and automatically selected ports (ephemeral ports), typically in the port range 49152 – 65535. Other applications may also open ephemeral ports. If a port is not recognized, the service related to that port should be investigated to determine if it is required for operation.

3.4. Default Accounts

Windows Server installs a default Guest account and a default Administrator account. The Guest account should be disabled, and the Administrator account should be renamed and not used. Each user, including Administrators, should have his or her own unique account.

The Microsoft SQL Server database also has a default sa account. This account should be disabled and individual system administrator accounts created as necessary.

3.5. Other Windows Security Settings

A Windows OS has hundreds of security settings. Microsoft and industry organizations, such as the Center for Internet Security (CIS), provide good security practice recommendations for each of these security settings. The Bandolier Security Audit File discussed in Section 5 will audit a Proficy Historian Server to these good security practice recommendations.

A portion of the OS security configuration recommendations are covered in the 3.5 subsections below. This is not a complete list; view the Microsoft or CIS guidance for a full set of Microsoft Server security configuration recommendations.

3.5.1. Password Policy

The Windows OS can enforce a password policy. The organization's password policy, if it exists, should be applied. The Microsoft and Center for Internet Security password policy recommendations are:

- Account Lockout Duration: 15
- Account Lockout Threshold: 15
- Reset Lockout account counter after: 15
- Enforce Password History: 24
- Maximum Password age: 90
- Minimum password age: 1
- Minimum password length: 8
- Password meet complexity requirements: Enabled

3.5.2. Audit Policy

The Windows audit policy will determine what security events are logged. Security event logs are helpful for after incident investigation and for detecting security incidents if the logs are monitored. Microsoft and the Center for Internet Security recommend the following audit policy:

- Audit Logon Events – Success, Failure
- Audit IPSec Driver Events – Success, Failure
- Audit Security State Change Events – Success, Failure
- Audit Security System Extension Events – Success, Failure
- Audit Process Creation Events – Success

- Audit Audit Policy Change Events – Success, Failure
- Audit Other Account Management Events – Success
- Audit Account Lockout Events – Success, Failure
- Audit Authentication Policy Change – Success, Failure
- Audit Authorization Policy Change Events – Success, Failure
- Audit Certification Service Events – Success, Failure
- Audit Computer Account Management Events – Success, Failure
- Audit Credential Validation Events – Success
- Audit Distribution Group Management Events – Success, Failure
- Audit File Share Events – Failure
- Audit Filtering Platform Policy Change Events – Success, Failure
- Audit Handle Manipulation Events – Failure
- Audit Logoff Events – Success
- Audit MPSSVC Rule-Level Policy Change Events – Success
- Audit Non-Sensitive Privilege Use Events – Failure
- Audit Other Account Logon Events – Success, Failure
- Audit other Logon/Logoff Events – Success, Failure
- Audit Other Object Access Events – Success
- Audit Registry Events – Failure
- Audit Security Group Management Events – Success, Failure
- Audit Special Logon Events – Success, Failure
- Audit User Account Management Events – Success, Failure

3.5.3. Enable Data Execution Prevention (DEP)

Data execution prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits. This good security practice does not interfere with the proper operation of the Proficy Historian Server and should be set to "Turn on DEP for all programs and services except those I select" to select the OptOut policy.

3.5.4. Signing the Components

All Historian components were digitally signed by trusted certificate. Which will give more trust on shipped components by GE to the end customer.

4 Securing the Proficy Historian Application

4.1. Proficy Historian Server Application Installation

During installation of the Proficy Historian Server application, there are choices that must be made, and some of these choices have security implications. The security related install options are listed below along with the recommended secure installation choice and rationale for that choice.

User Accounts Granted Administrative Access

Choices: All Users or Specific Users

Select “Specific Users” and enter the username. This user can be part of a domain or a local account on the Proficy Historian Server.

Do not select “All Users”. This selection introduces a security vulnerability as all users in the domain or with local accounts would have administrative rights to the Proficy Historian Server.

