



Proficiency Historian 2023

Getting Started Guide



Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2023, General Electric Company. All rights reserved.

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

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

Contents

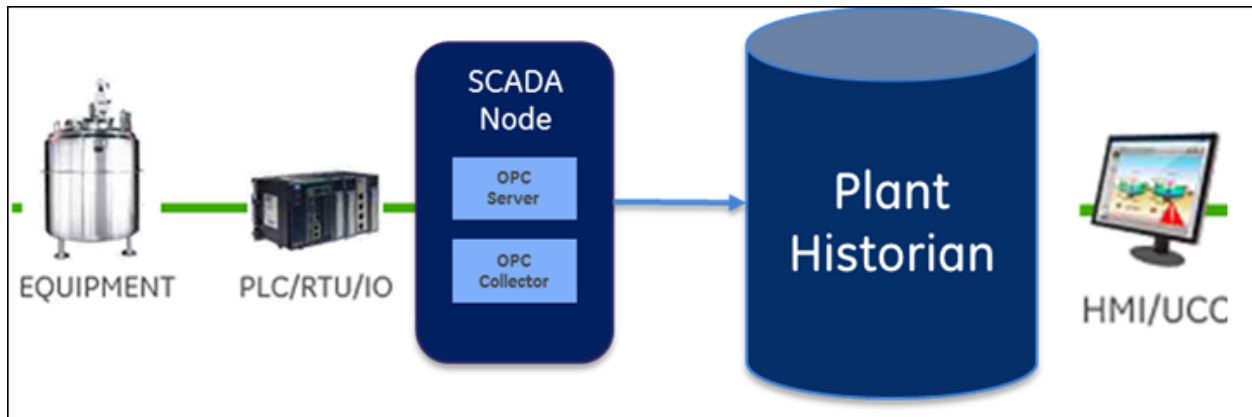
- Chapter 1. Getting Started Guide..... 4**
- Overview..... 4
- System Architecture.....8
- System Components..... 12
- About the Historian Server..... 19
- About Tags..... 20
- Prerequisites..... 21
- Setting Up the Historian Environment.....21
- Activate the Historian License.....21
- Hardware Requirements..... 26
- Software Requirements..... 31
- Compatibility with Other GE Products.....33
- Supported Formats..... 35
- Optimize Performance.....36
- Enable Trust.....38
- VMWare Support..... 38
- Installation..... 41
- Installation Workflow..... 41
- The Historian Server..... 44
- Alarms and Events..... 90
- Collectors..... 92
- Client Tools..... 100
- Web-based Clients..... 104
- Remote Management Agents..... 138
- Install the OPC UA HDA Server..... 141
- The Excel Add-In for Historian..... 146
- The Excel Add-In for Operations Hub..... 149

ETL.....	153
Stand-Alone Help.....	156
Using External Proficy Authentication or LDAP Groups.....	157
About Proficy Authentication.....	157
About Proficy Authentication Groups.....	158
Using Server Certificates.....	159
Map Remote Proficy Authentication Groups With Historian Proficy Authentication.....	159
Map LDAP Groups with Historian Proficy Authentication.....	161
Map LDAPS (LDAP via SSL) Groups with Historian Proficy Authentication.....	164
Remove Mapping Between Historian Proficy Authentication Groups and LDAP Groups.....	168
Remove Mapping Between Proficy Authentication Groups of Historian and an Existing Proficy Authentication Instance.....	170
Change the Log Levels of Proficy Authentication.....	171
Migrating Historian Data.....	172
Migrating the Alarms and Events Data.....	172
Using the Migration Tool.....	176
Data Migration Scenarios.....	179
Migration Tool Command-Line Syntax.....	183
Interoperability of Historian Versions.....	184
Migrate User Authentication Data from Historian to Common Proficy Authentication Service.....	185
Implementing Historian Security.....	188
Implementing Historian Security.....	188
Uninstalling Historian.....	229
Uninstalling Historian.....	229
Troubleshooting.....	230
Managing Historian Log Files.....	230
Troubleshooting the Historian Server.....	233
Troubleshooting Web-based Clients.....	235

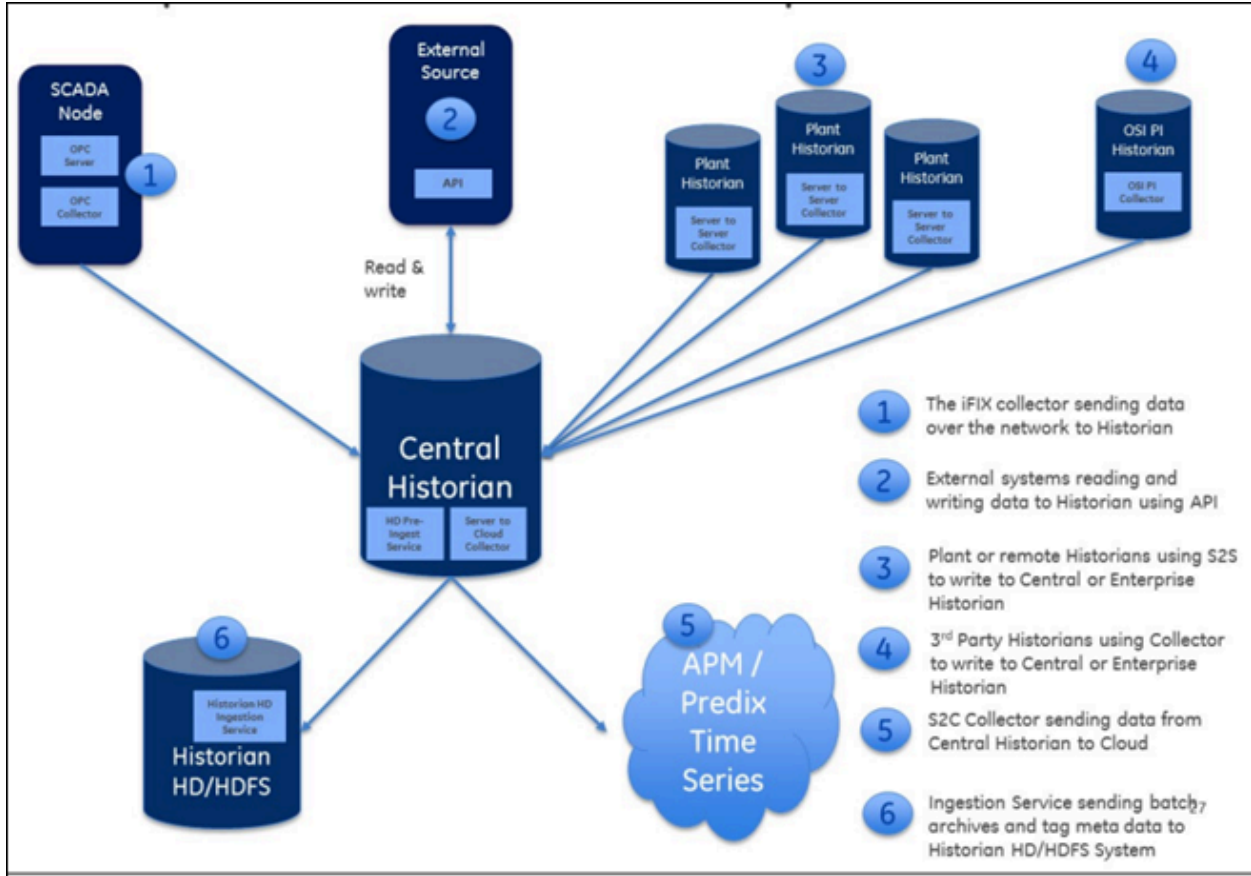
Chapter 1. Getting Started Guide

Overview of Historian

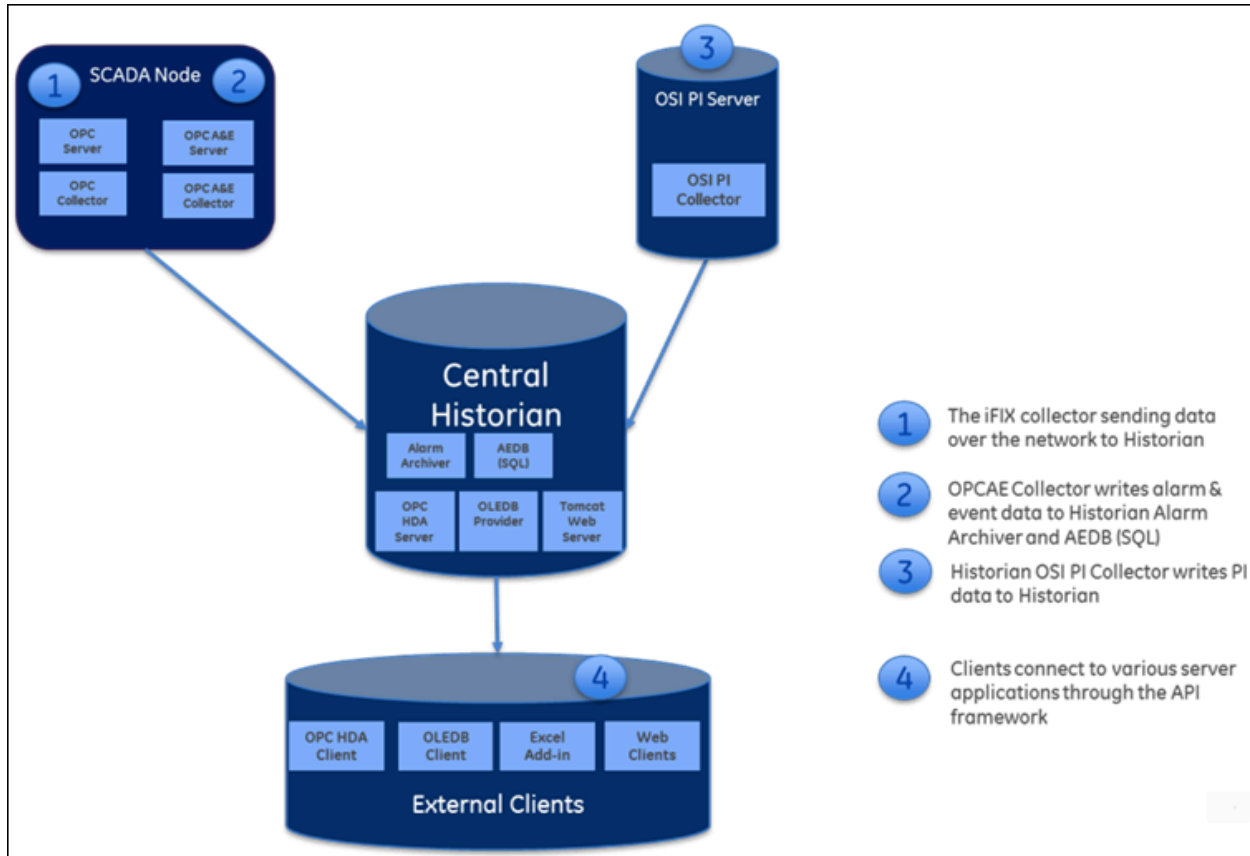
Proficy Historian is a high-performance data archiving system designed to collect, store, and retrieve time-based information at an extremely high speed. The following diagram shows an HMI or an OPC server from which data is collected and stored in Historian.