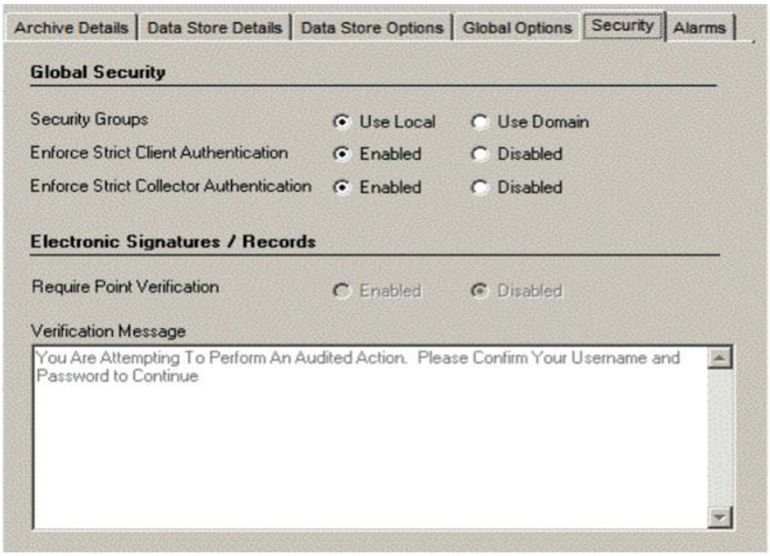
Historian Collector Services Account

Choices: Enter service account name and password or leave blank

Enter a username and password for the Collector Services account. The password should at least meet your organization’s password policy. Since this password will rarely be entered, consider increasing the length and complexity over what is required for a user password. Do not leave this selection blank; this would cause the Collector Services to run under the local system account, which is a bad security practice.

4.2. Strict Authentication

The Proficy Historian Server implements a Strict Authentication security feature for clients and Collectors. Strict Authentication is turned on by default in Proficy Historian Server Version 5.5 and later. This feature requires a user or service account in the domain, if applicable, or on the local system for client or Collector access.



Global Security

Security Groups ● Use Local ○ Use Domain

Enforce Strict Client Authentication ● Enabled ○ Disabled

Enforce Strict Collector Authentication ● Enabled ○ Disabled

Electronic Signatures / Records

Require Point Verification ○ Enabled ● Disabled

Verification Message

You Are Attempting To Perform An Audited Action. Please Confirm Your Username and Password to Continue

Figure 4 – Security Tab in Historian Administrator

Turning Strict Authentication off eliminates the requirement for a client or collector to authenticate to the Proficy Historian Server to perform client or collector activities. This would allow any attacker or malware with network access to the Proficy Historian Server to compromise the availability and integrity of the historical ICS data and is not recommended. The Strict Authentication configuration settings are found in the Security Tab in the Historian Administrator client, see Figure 4.

Below table provides guidelines about the different combinations of strict client and collector authentication options and their use:

Strict Client Authentication	Strict Collector Authentication	Comment
Enabled	Enabled	Use this for highest available security. You will need to install SIMs, if available on all pre-6.0 collectors and clients. Clients can refer to any program that connects to the Data Archiver. This includes Historian Administrator, Microsoft Excel, any OLEDB program, user written programs, or any other Proficy software.
Enabled	Disabled	Use this if you are unable to upgrade collectors to the latest version if there is no SIM update for your collector.
Disabled	Enabled	Use this if you have to support legacy clients and you are unable to install the SIM update on all clients.
Disabled	Disabled	Use this for maximum compatibility with existing systems.

4.3. Proficy Historian Security Groups

The Proficy Historian Server supports role-based access control with the following roles:

- **iH Security Admins:** Historian power security users. Security Administrators have rights to all Historian functions. This group also has the ability to change tag level security, archive security, and modify the Electronic Records and Signatures option. This is the only Historian security group that overrides tag level security.
- **iH Collector Admins**: Allowed to start and stop collectors, browse collectors, configure collectors, and add new collectors.
- **iH Tag Admins:** Allowed to create, modify, and remove tags. Tag level security can override rights given to other Historian security groups. Tag Admins can also browse collectors.
- **iH Archive Admins:** Allowed to create, modify, remove, backup, and restore archives.
- **iH UnAudited Logins:** Allowed to connect the DataArchiver without creating login successful audit messages.

- **iH UnAudited Writers:** Allowed to write data without creating any messages. iH UnAudited Logins – Allowed to connect the DataArchiver without creating login successful audit messages.
- **iH Audited Writers:** Allowed to write data and to produce a message each time a data value is added or changed.
- **iH Readers:** Allowed to read data and system statistics. Also allowed access to Historian Administrator.

An organization may not require all of these roles and should determine what roles fit the operation and monitoring of their ICS. The Proficy Historian Security Groups are defined either on the Local Server or in a domain based on the setting of the option on the Security Tab of the Data Store Maintenance screen in the Historian Administrator client, see Figure 4.

It is essential that an iH Security Admins security group be added to the Local Server or domain, as appropriate. If this iH Security Admins security group does not exist, all authenticated users will have administrator privileges to Proficy Historian Server application.