You can collect data from multiple SCADA systems and various applications, and store them in a central Proficy Historian server.



You can then use various clients to fetch and analyze this data.



Historian contains the following main components:

- **Data collectors:** Collect and analyze the tag data.
- **The Historian server:** Stores tag data.
- **Clients:** Retrieve tag data from the Historian server using APIs.

For information on how these components work in a Historian system, refer to [System Architecture \(on page 8\)](#).

Data Collectors

Collectors are applications that collect data from a wide variety of applications such as iFIX, CIMPLICITY, OPC servers, OSI PI, and text files (.csv or .xml). This data is then stored in the Historian server.

In addition, Historian contains the Calculation and the Server-to-Server collectors. The Calculation collector performs calculations and analyses on Historian data and stores the results in tags on the server. The Server-to-Server collector has the same calculation capabilities as the Calculation collector, but it stores the results in tags on a remote server.

Most collectors can perform first-order deadband compression, a browse-and-add configuration, and store and forward buffering.

**Note:**

Standard collectors that are included as part of the product will not consume a client-access license (CAL). Other interfaces developed by customers or system integrators using the Collector Toolkit or APIs will consume a CAL for each instance or connection.

Bi-Modal Collectors:

The Historian data collectors can send data to an on-premises Historian server as well as cloud destinations such as Google Cloud, Azure IoT Hub, AWS Cloud, and Predix Cloud. Therefore, these collectors are called bi-modal collectors. The following collectors, however, are not bi-modal collectors; they can send data only to an on-premises Historian server:

- The Calculation collector
- The File collector
- The HAB collector
- The iFIX Alarms and Events collector
- The OPC Classic Alarms and Events collector
- The OSI PI Distributor
- The Python collector
- The Server-to-Server distributor

The Historian Server

The Historian server is the central point for managing all of the client and collector interfaces, storing data and (optionally) compressing and retrieving data.

In the Historian server, data is stored in files called data archives. These files contain all the tag data gathered during a specific period of time (for example, time-based archives such as daily archives). They have the .iha extension.

You can store data of various data types such as Float, Integer, String, Byte, Boolean, Scaled, and binary large object data type (BLOB). The source of the data defines the ability of Historian to collect specific data types. If you have the license to store the alarms and events data, the server also manages the storage and retrieval of OPC Alarms and Events in a SQL Server Express.

You can further segregate your tags and archives into data stores. A data store is a logical collection of tags used to store, organize, and manage tags according to the data source and storage requirements. A data store can have multiple data archives, and includes logical and physical storage definitions.

The primary use of data stores is segregating tags by data collection intervals. For example, you can put name plate or static tags where the value rarely changes in one data store, and put process tags in another data store. This can improve the query performance.

The Historian Data Archiver is a service that indexes all the data by tag name and timestamp and stores the result in an .iha file. The tag name is a unique identifier for a tag (which is a specific measurement attribute). For iFIX users, a Historian tag name normally represents a Node.Tag.Field (NTF). Searching by the tag name and time range is a common and convenient way to retrieve data from Historian. If you use this technique to retrieve data from the archive files, you need not know which archive file contains the data. You can also retrieve data using a filter tag.

Clients

Clients are applications that retrieve data from the archive files using the Historian API.

The Historian API is a client/server programming interface that maintains connectivity to the Historian Server and provides functions for data storage and retrieval in a distributed network environment.

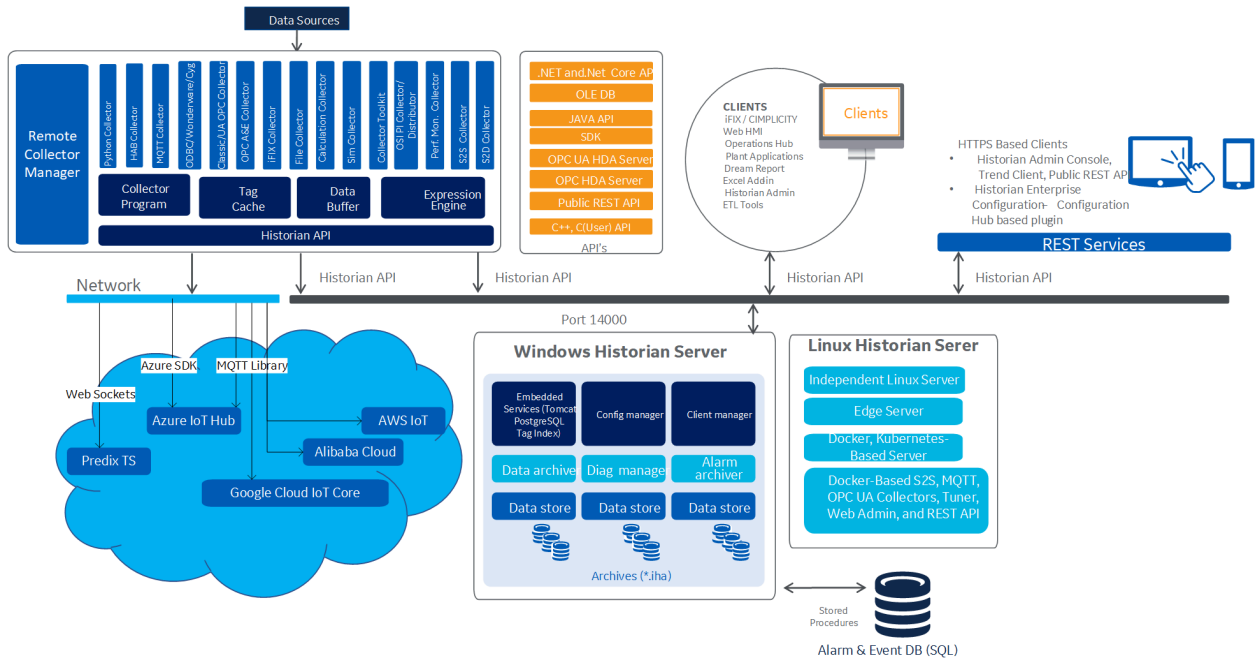
System Architecture

Standard or Stand-Alone Historian Architecture:

In this type of system, there is a single Historian server. It offers the following unique capabilities and benefits for a sustainable competitive advantage:

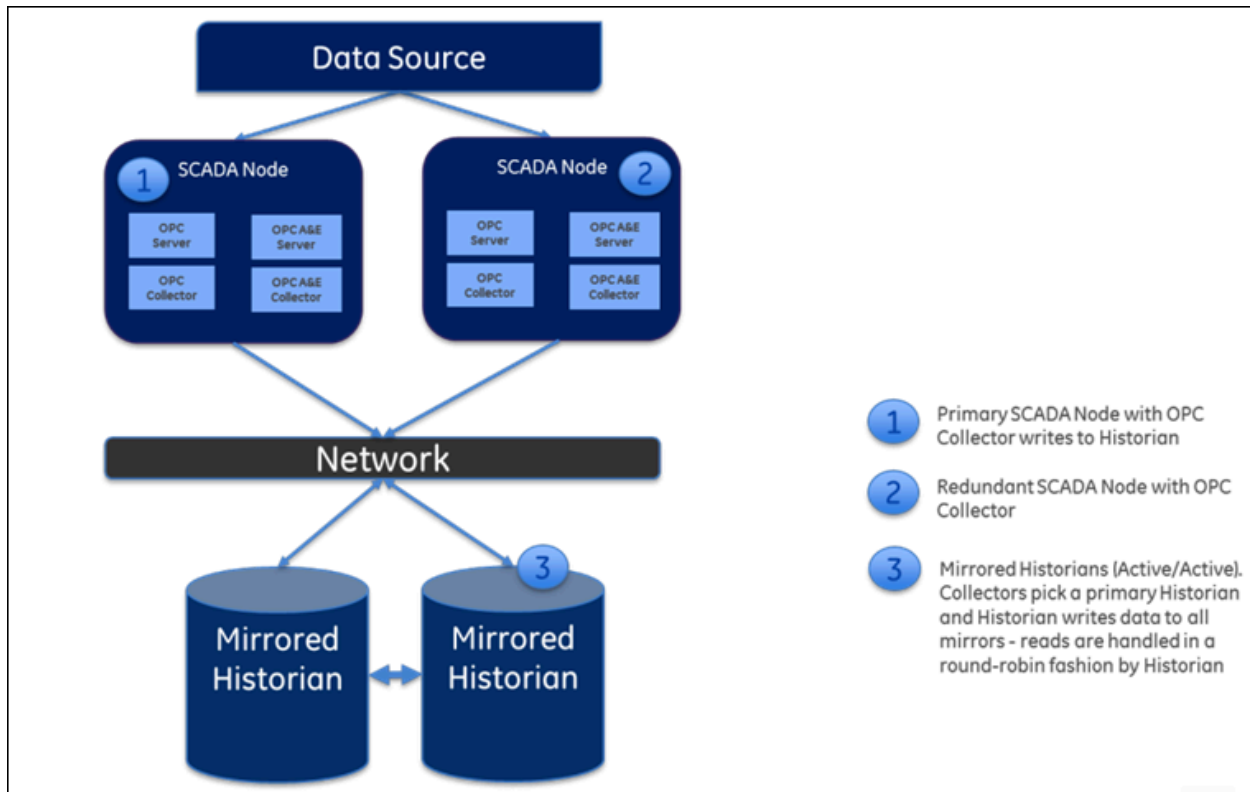
- Built-in data collection
- Good read/write performance speed
- Enhanced data security

The following image shows the architecture of a stand-alone Historian system (single server):



Horizontally Scalable Historian system:

In addition to the capabilities of a stand-alone Historian system, a horizontally scalable one offers data redundancy and high availability. You can have mirroring of stored data on multiple nodes to provide high levels of data reliability. Data mirroring also involves the simultaneous action of every insert, update, and delete operations that occur on any node. You can spread the data collection, server, administration, and client data retrieval functions across various nodes.



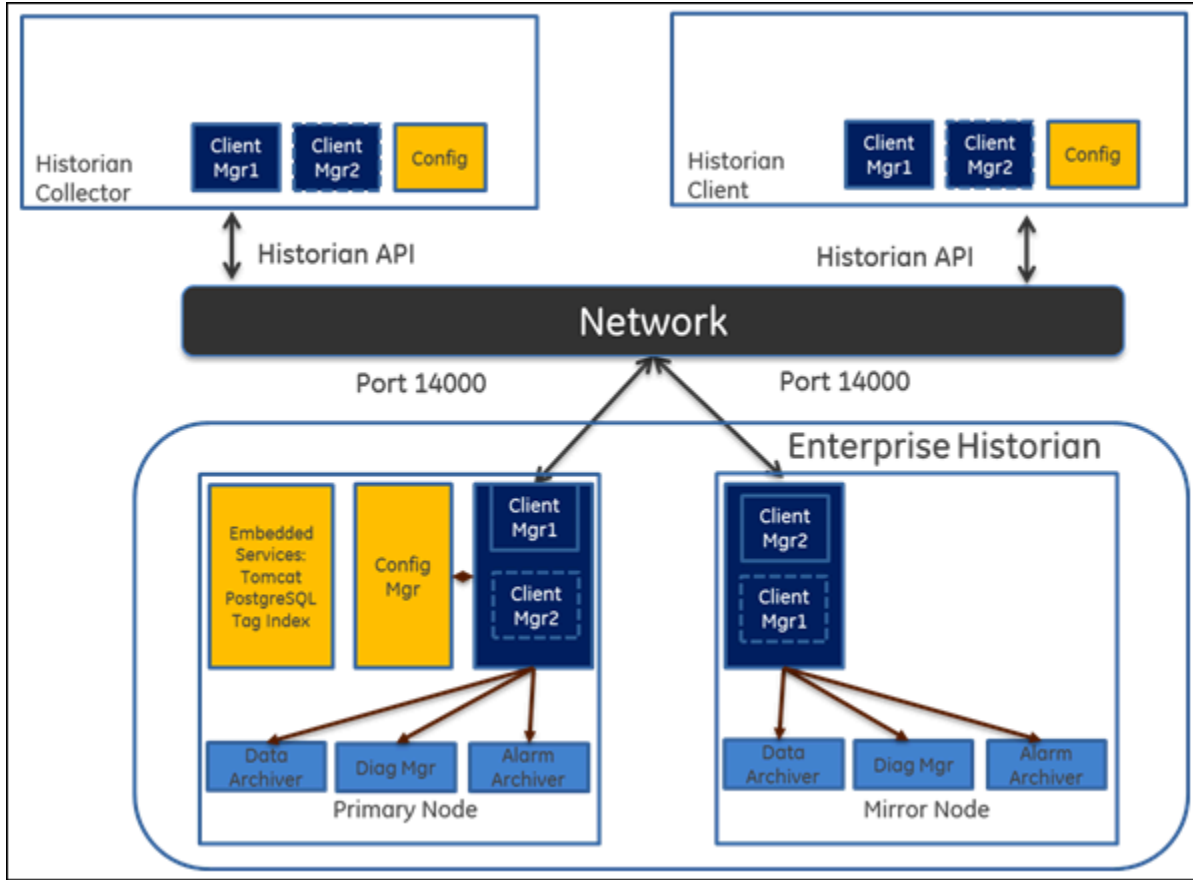
In a typical data mirroring scenario, one server acts as a primary server to which the clients connect. To create a mirror, you must add mirror nodes and establish a data mirroring session relationship between the server instances. All communication goes through Client Manager, and each Client Manager knows about the others.

When a client (either a writing collector or reading client) connects to the Client Manager, it gathers information about each Client Manager, along with all archive, tag, and collector configuration information, from the Configuration Manager, and stores this information locally in its Windows Registry.

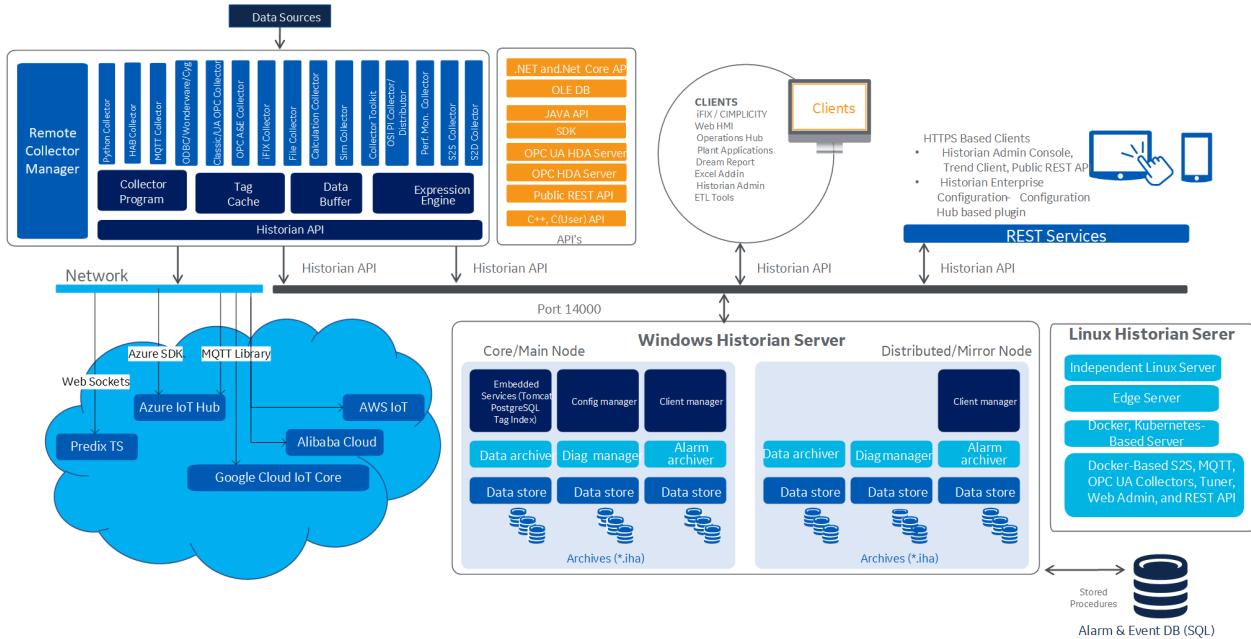
A relationship is then established between each remote client and a single Client Manager, which directs read and write requests across the other mirrors. If that relationship is broken, it will establish a new relationship with the next available Client Manager, which assumes the same responsibilities. This bond is maintained until that Client Manager is unavailable, and then the process of establishing a relationship with another Client Manager is repeated.

When more than one node is running, the Client Manager uses a "round robin" method between the good nodes to balance read loads. Each read request is handled by a node as a complete request.

Writes are sent independently but nearly simultaneously to any available data archiver so that the same tag shares a common GUID, name, timestamp, value, and quality as passed to it by the collector.



The following diagram shows the architecture of a horizontally scalable Historian system.



System Components

A typical Historian system contains components for the following functions:

- Data collection/migration
- Data storage
- Data management, analysis, and monitoring
- Data retrieval

All these components communicate with the Historian server through the Historian API. This topic describes the functions performed by each component.

Data Collection/Migration Components

Data collection/migration components are used to collect data from various sources and ingest the data into a Historian server (or to cloud). The following data collection/migration tools are used in Historian:

Data Collectors

Data collectors gather data from a data source based on a schedule or an event, process it, and forward it to the Historian server or a web socket for archiving. The following collector functions are common across all types of collectors (except the File collector):

- Automatically discovering available tags from a data source and presenting them to Historian Administrator and Configuration Hub.
- Providing options to send data to an on-premises Historian server or to cloud through a web socket connection
- Performing a first-level of data compression (collector compression).
- Responding to control requests, such as requests to pause or resume data collection.
- Maintaining a local cache of tag information to sustain collection while the server connection is down.
- Buffering data during loss of connection to the server and forwarding it to the server when the connection is restored.
- Optionally, automatically adjusting timestamps for synchronizing collector and archiver timestamps.
- Supporting the timestamp of both the collector and the device, as applicable.
- Scheduling data polling for a polled collection.

For mission-critical data collection, you can set up redundant collectors. Historian includes a mirroring option for high availability and load balancing, so the data is available all the time.

The File Collector

A File collector imports .csv and .xml files into the Historian server. These files can contain data, alarms, tag names, or other configuration information, and messages that you can import with a File collector.

The Extract, Transform, and Load Tools

Transferring data from one Historian server to another is typically performed by the data collectors. These tools provide a connected streaming data transfer mechanism (except the calculation and file transfer collectors). In a system where a steady network connection is not possible or not cost-effective, a periodic file-oriented data transfer is preferred. The Historian ETL tools consist of a comprehensive set of file-oriented data extraction, transfer, and loading tools.

Migration Tools

Migration tools are used to migrate existing Historian configuration and data and iFIX Alarms and Events collector data to the Historian server. Tags, collection rates, and deadbands for tags configured in Historian can be transferred by the migration tools.

The Collector Toolkit

Collector Toolkit is used to develop a customized collector. You can use Collector Toolkit to write programs that integrate with Historian and leverage the same configuration tools, redundancy schemes, and health monitoring as the collectors. It collects data and messages from a data source and writes them to a data archiver. Each deployment of a collector developed on the Collector Toolkit consumes a client access license (CAL).

Data Storage, Analysis, and Maintenance Components

Data collected by the collection/migration components is stored in the Historian server (or cloud). You can then analyze and maintain the data using the following components:

Historian Alarms and Events

Historian Alarms and Events provides tools to collect, archive, and retrieve alarms and events data in Historian.

Historian Administrator *(on page 10)*

Historian Administrator provides a graphical user interface for performing Historian maintenance functions in a Windows environment including:

- Tag addition, deletion, and configuration.
- Maintaining and backing up archive files.

- Data collector configuration.
- Security configuration.
- Searching and analyzing system alerts and messages.
- Configuring the Calculation collector to create a new tag based on calculations, and storing the result as time series data.
- Setting up your OPC Classic HDA server and OPC UA HDA server.

Historian Administrator

The Web Admin console provides a dashboard, which displays the health of the system in one convenient location. You can view the following diagnostics details:

- **Data node diagnostics:** Displays the Historian servers connected to the system.
- **Collector diagnostics:** Displays the details of the faulty collectors.
- **Client diagnostics:** Displays the top five busiest clients connected to the system.

The dashboard provides interactive configuration management, which helps you configure mirror nodes, tags, collectors, data stores, and archives. However, the functionality of the Calculation collector and the ability to configure OPC HDA servers are not included in the Web Admin console.

The Web Admin console uses a CAL.

The Historian Server

The Historian server performs the following tasks:

- Manages all system configuration information.
- Manages system security, audit trails, and messaging.
- Services write and read requests from distributed clients.
- Performs final data compression.
- Manages archive files.

Historian Diagnostics Manager

The Historian Diagnostics Manager monitors the health of the Historian system and executes a few rules on the nodes, collectors, and clients, and generates the appropriate fault record. The details of these faults are displayed in the Web Admin console.