The other security groups work in a similar way. If the security group does not exist for a function that is covered by that security group, then all authenticated users will have that privilege. An exception is if tag security group has been created that covers that function for the specified tag. Tag base access control, discussed in Section 4.4, has priority over role based access control in most cases. The only exception is users in the iH Security Administrators security group have no restrictions.

A security group for each role should be created, with the exact naming, to avoid the possibility of all users having unintended Proficy Historian privileges.

The Proficy team has developed two PowerShell scripts to add all of the Proficy Historian Security Groups.

- add_groups_local.ps1 adds all of the Proficy Historian Security Groups to the Local Server it is run on. The PowerShell script must be run by a user with Administrator rights.
- add_groups_domain.ps1 adds all of the Proficy Historian Security Groups to the Domain it is run on. The PowerShell script must be run by a Domain Administrator.

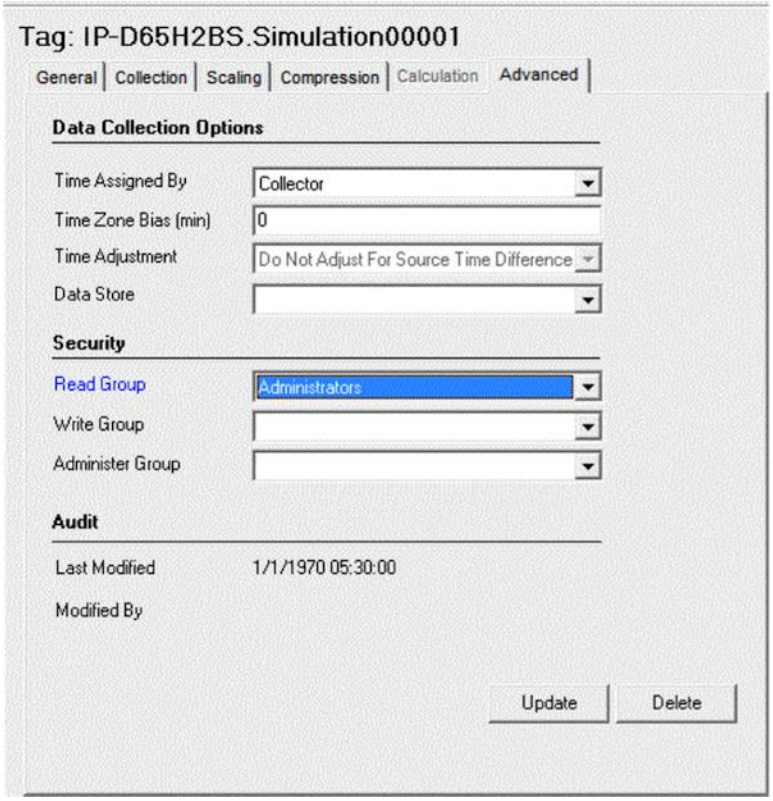
Neither of these PowerShell scripts adds a user to any of the Proficy Historian Security Groups. The scripts only create the groups to prevent unintentional Proficy privileges being provided to all local or domain users.

4.4. Tag Level Security

The Proficy Historian Server also supports tag-based access control. This is recommended if there are specific high impact tags that should not be read, written to or modified by a role that would normally have those permissions. The tag-based access control settings take priority over the role-based privileges with the sole exception of the iH Security Administrator role. The Security Administrator has the ability to read, write and perform administrative functions on all tags in the Proficy Historian regardless of any tag level access control.

Tag level security is configured in the Tag Maintenance screen of the Historian Administrator client, see Figure 5. Each tag or group of tags can have a Windows security group assigned for Read, Write and Administer privileges. These Windows security groups could be the Proficy Historian security groups discussed in Section 4.3, but more likely they will be specially created Windows security groups based on the collection of tags.

In addition to providing more granular authorization on specific tags, tag level security can also be used to create Areas of Responsibility (AoR). This is common in Proficy Historian Servers that collect, store and make available historical ICS data from multiple plants or SCADA systems. One group of users responsible for a plant may need writer privileges for their plant and read privileges for another plant. By layering role based and tag based access control this and most other desired authorization schemes are possible with the Proficy Historian Server.



Tag: IP-D65H2BS.Simulation00001

Data Collection Options

Time Assigned By: Collector

Time Zone Bias (min): 0

Time Adjustment: Do Not Adjust For Source Time Difference

Data Store:

Security

Read Group: Administrators

Write Group:

Administer Group:

Audit

Last Modified: 1/1/1970 05:30:00

Modified By:

Figure 5 – Tag Maintenance Tab in Historian Administrator

4.5. Privileges on Proficy Historian Server Directories

The least privilege security principle should also be applied to file and folder access. The Proficy Historian Server installation process creates the folders listed in the table below. The required privileges for Proficy Historian Server operation are listed for each folder.