The following are the faults and their severity level:

Fault Type	Fault Description	Fault Level
Collector Status Fault	Generated when the collector goes to the Unknown or Stopped state.	Error
Collector Overrun Fault	Generated when at least one overrun occurs on a collector in last 24 hours.	Warning
Collector OutOfOrder Fault	Generated when at least one OutOfOrder occurs on a collector in last 24 hours.	Information
Collector StoreForward Fault	Generated when the collector Last Data Sample Time Stamp is delayed by more than an hour.	Information
Collector ConnectDisconnect Fault	Generated when the collector is Disconnected and connected at least once in last 24 hours.	Information
Service DiskSpace Fault	Generated when a node disk space is about to reach its free space limit.	Warning
Client InActive Fault	Generated when a client is not active for the last one hour.	Information
Client BusyRead Fault	Generated when the client makes relatively more number of reads per minute.	Information
Client BusyWrite Fault	Generated when the client makes relatively more number of writes per minute.	Information
Client TimedOutRead Fault	Generated when the client makes a timed out read query.	Warning

Client Manager

Client Manager acts as the client connection manager and message router for the system. It examines messages and forwards them to the correct data archiver or to Configuration Manager. This service is deployed only for mirrored systems.

Configuration Manager

Configuration Manager maintains and distributes the entire system configuration. There can be multiple Historian nodes but only one Configuration Manager. This Configuration Manager node is used to store system configuration, such as tag names, collector names, and Historian node names. This service is deployed only for mirrored systems.

Configuration Hub

Configuration Hub allows you to manage the Historian systems and its components, including:

- Creating a Historian system, and adding its components
- Creating mirror groups
- Creating and managing data stores
- Installing and managing collector instances

Using Configuration Hub, you can achieve high availability of servers in a Historian system.

Remote Collector Manager

Typically, collectors are distributed geographically, and so, accessing them can be challenging and not cost-effective. To overcome this challenge, the Remote Collector Management agent provides the ability to manage collectors remotely.

Historian Tomcat Container

An instance of Tomcat is used exclusively by Historian as an open source Java-based web server to support the Web Admin console and Trend Client. It supports SSL and the use of certificates for enhanced security.

Proficy Authentication Tomcat Container

An instance of Tomcat is used exclusively as an open source Java-based web server to support external Proficy Authentication.

Historian PostgreSQL Database

An instance of PostgreSQL is used exclusively to store tag names to improve searching for tags in the Trend tool and Web Admin console.

Proficy Authentication PostgreSQL Database

An instance of PostgreSQL is used exclusively to store Proficy Authentication details.

Reverse Proxy Service

Provides secure connection by supporting https protocol.

Indexing Service

The indexing service speeds up search results. It periodically queries the database, creates a tag index, and stores the information in the PostgreSQL database instance.

Excel Add-in for Historian

Excel Add-in is a very useful tool for presenting and analyzing data stored in archive files. Using this tool, you can design custom reports of selected data, automatically process the information, and analyze the results. You can also use it for performing tag maintenance functions in Historian, such as adding tags, importing or exporting tags, or editing tag parameters.

Excel Add-in for Operations Hub

The Excel Add-in for Operations Hub enables you to query historical data of objects and object types defined in Operations Hub.

Customers purchasing Historian Standard or Enterprise licenses now receive a no-cost license for the Operations Hub server and the Historian Analysis run-time application. The Operations Hub server enables customers to define an asset model including tag mapping. The Historian Analysis application is a pre-built Operations Hub HTML5 application that enables users to do advanced trend analyses, including the ability to make annotations.

The OPC Classic HDA Server

The OPC Classic HDA server reads the raw data stored in Historian and sends it to the connected OPC clients. The Historian OPC Classic HDA server complies with OPC Server HDA 1.20 standards.

Historian SDK

The Historian Software Development Kit (SDK) is designed for writing Visual Basic (VB) or Visual Basic for Applications (VBA) scripts. Using the SDK, you can develop your own scripts to perform selected repetitive or complex tasks or to make your own custom user interface. To use the SDK, create a VB/VBA project with the SDK as a project reference.

Data Retrieval Components

Data retrieval components are used to retrieve data that is stored in the Historian server. Historian contains the following data retrieval components:

Historian Alarms and Events

Historian Alarms and Events provides tools to collect, archive, and retrieve alarms and events data in Historian.

Client Manager

Client Manager acts as the client connection manager and message router for the system. The Client Manager will examine messages and forward them to the correct Data Archiver or to the Configuration Manager. This service is deployed only for mirrored systems.

Configuration Manager

Configuration Manager maintains and distributes the entire System configuration. There can be multiple Historian nodes but only one Configuration Manager. This Configuration Manager node is used to store system configuration, such as tag names, collector names and Historian Node names. This service is deployed only for mirrored systems.

Proficy Authentication Tomcat Container

An instance of Tomcat is used exclusively by Historian as an open source Java-based Web server to support an external Proficy Authentication.

Historian PostgreSQL Database

An instance of PostgreSQL is used exclusively by Historian to store tag names to improve searching for tags in the Trend tool and Web Admin console.

The OPC Classic HDA Server

The Historian OPC Classic HDA server reads the raw data stored in Historian and sends it to the connected OPC Classic HDA collectors. The Historian OPC Classic HDA server is in compliance with OPC Server HDA 1.20 standards.

The OPC UA HDA Server

The Historian OPC UA HDA server retrieves historical process data from Proficy Historian, and sends it to OPC UA HDA clients. It dynamically updates the clients when tags are added and/or deleted in Historian. Clients that comply with this specification can connect to the OPC UA HDA server to retrieve data from Historian.

For information, refer to the OPC UA HDA Server section of the online documentation.

User API

The Historian User API is intended to provide high speed read/write access to Historian data and read access to Historian tags. There is no access to alarms, events, or messages.

Since the Historian User API is the basic building block for connectivity, all Historian functions, including data collection, administration, and data retrieval, use the Historian API. You can use the Historian User API to connect to a local Historian server or a remote one (by just providing the IP address or host name of the server).

Use the API to develop applications in C or C++, which read and write data to the Historian server when the Historian SDK and Historian OLE DB do not meet your project requirements for performance or programming language.

Historian allows you to develop both 32-bit and 64-bit User API programs.

**Note:**

If you want to build a 32-bit User API program on a 64-bit operating system, then you need to rename the `ihuapi32.lib` to `ihuapi.lib` and include it in your program.

REST APIs

Historian includes a REST API to connect your Java Web-based Clients with Historian data.

Historian SDK

The Software Development Kit (SDK) is designed for writing Visual Basic (VB) or Visual Basic for Applications (VBA) Scripts. Using the SDK, you can develop your own scripts to perform selected repetitive or complex tasks or to make your own custom user interface. To use the SDK, create a VB/VBA project with the SDK as a project reference. Refer to the *SDK Help* system for more information.

Historian Client Access API

The Historian Client Access API is a .NET Core assembly that interacts with Historian from any .NET Core applications. Since it works with .NET Core, it is platform-independent - you can use it on any operating system, such as Windows, Linux, and Mac OS.

**Note:**

You can still use the old Client Access API, which is a .NET assembly. It is installed when you install Client Tools.

JAVA APIs

Most open source, quick development applications rely on JAVA as their programming language. To enable easier integration with Historian, JAVA APIs are provided. The JAVA APIs support 64-bit Windows Operating Systems.

About the Historian Server

The Historian server is the central point for managing all of the client and collector interfaces, storing data and (optionally) compressing and retrieving data.

In the Historian server, data is stored in files called data archives. These files contain all the tag data gathered during a specific period of time (for example, time-based archives such as daily archives). They have the .iha extension.

You can store data of various data types such as Float, Integer, String, Byte, Boolean, Scaled, and binary large object data type (BLOB). The source of the data defines the ability of Historian to collect specific data types. If you have the license to store the alarms and events data, the server also manages the storage and retrieval of OPC Alarms and Events in a SQL Server Express.

You can further segregate your tags and archives into data stores. A data store is a logical collection of tags used to store, organize, and manage tags according to the data source and storage requirements. A data store can have multiple data archives, and includes logical and physical storage definitions.

The primary use of data stores is segregating tags by data collection intervals. For example, you can put name plate or static tags where the value rarely changes in one data store, and put process tags in another data store. This can improve the query performance.

The Historian Data Archiver is a service that indexes all the data by tag name and timestamp and stores the result in an .iha file. The tag name is a unique identifier for a tag (which is a specific measurement attribute). For iFIX users, a Historian tag name normally represents a Node.Tag.Field (NTF). Searching by the tag name and time range is a common and convenient way to retrieve data from Historian. If you use this technique to retrieve data from the archive files, you need not know which archive file contains the data. You can also retrieve data using a filter tag.

The Historian server performs the following tasks:

- Manages all system configuration information.
- Manages system security, audit trails, and messaging.
- Services write and read requests from distributed clients.
- Performs final data compression.
- Manages archive files.

About Tags

A Historian tag is used to store data related to a property.

For example, if you want to store the pressure, temperature, and other operating conditions of a boiler, a tag will be created for each one in Historian.

When you collect data using a collector, tags are created automatically in Historian to store these values. These tags are mapped with the corresponding properties in the source.

For example, suppose you want to store OSI PI data in Historian. You will specify the OSI PI tags for which you want to collect data. The OSI PI collector creates the corresponding tags in Historian, and it stores the values in those tags.

You can also choose to create tags manually (for example, to store the result of a calculation performed by the Calculation collector).

Prerequisites

Setting Up the Historian Environment

Identify the computers that will function as your clients, data collectors, administration workstations, and archiver.

1. Set up each computer.
See [Hardware Requirements \(on page 26\)](#), and refer to the user manual that accompanies each component for the setup information.
2. Use a login account with administrator rights so that you can install Historian later.
See [Software Requirements \(on page 31\)](#), and refer to the user manual that accompanies each software product for the setup information.
3. Activate the license key on your Historian server node. Additional licenses may be required on other nodes (such as mirroring and collector nodes) depending on your configuration requirements. See [Activate the Historian License \(on page 21\)](#).
4. Disable the guest account in Windows security if you want to limit authentication to known Windows users only.
5. Ensure that the protocols and ciphers (TLS 1.0, 1.1, and 1.2) required to install Historian are available.

Activate the Historian License

Advantage Licensing is the software system for activating and managing product licenses. Using the tools in licensing and our Customer Center website, you can view, activate, and manage licenses at your site.

Using Advantage Licensing, you can:

- View current licenses for the products residing on a computer.
- Choose a licensing method (Internet, local intranet, or file-based).
- Change licenses (Activate, Return, Refresh).

Historian is available in three license types:

- Essentials
- Standard
- Enterprise

The Essentials edition is included as the on-board Historian with the purchase of some iFIX and CIMPLICITY licenses, and cannot be licensed or sold outside of those packages. Essentials edition customers who require options available in the Standard or Enterprise editions or require more than a 1000 tags must purchase either a Standard or Enterprise License with the appropriate tag count.

Historian HD is sold and licensed separately from Historian. Historian HD provides the Historian user a standard method to move Historian tag configuration and historical archive data from a Windows environment to a Hadoop Distributed File System (HDFS). HDFS is the primary distribution storage used by Hadoop applications.

A component that is used only by the Historian HD license is installed with your Historian installation: the Historian Archive Ingestion service. This service is reserved for use only with the Historian HD big data analytics platform and is listed as Manual under Startup Type. Stopping this service does not impact the Historian functionality. Unless you are licensed to use Historian HD, do not attempt to start or monitor this service, as it may impact the ability to run the Historian Data Archiver service. For more information regarding Historian HD, refer to <https://www.ge-ip.com/products/proficy-historian-hd/p3714>.

The following table provides information on the availability of each Historian component for each license type. Optional indicates that the component is not available by default, but can be purchased separately.



Note:

For a Calculation collector and a Server-to-Server collector, you can either opt for stand-alone use of bi-modal collectors or add Enterprise collectors to the Standard Historian license. Using these options, you can quickly and easily send data from one Historian server to another or directly to Predix Timeseries. For information on the pricing, contact the Support team.

Component	Essentials	Standard	Enterprise	Distributed
Server Functionality				
Data modification	Yes	Yes	Yes	Yes
Client Access Licenses (CALs)	2	2500	2500	2500
Cluster support	No	Yes	Yes	Yes

Component	Essentials	Standard	Enterprise	Distributed
Collector redundancy	Optional	Yes	Yes	Yes
Horizontal scalability (data mirroring)	No	No	Yes	Yes
Data stores	5	10	20	20
Data stores expansion (200)	No	No	Optional	Optional
Digital / Enumerated / Array Tags	Yes	Yes	Yes	Yes
Distributed Historian	No	No	No	Yes
Electronic signatures	No	Optional	Optional	Optional
The Extract, Transform, and Load (ETL) tools	No	No	Yes	Yes
Fault-tolerant computer support	Yes	Yes	Yes	Yes
Maximum historical tags	1,000	50,000	20,000,000	20,000,000
Microsecond support	No	Yes	Yes	Yes
The OLE DB provider	Yes	Yes	Yes	Yes
The OPC Alarms and Events server	No	Optional	Yes	Yes
The OPC Classic HDA server	Yes	Yes	Yes	Yes
The OPC UA HDA server	No	Yes	Yes	Yes
The Historian server	Yes	Yes	Yes	Yes
Remote Collector Management	No	No	Yes	Yes
SCADA buffer (10000 tags, 200 days)	Yes	Yes	Yes	Yes
User-Defined multi-field tags	No	Yes	Yes	Yes
Client Functionality				
The Historian Model	No	Yes	Yes	Yes
The Historian Excel add-in	Yes	Yes	Yes	Yes
Historian Administrator	Yes	Yes	Yes	Yes
Operations Hub Freemium	No	Yes	Yes	Yes
The Web Admin console	No	Yes	Yes	Yes

Component	Essentials	Standard	Enterprise	Distributed
Trend Client	No	Yes	Yes	Yes
Configuration Hub	Yes	Yes	Yes	Yes
Collector Functionality				
Aveva (Wonderware) Collector with the cloud option	No	Yes	Yes	Yes
The Calculation collector	No	Available as a part of the Enterprise Collectors option	Yes	Yes
Collector Toolkit SDK	No	Yes	Yes	Yes
The CygNet collector with the cloud option	No	Yes	Yes	Yes
Expressions	No	No	Yes	Yes
The File collector	No	Yes	Yes	Yes
The HAB collector	No	Yes	Yes	Yes
The iFIX collector	Yes	Yes	Yes	Yes
The MQTT collector	No	Yes	Yes	Yes
The ODBC collector with the cloud option	No	Yes	Yes	Yes
The OPC Classic Alarms and Events collector	No	Optional	Yes	Yes
The OPC DA collector with the cloud option	Yes	Yes	Yes	Yes
The OPC Classic HDA collector with the cloud option	No	Yes	Yes	Yes
The OPC UA Data Access (DA) collector with the cloud option	No	Yes	Yes	Yes
The OSI PI collector with the cloud option	No	Yes	Yes	Yes
The OSI PI distributor	No	Yes	Yes	Yes

Component	Essentials	Standard	Enterprise	Distributed
The Python collector	No	Available as a part of the Enterprise Collectors option	Yes	Yes
The Server-to-Server collector with the cloud option	No	Available as a part of the Enterprise Collectors option	Yes	Yes
The Simulation collector	Yes	Yes	Yes	Yes
The Windows Performance collector	No	Yes	Yes	Yes

**Note:**

* Starting Historian 7.2, SCADA buffer count is increased from 2500 to 10000. Historian Essentials license includes 2500 buffered tags and a 200-day circular buffer if permanent storage is less than 1000 tags (that is, if CIMPLICITY points are 1500 and below). It includes 10000 buffered tags and a 200-day circular buffer if permanent storage is 1000 tags (that is, if CIMPLICITY points are 5000 and above).

To activate the Historian license:

1. If the license is already activated on your system, access License Client, select **Advanced > Clear license information on this computer**.
2. If you received an email containing an activation code, you must migrate to Advantage Licensing. Get the latest licensing software at <http://digitalsupport.ge.com>.

If you did not receive an activation code, follow the instructions about M4 keys at <http://digitalsupport.ge.com>.

3. For all Windows operating systems, ensure that they are updated with the most recent Windows updates:

- If you are using Windows Server 2012 R2, you must install the update described in <http://support.microsoft.com/kb/2919355>.

Follow the instructions in KB2919442 and then KB2919355 before proceeding to KB2999226. This update must be installed before you install the License Client.

4. Download the Historian software.

https://www.youtube.com/embed/x_FLVpg5kyU

5. Install the licensing software.

<https://www.youtube.com/embed/38fdDtZjZJs>

6. Activate the Historian license.

<https://www.youtube.com/embed/HSieM78vFcU>

Hardware Requirements

Table 1. Historian Server

Hardware Component	Standard Historian	Enterprise Historian, Data Mirroring
RAM	8 GB	16 GB or 32 GB (recommended)
Disk size	80 GB free hard-drive space	250 GB (minimum)
Processor type	Intel Core i3 or i5 or i7 CPU or an equivalent AMD Phenom CPU	Intel Core-i5, i7 family, or equivalent
CPU		Dual/Quad cores
CPU speed	2.4 GHz	2.8 GHz
Recommended CPU clock	2.4 GHz	2.8 GHz
Storage type		SAS SSD with RAID Level 0 configured
Operating system		<ul style="list-style-type: none"> • Microsoft® Windows® Server 2019 (64-bit) • Microsoft® Windows® Server 2016 (64-bit)

Table 1. Historian Server (continued)

Hardware Component	Standard Historian	Enterprise Historian, Data Mirroring
		<ul style="list-style-type: none"> • Microsoft® Windows® Server 2012 R2 (64-bit) • Microsoft® Windows® 10 IoT (32-bit or 64-bit) • Microsoft® Windows® 10 (32-bit or 64-bit) • Microsoft® Windows® 8.1 Professional (32-bit or 64-bit)
Tags		Up to 50,000
Years of data online		1 year
Other requirements	<ul style="list-style-type: none"> • A DVD-ROM drive. • 100 Mbps TCP/IP-compatible network interface adapter for network communication and certain I/O drivers. 	

The size of a Historian server is determined by:

- The number of tags from which data is collected. The number of tags is an indicator of the number of concurrent users likely to access the system. The primary factor is server memory requirements; CPU load is a secondary factor. If the number of concurrent users is significantly different from the suggested guidelines, adjust server memory size accordingly.
- The rate of alarms and events collection.
- The frequency of data collection.
- The amount of data you want to keep online.

The following table provides the recommended hardware components for a Historian server with the Standard license based on the number of tags that you want to use. These recommendations may vary based on years of data online, update rate, data compression setting, and other tag configuration parameters.

Hardware Component	Less Than 10,000 Tags	10,000 to 50,000 Tags	100,000 to One Million Tags	One Million to Two Million Tags	Two Million to Five Million Tags
RAM (in GB)	8 GB/16 GB (recommended for a single node setup)	16 or 32	16 or 32	16 or 32	32 or 64
Disk Size (in GB)	100 or 250	250	250	500	500
Processor Type	Intel Core-i5, i7 family, or equivalent	Intel Core-i5, i7 family, or equivalent	Intel Xeon (56xx, E5 family or AMD Opteron 42xx/62xx family)		
CPU	Dual/Quad core	Dual/Quad core	Dual/Quad core	2-socket	2-socket or 4-socket
CPU Speed (in GHz)	2.8	2.8	2.8	2.6	2.6
CPU clock speed (in GHz)	2.8	2.8	2.8	2.6	2.6
Storage Type	SAS SSD with RAID level 0 configured	SAS SSD with RAID level 0 configured	Direct-attached or shared storage with SAS enterprise class drives. Hardware RAID controller with cache memory. SAN recommended over NAS		High speed shared storage with SAS or SSD drive types. Hardware RAID controller with cache memory. SAN recommended over NAS.
Years of data online	1	1	1	1	1

**Note:**

- The Historian server runs only on 64-bit versions of Windows.
- When possible, for performance reasons, consider using computers with multiple disk drives so that archives and buffers can be given their own drive. Or, multiple data stores can each have their own drive.
- Sustained event rate is 60-100 million samples per minute.
- Historian supports Intel Core i3, i5, i7 Duo based processors as long as they are compatible with the operating system.
- Historian does not support Titanium processors.

System performance may vary depending on the hardware specifications, operating system, and tuning parameters. The following table provides sample hardware specifications for medium-sized and large-sized servers.

Hardware Component	For a Medium-Sized Server	For a Large-Sized Server
Processor type	Intel Xeon 5540	Intel Xeon E5-2670 or E5-4650
CPU	Dual socket	Dual socket or quad-socket
CPU speed (in GHz)	2.5	2.7
RAM (in GB)	64	256

Table 2. Collectors

Hardware Component	Recommendation
RAM	8 GB
Disk size	80 GB
Historian collectors	32-bit or 64-bit

Note:

GE Data Collector for Wonderware support 64-bit only

**Note:**

- Historian Collectors work as 32-bit applications on a 64-bit Windows operating systems using WoW64 mode (Windows-on-Windows 64-bit). However, you can read and write data from a 64-bit Historian Server.
- RAM and Disk Size required may vary based on the collectors available on the system.
- Recommended number of tags per collector is 20 to 30K.
- For iFIX systems, count each Node.Tag.Field (NTF) as a separate tag when you determine the size of the system. For example, FIX.FIC101.F_CV and FIX.FIC101.B_CUALM (current alarm) both count as tags, even though they are derived from the same iFIX tag.

Microsoft Windows Server

Many desktop-class computers are not certified to run Windows. Check the Microsoft website and your computer hardware vendor website for possible conflicts between your hardware and Windows server. These specifications are sufficient to meet the needs of a small pilot application. However, production system requirements may be significantly different depending on many application-specific factors. Please contact your product manager to review the requirements of your application.