4.6. Securing Communication Between Proficy Historian Components

The communication between the Collectors and Proficy Historian Server, as well as communication between two Proficy Historian Servers, does not have native security controls. There is no encryption to prevent a loss of confidentiality, and there is no authentication to detect a loss of integrity. While it is a good security practice to secure all communication between servers and components, the threat to the communication is indirectly correlated to the trustworthiness of the zone. For example, the threat to communication between a Collector and Proficy Historian Server both on the ICS Trusted Zone would be small compared to the threat to communication between a Proficy Historian Server on an ICS DMZ and a Proficy Historian Server on the Corporate Network (an Untrusted Zone).

IPSEC can be used to encrypt and authenticate communication between Proficy Historian components if this is a security requirement. This is a security protocol supported by the Microsoft Windows Server OS, and there are no special requirements to implement this for Collector to Proficy Historian Server or Proficy Historian Server to Proficy Historian Server communications. If IPSEC is deployed there will be changes required in the firewall ruleset to allow IPSEC communication through the firewall rather than TCP/14000 communication.

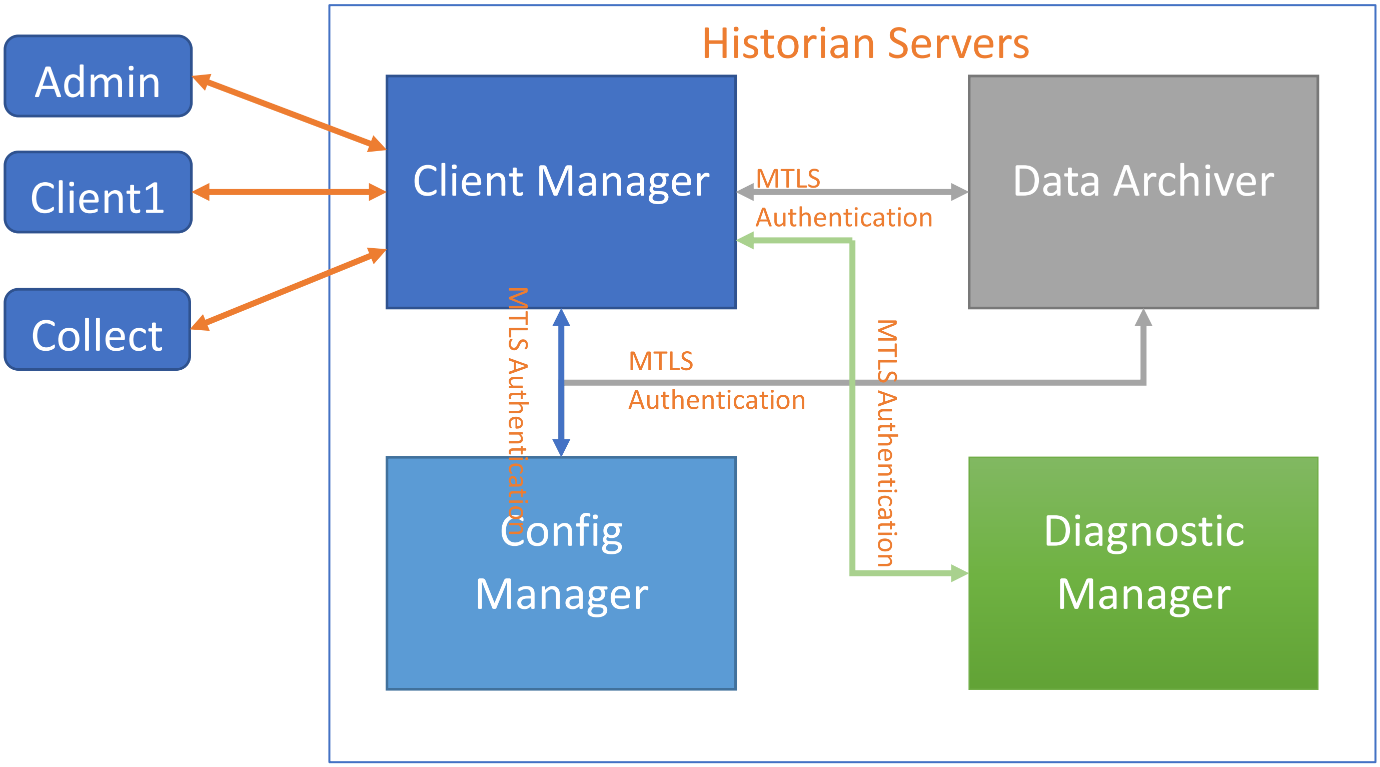
At a minimum, all Proficy Historian Server communication over a public network should be encrypted in transit. For example, the data should be encrypted if it is sent from a factory to the corporate headquarters over a public network. Another example is data sent to a vendor or third party over the Internet should be encrypted.