Table 3. Microsoft Cluster Service

Hardware Component	Requirement
CPU speed, processor type, and RAM	A 2.6 GHz clock-speed Intel Core i3 or i5 or i7 or Xeon or equivalent AMD Opteron CPU with minimum 8 GB RAM.
Disk size	A 80 GB free hard-drive space and a 40 GB shared SCSI hard-drive (RAID preferred).
Other requirements	Two 100Mbit TCP/IP-compatible network interface adapters for network communication and certain I/O drivers (One for public network, another for private network).

**Note:**

The configuration of each server added to the cluster must be identical to the other servers in the cluster.

Table 4. Data Mirroring and Redundancy Service

Hardware Component	Requirement
Operating system	A 64-bit Windows operation system.
RAM	Minimum 8 GB RAM. <div data-bbox="480 506 1419 686" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;">  Note: If you are using single node setup, it is recommended to use 32 GB RAM. </div>
Processor type	A dual core processor.

Ensure that you are using the same hardware requirement for the mirror node as well.

Network Speed

For a large Configuration Hub setup, it is recommended that the network speed is 1 GBPS.



Note:

- If you are using a single node setup, then it is recommended to use 32 GB RAM.
- Ensure that you are using the same hardware requirement for the mirror node as well.
- You must have a minimum of 10 GB free space available for the data archiver to start.
- Many desktop-class computers are not certified to run Windows server. Check the Microsoft website and your computer hardware vendor website for possible conflicts between your hardware and Windows server. These specifications are sufficient to meet the needs of a small pilot application. However, production system requirements may be significantly different depending on many application-specific factors. Please contact your product manager to review the requirements of your application.

Software Requirements

This topic describes the minimum software requirements for Historian.

• **Operating System:** Historian requires one of the following operating systems, with latest service packs or revisions:

- Microsoft® Windows® Server 2022 (64-bit)
- Microsoft® Windows® Server 2019 (64-bit)
- Microsoft® Windows® Server 2016 (64-bit)
- Microsoft® Windows® 11 (64-bit)
- Microsoft® Windows® 10 (64-bit), Professional ,or Enterprise Edition.
- Microsoft® Windows® 10 IoT Enterprise with LTSC enabled.



Note:

The Historian server runs on a 64-bit Windows operating system only.

Historian 7.2 32-bit components such as Collectors, Excel Add-in 32-bit, Interactive SQL 32-bit, APIs, and Non-Web Administrator work as 32-bit application on 64-bit Windows operating systems using WoW64 mode (Windows-on-Windows 64-bit). However, you can read and write data from a 64-bit Historian Server.

If you use Historian 6.0 or later on Windows Server 2008 R2, you must go for a Full Installation and not Core Installation of Windows.

• **Network Interface Software:** The TCP/IP network protocol is required.

• **Microsoft®.NET Core or .NET Framework:** Historian requires the following .NET frameworks: To install the framework, you must configure your proxy server for internet access.

- **Microsoft®.NET Core Framework 3.1:** This is required if you want to use the new Client Access API.
- **Microsoft®.NET Framework 4.8:** This is required on the machine on which you will install the Excel Add-in for Operations Hub. In addition, this is required for Historian collectors.
- **Microsoft®.NET Framework 4.5.1:** This is required for all the other Historian components. You can install it manually, or you will be prompted to download and install it while installing Historian.



Note:

If your machine is Firewall/proxy-enabled, Microsoft .NET Framework may not be installed automatically. In that case, before installing Historian, you must install Microsoft .NET Framework manually (if it is not available).

- **Microsoft® SQL Server®:** Historian requires one of the following 32-bit or 64-bit Microsoft® SQL Server® SQL server systems to configure archiving for alarms and events or to use Historian as a linked server:
 - Microsoft® SQL Server® 2019
 - Microsoft® SQL Server® 2017

**Note:**

The collation for your alarms and events database must match the collation of your SQL Server. This happens automatically by default unless the alarms and events database is moved to another SQL server.

- **Browser:** You can access the Web Admin console and Trend Client using the following browsers:
 - Firefox version 46 or later
 - Google Chrome version 39 or laterTo access Configuration Hub, use Google Chrome only.
- **Screen Resolution:** You can access Configuration Hub, the Web Admin console, and Trend Client using the following screen resolutions:
 - 1280 x 1024
 - 1366 x 768
- **Microsoft Excel:** The Excel Addin for Historian or the Excel Addin for Operations Hub requires any of the following versions of Excel:
 - Microsoft® Excel® 2021 (32 & 64 bit)
 - Microsoft® Excel® 2019 (32 & 64 bit)
 - Microsoft® Excel® 2016 (32 & 64 bit)
 - Microsoft® Excel® 2013 (32 & 64 bit)
- **Web Server:** The web server requires the following applications:
 - Microsoft®.NET Framework 4.5.2
 - Historian Client Tools 7.0 or later
 - OLE DB, User API, and Historian Client Access Assembly

Compatibility with Other GE Products

Several GE products work with Historian. The following is a general set of required versions to work with Historian.

**Important:**

If you want to enable the Strict Authentication feature in Historian 7.2, be aware that you will need to apply the latest SIMs that support this feature for all Proficy clients that connect to the Archiver, including the ones listed in this table. In addition, there may be SIMS to allow pre-5.0 collectors and client applications such as Excel Add-In to connect. Refer to the SIM download page for update for Historian and other Proficy products.

Product	Supported Version
CIMPLICITY	11.1, 2022
iFIX	6.5, 2022, 2023 pre-release
Plant Applications	8.2, 2022, 2023 pre-release
Workflow	2.6, 2.6 SP1
Operations Hub	2.1, 2022, 2023 pre-release
Configuration Hub	2023
Proficy Authentication	2023
Dream Reports	2020 for Proficy

* For customers using iFIX, there was a change in the HKEY_CURRENT_USER registry values for WebSpace and it will no longer work with the existing SIM. Ensure that you get the latest iFIX SIMs. The following article provides additional instructions: https://ge-ip.force.com/communities/en_US/Article/iFIX-WebSpace-Strict-Historian-Authentication

** For Plant Apps customers using the `Historian Type = 'GE Proficy - Historian 3.0'` to connect to Historian 7.2, both the Enabled and Disabled options for Enforce Strict Client Authentication selection are supported.

** For Plant Apps customers using the 'Historian Type = 'GE Proficy – Historian' to connect to Proficy Historian 7.2, only the Disabled option for Enforce Strict Client Authentication selection is supported.

In Historian 5.0, the Historian HKEY_CURRENT_USER registry key values were changed. The programs accessing the server collection through the SDK are unaffected. Any program or script that directly accesses the registry keys or any Terminal Server login scripts that try to configure a list of servers by importing registry keys directly will no longer work. Such programs need to access the server collection via SDK calls, not directly.

Historian REST APIs are required to integrate between Historian and Operations Hub. Historian REST APIs are installed automatically when you [install Historian Web-based Clients \(on page 109\)](#).

Supported Regional Settings, Data Types, and Date/Time Formats

Supported Regional Settings

Historian supports the following regional settings available in Control Panel:

- Decimal symbol - one character
- Digit grouping symbol
- List separator - one character
- Time style
- Time separator
- Short date style
- Date separator

Supported Data Types

Data Type	Size
Single Float	4 bytes
Double Float	8 bytes
Single Integer	2 bytes
Double Integer	4 bytes
Quad Integer	8 bytes
Unsigned Quad Integer	8 bytes
Unsigned Single Integer	2 bytes

Data Type	Size
Unsigned Double Integer	4 bytes
Byte	1 byte
Boolean	1 byte
Fixed String	Configured by user.
Variable String	No fixed size.
Binary Object	No fixed size. Historian does not support the use of the Binary Object data type with the Data Collectors. Refer to the SDK online Help for more information on working with BLOB data types.
Scaled	2 bytes

Supported Date Formats

Historian supports the following short date formats, some of which may not be available in certain language versions of Windows:

- dd/mm/yy
- dd/yy/mm
- mm/dd/yy
- mm/yy/dd
- yy/dd/mm
- yy/mm/dd

Avoid changing the time style or short date style in regional settings to values that are outside of the standard styles provided.

Optimize Performance

You can optimize performance in the following ways:

- **Optimize virtual memory:** Through the use of paging files, Windows allocates space on your hard drive for use as if it were actually memory. This space is known as virtual memory. This topic describes how to optimize the virtual memory on the Historian archiver computer.

**Note:**

If the paging file is set to grow dynamically, your system may experience severe performance problems during runtime. To ensure optimal performance, the Initial Size and Maximum Size values for the paging file must be the same so that the paging file does not grow dynamically. For more information on creation and sizing of Windows paging files, refer to Microsoft Windows Help.

- **Optimize the server performance:** If the file sharing and printer sharing options on the computer on which you want to install Historian is set to maximize data throughput, it can lead to excessive paging when dealing with large files, which can interfere with applications like Historian. You can change these settings to optimize the performance.

1. To optimize virtual memory:
 - a. Access Control Panel, and then select **System > Advanced system settings > Advanced**.
 - b. Under **Performance**, select **Settings > Advanced**.
 - c. Under **Virtual Memory**, select **Change**.
 - d. In the **Initial size** and **Maximum size** fields, enter a value equal to three times your physical memory.
 - e. Select **Set**, and then select **OK**.
2. To optimize server performance:
 - a. Access Control Panel.
 - b. Select **Network and Sharing Center**.
 - c. Select the network that you use.
The **<network name> Status** window appears.
 - d. Select **File and Printer Sharing for Microsoft Networks**, and select **Properties**.
 - e. Select **Properties**.
 - f. Ensure that the **Maximize Data Throughput for Network Applications** option is selected.
 - g. Select **OK**.

Enable Trust for Proficy Historian for a Self-signed Certificate

During Historian installation, a self-signed certificate is generated that you use with Historian web applications. A self-signed certificate is a certificate that is signed by itself rather than signed by a trusted authority. Therefore, a warning appears in the browser when connecting to a server that uses a self-signed certificate until it is permanently stored in your certificate store. This topic describes how to ensure that Google Chrome trusts the self-signed certificate.

1. Using Google Chrome, access the site to which you want to connect.
A message appears to inform you that the certificate is not trusted by the computer or browser.
2. Select **Not Secure** in the URL, and then select **Certificate**.
The **Certificate** window appears.
3. Select **Certification Path**, select the root certificate, and then select **View Certificate**.
The **Certificate** window appears, displaying the **General**, **Details**, and **Certification Path** sections.
4. Select **Details**, and then select **Copy to File**.
5. Follow the on-screen instructions to save the certificate to a local file. Use the default format: **DER encoded binary X.509 (.CER)**.
6. Right-click the .CER file that you have exported, and select **Install Certificate**.
The **Certificate Import Wizard** window appears.
7. Select **Trusted Root Certificate Authorities**, and then select **OK**.



Note:

Do not let the wizard select the store for you.

A **Security Warning** window may appear. If it does, ignore the message by selecting **Yes**. The certificate is installed.

8. Restart the browser, and connect to the server.
9. Open the URL authenticated by the certificate.
If error messages do not appear, the certificate is successfully imported.

VMWare Support

Historian provides support for VMware ESXi server version 5.0 and later. The virtualization capability provided by VMware lets you run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical computer. Please be aware that while we have tested VMware ESXi 5.0 and above, issues with the VMware software or the virtualized environment are outside the scope of GE Digital's responsibility. You must use VMware Compatibility Hardware and Software

before installing Historian 7.0 or greater Data Archiver on a Virtual Machine. For the current release, the only supported type of Proficy licensing for use with VMware is keyless (software) licensing.

**Note:**

VMware Player is not supported.

**Important:**

Advanced features of the ESXi server (such as VMotion, High Availability, and Clustering support) have not been tested with Historian.

For information regarding VMware compatibility and its supported software and hardware environments, refer to <http://www.vmware.com/resources/guides.html>.

VMWare Best Practices and Limitations

Disk Growth

To prevent disk growth during run time, make sure you pre-allocate the hard disk in your VMware image.

**Important:**

If the VMware disk needs to grow at runtime because of IHA growth or creation, the Data Archiver will be slowed. If there is not enough disk space on the host machine to grow the VMware disk, the archiver may lose data.

Suspended Images/Power Metered Images

ESXi servers have power meter functions and options as well as the ability to suspend images to conserve power. We do not recommend or support these functions due to the potential effects on the Guest operating system, specifically in regards to polling I/O and timely updates.

I/O Devices and Connections and VMware

There are a multitude of devices and methods of communications on the market. These devices may be used if you can successfully connect them from the virtual machine through the physical HOST, but we do not support the setup of that connection. Be aware that device drivers used to write to proprietary cards for the ESXi HOSTS as part of virtual device setup can cause issues.

USB Controller Limitations

The USB controller has these limitations when using Historian and VMware:

- Minimum virtual hardware version 7 is required.
- Only one USB controller of each type can be added to a virtual machine.
- The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes an additional number of controllers and you connect USB devices to these controllers, the devices are not available to be passed through to a virtual machine.
- You must add a USB controller to a virtual machine before you can add a USB device.
- You must remove all USB devices from a virtual machine before you can remove the controller

USB Device Limitations

USB devices have these limitations when using Historian and VMware:

- A virtual machine may have up to 20 USB devices attached to it; however, each unique USB device can only be attached to one virtual machine at a time.
- Unsupported USB devices may not interact as expected with other ESXi features.

Additional VMware Notes

GE Digital cannot guarantee the performance of the Historian software in a virtualized environment due to the wide range of parameters associated with the hardware, configuration, memory settings, third-party software installations, and the number of virtual machines running; all of which can affect performance. Therefore, GE Digital cannot provide support related to the performance of the Historian software running on a virtual machine if it is determined that the issue is related to the virtual environment. Also, GE Digital does not provide support or troubleshoot a customer's virtual machine infrastructure.

It is the responsibility of you, the customer, to ensure that the performance of the Historian software and any third-party applications (especially those not recommended by GE Digital) are adequate to meet the needs of your run mode environment. GE Digital does not support issues related to functionality that is not available as a result of running in a virtual machine infrastructure. Examples include the functionality of card level drivers such as those for the Genius® family of drivers, the Allen-Bradley® DH/DH+ drivers, the Cyberlogic's MBX® Driver for the SA85 card, as well as functions requiring direct video access. Check with the vendor of your third-party application for support statements regarding that third-party product's ability to run in a virtualized environment.

For more detailed information regarding VMware specifications and requirements, visit the VMware web site: <http://www.vmware.com/resources/compatibility/search.php>.

Installation

Historian Installation Workflow

1. Design your system architecture.

Decide what collectors to instantiate on which nodes, which computers to designate as the Historian server and Historian Administrator, whether or not they will be web-based, and how much memory and disk space you can assign to buffers and archives. Record the computer names of each node.

2. Ensure that data sources are installed.
3. [Set up your Historian environment \(on page 21\)](#).
4. On the server node, launch the installer, select **Install Historian**, and follow the on-page instructions to [install Historian \(on page 46\)](#) on a single server or in a distributed environment.
5. [Activate your product license \(on page 21\)](#).
6. [Install the collectors \(on page 92\)](#).
7. Restart your computer if prompted to do so.
8. As needed, [install Web-based Clients \(on page 104\)](#).
9. Perform post install setup for MTLS features, by installing certificates:
 - [Install Certificates for Proficy Historian \(on page 58\)](#)
 - [Install Proficy Historian Certificates on Different Computers \(on page 66\)](#)
10. For the Windows-based Historian Administrator clients, start the Administrator from **Historian Startup Group**.

When the home page for Historian Administrator appears, you are ready to set up archives, collectors, and tags in the **Data Store Maintenance**, **Collector Maintenance**, and **Tag Maintenance** pages.

The following table provides a list of installation options available in Historian, along with purpose of installing each one.

Installation Option	When to Install
Historian Server (on page 44)	Installing the Historian server is mandatory to work with Historian. If you want to use Web-based Clients, you must provide the Proficy Authentica-

Installation Option	When to Install
	<p>tion server details while installing the Historian server.</p> <p>When you install the Historian server, the following components are installed as well:</p> <ul style="list-style-type: none"> • The RemoteCollectorConfigurator utility: A command-line tool, which allows you to manage collectors remotely. • The Proficy Authentication Configuration tool: A utility that allows you to specify the Proficy Authentication server details to match with the Proficy Authentication server used by Web-based Clients.
<p>Alarms and Events (on page 90)</p>	<p>Install Alarms and Events if you want to retrieve and store alarms and events data from any OPC-compliant alarms and events server using the OPC Classic Alarms and Events collector.</p>
<p>Collectors (on page 92)</p>	<p>Installing collectors is mandatory to collect and store data in Historian.</p> <p>When you install collectors, all the collectors and the Remote Management Agents are installed. You must then create instances of each collector and manage them using Configuration Hub.</p> <p>When you install collectors, if iFIX/CIMPLICITY are installed on the same machine, instances of the following collectors are created automatically:</p> <ul style="list-style-type: none"> • The iFIX collector • The iFIX Alarms & Events collector • The OPC Classic Data Access collector for CIMPLICITY • The OPC Classic Alarms and Events collector for CIMPLICITY

Installation Option	When to Install
Client Tools (on page 100)	<p>Install Client Tools if you want the following components:</p> <ul style="list-style-type: none"> • Client Tools • Historian Administrator • OLE DB driver and samples • The OPC Classic HDA server • User API and SDK • Historian Client Access API • Collector Toolkit
Web-based Clients (on page 104)	<p>Install Web-based Clients if you want to manage Historian administrative tasks and analyze the data using components such as Configuration Hub, the Web Admin console, Trend Client, and REST APIs.</p> <p>To use Web-based Clients, you need Proficy Authentication (UAA server) to handle user authentication. It provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.</p> <p>During the Web-based Clients installation, you can choose to install a Proficy Authentication instance and Configuration Hub, or you can use existing ones.</p>
Historian Remote Management Agents (on page 138)	<p>Remote Management Agents (RMA) include Remote Collector Manager, which is used to manage collectors remotely.</p> <p>RMA is installed automatically when you install collectors. If, however, you are using RMA version 8.1, and you want to upgrade only RMA (and not the collectors), use this option.</p>
Excel Add-in for Historian (on page 146)	<p>Install Excel Add-in for Historian make bulk changes to tag parameters using Excel, and then</p>

Installation Option	When to Install
	import it to Historian. You can also perform mathematical, retrieve selected data, generate reports and charts, and so on.
Excel Add-in for Operations Hub (on page 149)	Install Excel Add-in for Operations Hub if you want to query historical data of objects and object types defined in Operations Hub.
ETL Tools (on page 153)	Install the Historian Extract, Transform, and Load (ETL) tools if you want to transfer data where there is limited internet connectivity.
The OPC UA HDA Server (on page 141)	Install the OPC UA HDA server if you want to use Historian as an OPC UA HDA server. You can then connect any OPC UA HDA clients with the server.
Standalone Help (on page 156)	Install Standalone Help to access the Historian product documentation offline.

About Installing the Historian Server for the First Time

You can choose one of the following types of installation:

- **Single server:** This is for a stand-alone Historian system, which contains only one Historian server. This type of system is suitable for a small-scale Historian setup.
- **Mirror primary server and distributed/mirror node:** This is for a horizontally scalable Historian system, which contains multiple Historian servers, all of which are connected to one another. This type of system is used to scale out the system horizontally. For example, if you have 5,00,000 tags in your Historian system, you can distribute them among the various servers to improve performance.

In this setup, one of the nodes acts the primary server, whereas the others are the distributed/mirror servers. Configuration Manager and the embedded web services are installed only on the primary server, which are used by the distributed/mirror servers as well.

When the Archive Duration property is changed in a distributed environment, the changes will take effect after 15 minutes.

The distributed environment works only for tag data; it does not work for alarms and events data. Therefore, do not install alarm archiver in a distributed environment.

In this setup, one of the nodes acts the primary server, whereas the others are the distributed/mirror nodes.

For all these types of installation, you can use [the GUI-based installer \(on page 46\)](#) or [the Command Prompt window \(on page 52\)](#). You can also [install the Historian server in a cluster environment \(on page 70\)](#).

This section provides the high-level steps in installing the Historian server for the first time. You can perform the same steps to upgrade the server. If you are upgrading from either Historian 6.0 Enterprise or previous releases of Historian 7.2 (including any of the service packs), both Client Manager and Configuration Manager services will be removed. However, this will have no impact on your data or use of Historian unless you intend to use a distributed system.

**Note:**

The number of alarms in the Historian Alarms and Events database, and the frequency of new events being added during the installation, impact the time it takes to install Historian. For example, an installation for a system with 1.5 million alarms can take up to three hours to complete.

**Important:**

You cannot use size-based archives with a Historian Mirror Primary Server and Historian Mirror Node installation. This is because having archives of different sizes introduces archive synchronization risks in a mirrored environment. The restriction is enforced on all Historians, even those not using mirroring.

**Important:**

Be aware that you cannot close your current archive with a Historian Mirror Primary Server and Historian Mirror Node installation. This is because closing the current archive introduces archive synchronization risks in a mirrored environment. The restriction is enforced on all Historians, even those not using mirroring.