Proficy Historian Server customers should make the security decision on encryption in transit between Proficy Historian components based on:

- the impact if data confidentiality is lost (the data can be recovered by an adversary)
- the impact if data integrity is lost (the data is modified in transit)
- the security of network used to pass the data between Proficy Historian Components

4.6.1 Certificate based Authentication between Historian Servers

Mutual TLS design approach used for trusted authentication between Proficy Historian Servers (Client Manager, Data Archiver, Configuration Manager, Diagnostics Manager). Implementing Mutual TLS using Microsoft SSPI SChannel api is used. For more information, please refer: https://learn.microsoft.com/en-us/windows/win32/secauthn/initializesecuritycontext--schannel



Example: Data Archiver (DA) securely authenticating Client Manager (CM)

When CM trying to connect to DA

DA presents its TLS certificate.

CM verifies the DA's certificate.

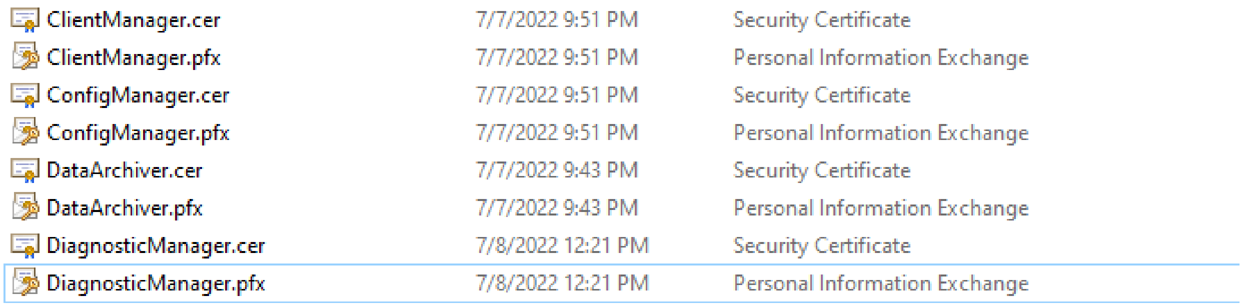
CM presents its TLS certificate.

DA verifies the CM's certificate.

DA grants access.

CM and DA authenticates each other over encrypted TLS connection. Similarly each server authenticates securely with other servers.

For incorporating this functionality, Proficy Historian 2023 installer ships below certificates in the path: C:\Program Files\Proficy\Proficy Historian\MTLS



ClientManager.cer	7/7/2022 9:51 PM	Security Certificate
ClientManager.pfx	7/7/2022 9:51 PM	Personal Information Exchange
ConfigManager.cer	7/7/2022 9:51 PM	Security Certificate
ConfigManager.pfx	7/7/2022 9:51 PM	Personal Information Exchange
DataArchiver.cer	7/7/2022 9:43 PM	Security Certificate
DataArchiver.pfx	7/7/2022 9:43 PM	Personal Information Exchange
DiagnosticManager.cer	7/8/2022 12:21 PM	Security Certificate
DiagnosticManager.pfx	7/8/2022 12:21 PM	Personal Information Exchange

4.7. Backup and Recovery

Redundancy is often used in ICS to deal with hardware and software failures that make the primary system unavailable. Redundancy is typically less effective in the case of a cyber-attack because the redundant system is susceptible to the same attack that made the primary system unavailable. Therefore, it is important to implement a backup and recovery process that meets the recovery time requirements set by management. These requirements are likely to vary based on what the historical ICS data is used for and other industry or company specific factors.

There are three parts to restoring the Proficy Historian Server:

1. Restoring the computing platform, operating system and Proficy Historian applications

The same process that was used for the initial install of the Proficy Historian can be used to restore the Proficy Historian Server to its initial, pre-configured state. This requires the appropriate software be readily available.

Imaging and other solutions can make restoration faster, and easier, for this part of recovery.

2. Restoring the Proficy Historian Configuration file

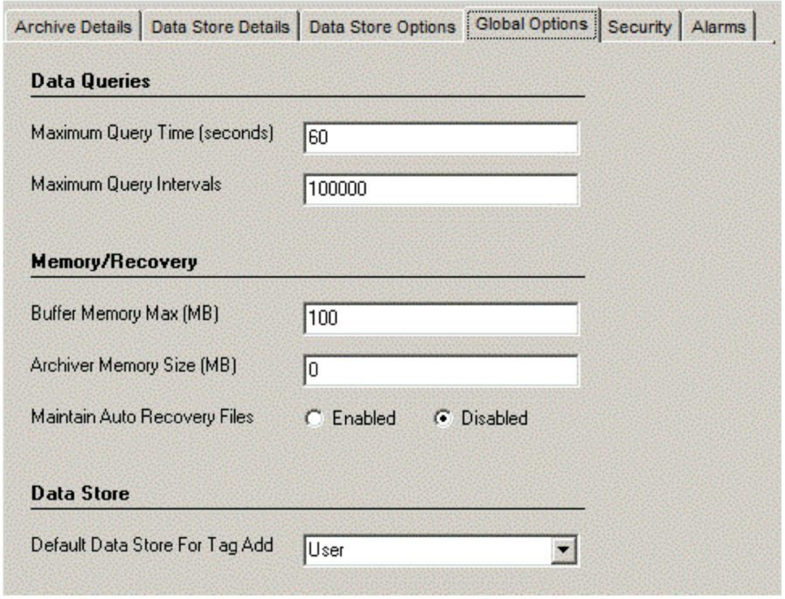
   The Proficy Historian Configuration file is the .ihc file. It is backed up any time the current archive file is backed up. It can also be backed up hourly as part of the Auto Recovery files.

3. Restoring the Proficy Historian Archives

   The Proficy Historian Archives should be backed up periodically to meet the organizations historical ICS data record keeping requirements and enable restoration in case of cyber or another incident.

Proficy Historian Server Administrators should periodically test the backup and recovery process to verify it meets the recovery requirements set by management. It is a good security practice to store a periodic backup offsite in a secure location. This prevents a physical incident, such as a fire, from destroying the Proficy Historian Server and the backup that would restore the server.

The Proficy Historian Server has a “Maintain Auto Recovery Files” option set in the Global Options tab of the Historian Administrator, see Figure 6. If enabled, the Proficy Historian Server will save a copy of the latest archive file (.iha) and latest Proficy Historian Configuration file (.ihc) every hour. This will increase the likelihood of recovery after incident, but it will also impact performance.



Data Queries

Maximum Query Time (seconds): 60

Maximum Query Intervals: 100000

Memory/Recovery

Buffer Memory Max (MB): 100

Archiver Memory Size (MB): 0

Maintain Auto Recovery Files: ○ Enabled ● Disabled

Data Store

Default Data Store For Tag Add: User

Figure 6 – Maintain Auto Recovery Files

4.8. Electronic Signature

Historian includes an Electronic Signature and Electronic Records security feature. This option provides installations concerned with the FDA's 21 CFR Part 11 regulation or any site interested in added security or tracking the ability to require a signature and password every time a change in data or configuration is requested. Please refer Historian documentation for more information.

4.9. User Account and Authentication (Proficy Authentication)

The Historian environment provides a set of REST APIs, web components to query data from the Server. Historian uses the User Account and Authentication (Proficy Authentication) service as a trusted source of tokens issued for authentication. The Proficy Authentication is a multi-tenant identity management service, used in Cloud Foundry, but also available as a standalone OAuth2 server. Its primary role is as an OAuth2 provider, issuing tokens for client applications to use when they act on behalf of Cloud Foundry users. It can also authenticate users with Cloud Foundry credentials and can act as an SSO service using those credentials, or others. It contains endpoints for managing user accounts, registering OAuth2 clients, and other management functions.

Here is how simple workflow process:

Historian incorporates the use of User Account and Authentication (Proficy Authentication) tokens into the security model, which includes:

- Retrieving the token from the Proficy Authentication service.
- Passing the JSON Web Token (JWT) to the REST service.
- Connecting the REST service with Historian Data Archiver, which connects to Windows Active Directory to authenticate the correct user.
- Passing authorization and authentication back to the REST service based on any Historian Security Groups defined (Read/Write/Admin), which allows appropriate access to the user.

5 Maintaining and Monitoring the Proficy Historian

5.1. Auditing the Proficy Historian Server

The Windows OS, Microsoft SQL Server and Proficy Historian Server application has a large number of security settings. GE has developed a security auditing capability that using the Coverity, Burp, White source scan and a GE provided audit file.

If the owner/operator has a security policy that makes settings more secure or different in any way than what is in the audit file it will record this as a non-compliance. The audit file can be edited by the owner/operator to adjust approved security settings that differ from the recommended configuration.

A security audit of the Proficy Historian Server should be done at installation to verify it has been deployed securely. The security audit then can be performed again periodically or when the security posture was likely to have changed.

5.2. Security Patching

Software has bugs and some of these bugs can lead to vulnerabilities. This is true of Microsoft OS, GE's Proficy Applications and other software providers. Organizations that deploy the GE Proficy Historian Servers should add all of the software on that server to their security patching program. As in any ICS application, appropriate testing and a phased roll out of security patches are recommended for any servers that could affect operations.

The GE Intelligent Platforms Support website (login required), www.digitalsupport.ge.com, is the best place for security patches related to the Proficy Historian Server. The GE Intelligent Platforms Product Security Advisories support page will identify any discovered vulnerabilities and the security patch or other remediation recommendations to address the vulnerability. An Auto-Notification Service is available on the support site to notify customers when new security advisories are issued.

GE analyzes the applicability and tests the compatibility of Microsoft security patches and places the results on the Important Microsoft Update Page on the support site. A preliminary analysis is performed and released within two business days for all patches Microsoft classifies as Critical. A more detailed analysis of all Microsoft security patches classified as Critical or Important will be released within seven business days. An analysis of security patches classified as Moderate will be provided based on the applicability in GE's judgment.

There is no single answer to how frequently an ICS server should be patched, and ICS owner/operators should consider different security patching intervals based on the exposure of the Proficy Historian Server to potential attackers and the impact to the organization if the Proficy Historian Server is unavailable to do a patching related outage. For example:

- A Proficy Historian Server on the Corporate Network is exposed in the same manner as other servers and should follow the Corporate Network patching interval and process.
- A Proficy Historian Server in an ICS DMZ is accessed by one or more systems on the Corporate Network. It is more exposed to attackers than a Proficy Historian Server in the ICS Trusted Zone. In addition, an outage in a Proficy Historian Server in an ICS DMZ should not affect operations. Therefore, it often has a shorter security patching interval than systems in the ICS Trusted Zone, and often is patched on the same schedule as systems on the Corporate Network.
- A Proficy Historian Server in an ICS Trusted Zone that is not relied on for operations, and communicates with a Proficy Historian Server on the ICS DMZ, may warrant more frequent security patching than other systems on the ICS Trusted Zone.
- A Proficy Historian Server in an ICS Trusted Zone that is relied on for operations should have a similar security patching interval as other servers and workstations required for monitoring and control of an ICS.

Security Zone	Security Patching Interval
Corporate Zone	Monthly / Same As Other Corporate Servers
ICS DMZ (not used by Operations)	Monthly

ICS Trusted Zone	Quarterly

Figure 7 – Sample Proficy Security Patching Interval

While the security patching interval may vary based on where the Proficy Historian Server is deployed and its use in monitoring and controlling the ICS, every Proficy Historian Server, and all software on the Proficy Historian Server, should be part of the security patching program.

6 Remote management of the Proficy Historian

6.1. Remote Collector Management (RCM) Agent

Proficy Historian Server now capable of remotely managing of its connected collectors using Collector-Manager Agent. This agent software needs to install on all machines where collectors are running that are to be managed.

With Historian REST API, Historian Server; using RCM-Agent, users can perform:

1. Starting of the collector
2. Stopping of the collector
3. Restart of the collector
4. Enabling debug mode of the collector
5. Clear/Move of collector buffer files
6. Current status of the collector
7. Pause/resume of data collection
8. Version of the collector operations centrally

This functionality applicable to the collectors running in command-mode or service-control-mode.

Performing RCM operations, user should be member of one of the groups **iH Security Admins, iH Collector Admins, iH Tag Admins** group.

Agent software and Historian Server communicate each other without any additional port/firewall rules.

7 Horizontal Scalability

The goal of Horizontal Scalability (mirroring and distributed) has been to have any user of the system, APIs, or tools be unaware that the historian is mirrored or distributed. Historian should be a system that has data stores, tags, collectors, alarms, etc. The user interacts with the system to store and retrieve data, but they are unaware that the system is mirrored or distributed. Further, this means any application written against the APIs will work with mirror or distributed and no special coding is needed.

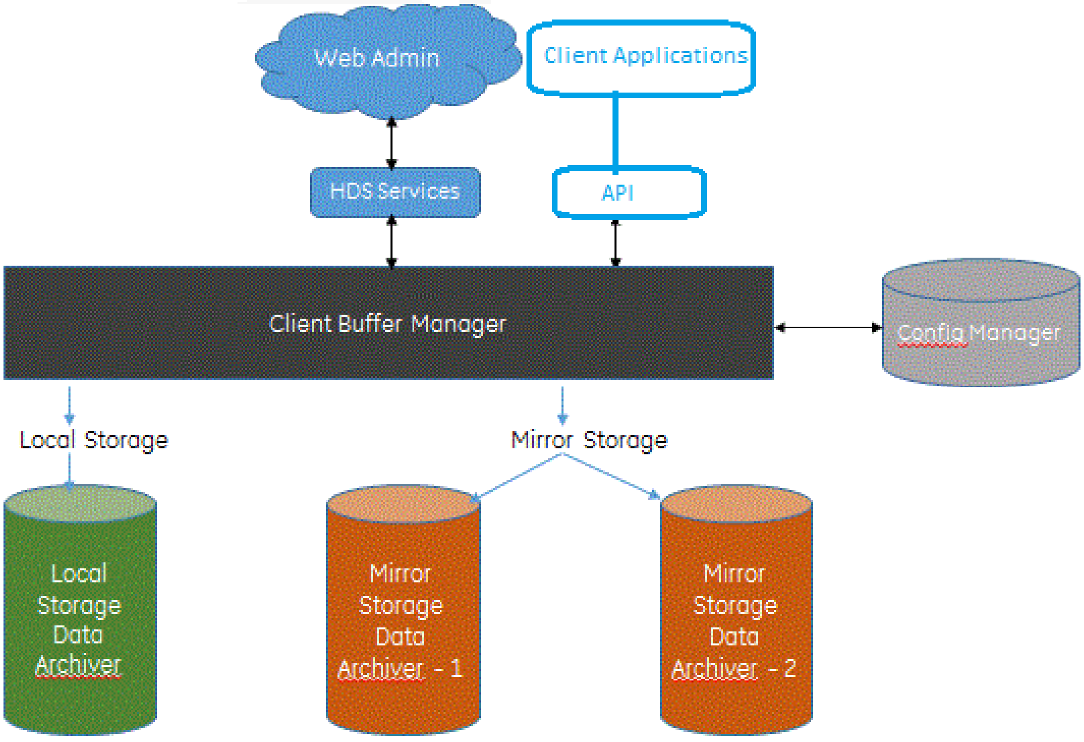
User doesn't need to know underlying Historian System has multiple Historian servers and those can be attached/removed. Historian System Administrators can horizontally increase the nodes for better performance, space without changing the client code.

In Historian we have Data Stores. A Data Store is a grouping of tags. So, when you create a tag you assign it to a Data Store. When you write data to the tag it is stored in the archives of this Data Store. Since we want Historian to be the same in mirror, distributed or neither, this concept does not change.

What was added during mirroring is the concept of storage. The administrator will define storage space in the Historian system, and then Data Stores are assigned to these storages. There are two types of storage, Distributed and Mirrored. When you define a Mirrored storage, you specify 1 to N historian nodes that are part of the Mirror.

Analogy:

In Windows, different Basic/Dynamic/RAID types of disks. We have a computer (case, CPU, memory, graphics card). That would be a basic Historian system of ConfigManager and ClientManager. No storage yet. Now we add a hard drive. We create one partition, that is storage on the computer. We format it and it is drive C:. For Historian, the disk is like adding a node to the Historian system. We added some storage ability to Historian. And since we just had one simple partition here, it is Local storage on that new node. We can put our Data Stores on this storage. So, we have a Historian with one node, local storage, all Data Stores go there. That's a very basic Historian system. Now say we need more space. In our computer analogy you would add a new hard drive and partition it as D:. In Historian, if we need more space, we add a new node, it gets Local storage, now you can put new Data Stores on either this new storage or any other defined storages. In our computer analogy, if you wanted some redundancy you might add two drives to the system, then when partitioning the disk you tell windows to create a MIRRORED partition on disk3 and disk4 and call it E:. Historian is really the same, you add a couple nodes and create a Mirrored storage that is on the two nodes. Now you put any Data Store you want on this storage and it becomes mirrored. Of course, in a computer you could mix both simple hard drives and Mirrored/RAID hard drives in one system. Historian also will support this. You might create local storage on each node, then mirrored storage between some set of nodes. Now simply put the DataStores where you want. Choose Local storage on various nodes to distribute the data and choose mirrored storage to mirror. Hopefully the analogy clears this up and doesn't confuse it more.



Horizontal Scalable System Environment