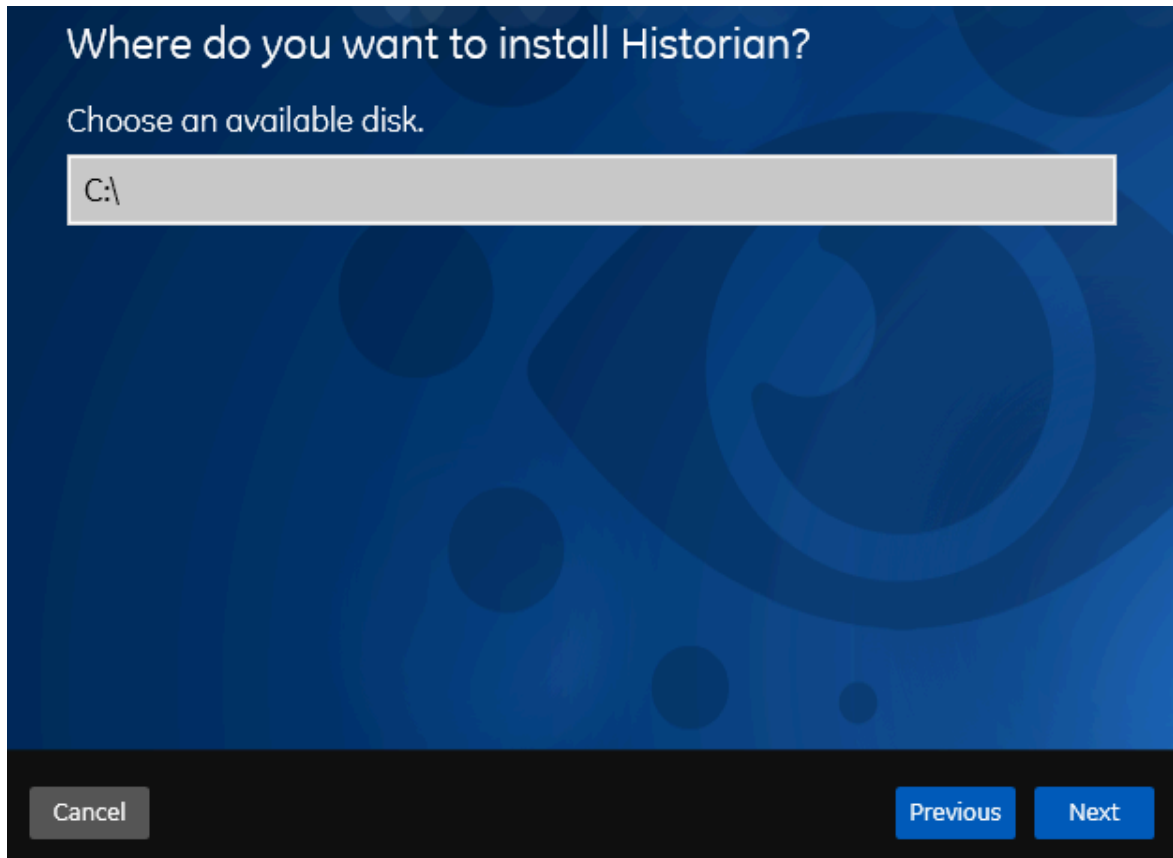
Install the Historian Server Using the Installer

- [Set up the Historian environment \(on page 21\)](#).
- If you are changing the role of a Historian server that was previously a distributed/mirror server to any other configuration (single-server or mirror primary server), you must first [Uninstalling Historian \(on page 229\)](#).
- If you are installing a distributed/mirror server, use the same configuration, license key, installation drive, Proficy Authentication instance, and domain as the primary server.

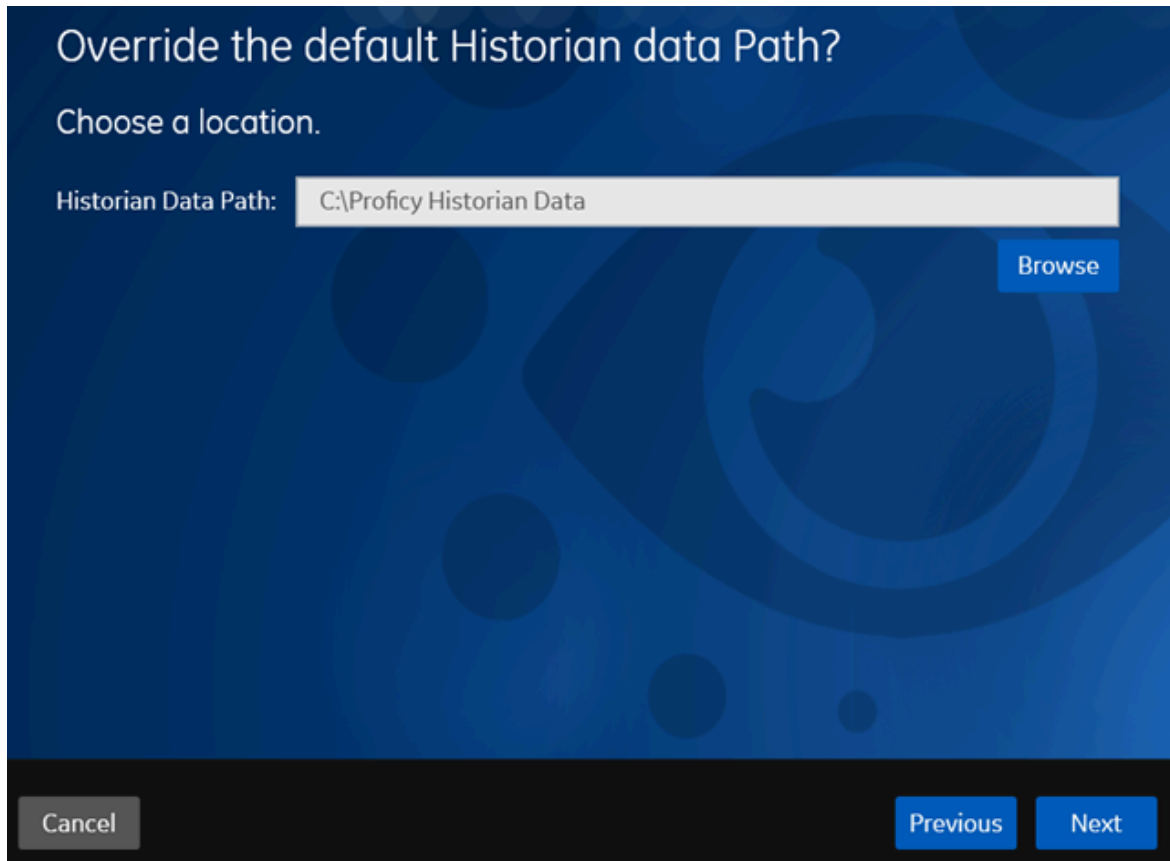
This topic describes how to install the Historian server using the installer.

You can also [install it at a command prompt \(on page 52\)](#).

1. Log in as an administrator to the machine on which you want to install the Historian server.
2. Run the `InstallLauncher.exe` file.
3. Select **Install Historian**.
The welcome page appears.
4. Select **Next**.
The license agreement appears.
5. Select the **Accept** check box, and then select **Next**.
The **Where do you want to install Historian?** page appears.



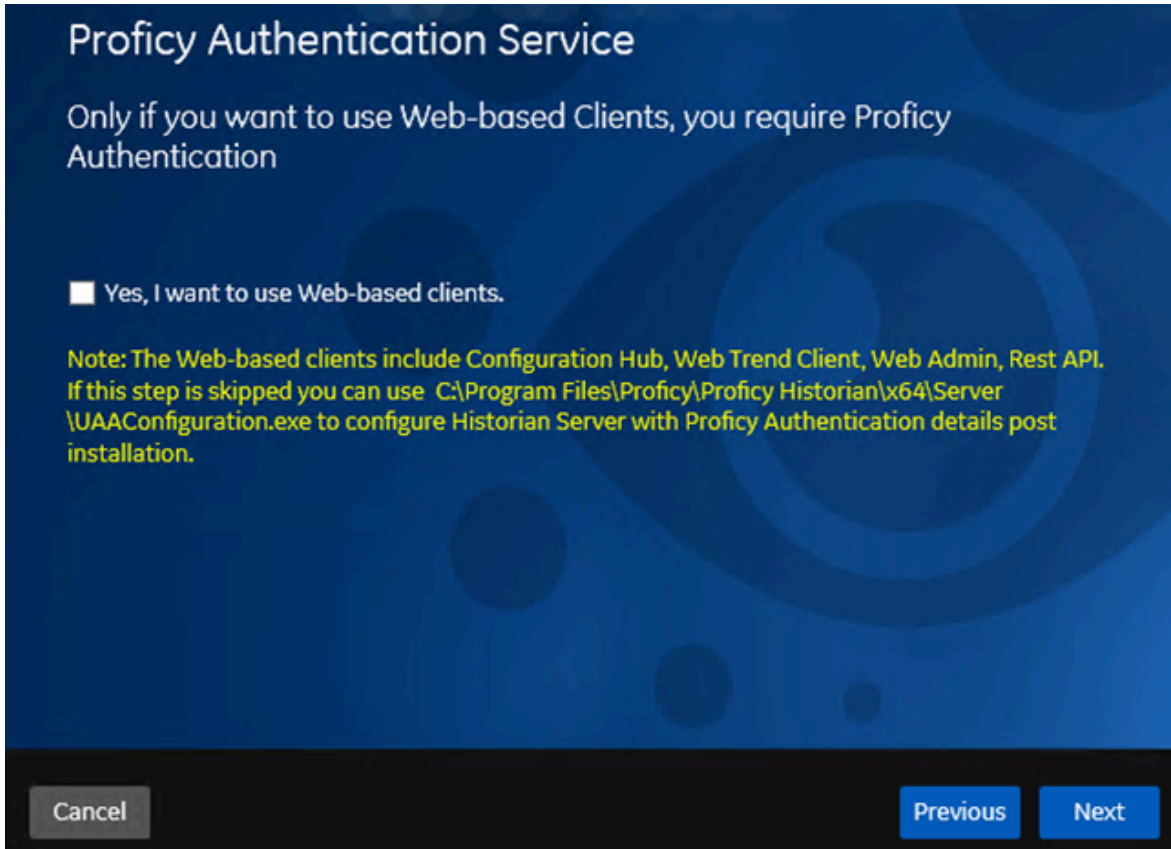
6. If needed, change the default installation drive of the Historian server, and then select **Next**. The **Override the default Historian data Path?** page appears.



7. If needed, change the default folder of the log files, and then select **Next**. If you want to include the Historian server in a cluster, enter the path to the shared folder of the cluster.

The **Proficy Authentication Service** page appears.

Only if you want to use Web-based Clients (such as Configuration Hub, Trend Client, the Web Admin console, and REST APIs), you need Proficy Authentication. Otherwise, you can skip this step. If you use Web-based Clients, Proficy Authentication is required for user authentication. It provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.



8. If you want to use Web-based Clients, select the **Yes, I want to use Web-based Clients** check box, and provide values as described in the following table.

Field	Description
Proficy Authentication server name	Enter the name of the machine on which the Proficy Authentication server is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. By default, the local hostname is considered.
Public https port	Enter the port number used by the Proficy Authentication service. The default value is 443. Ensure that this port number matches the one on the TCP Port Assignments page during Web-based Clients installation.



Note:

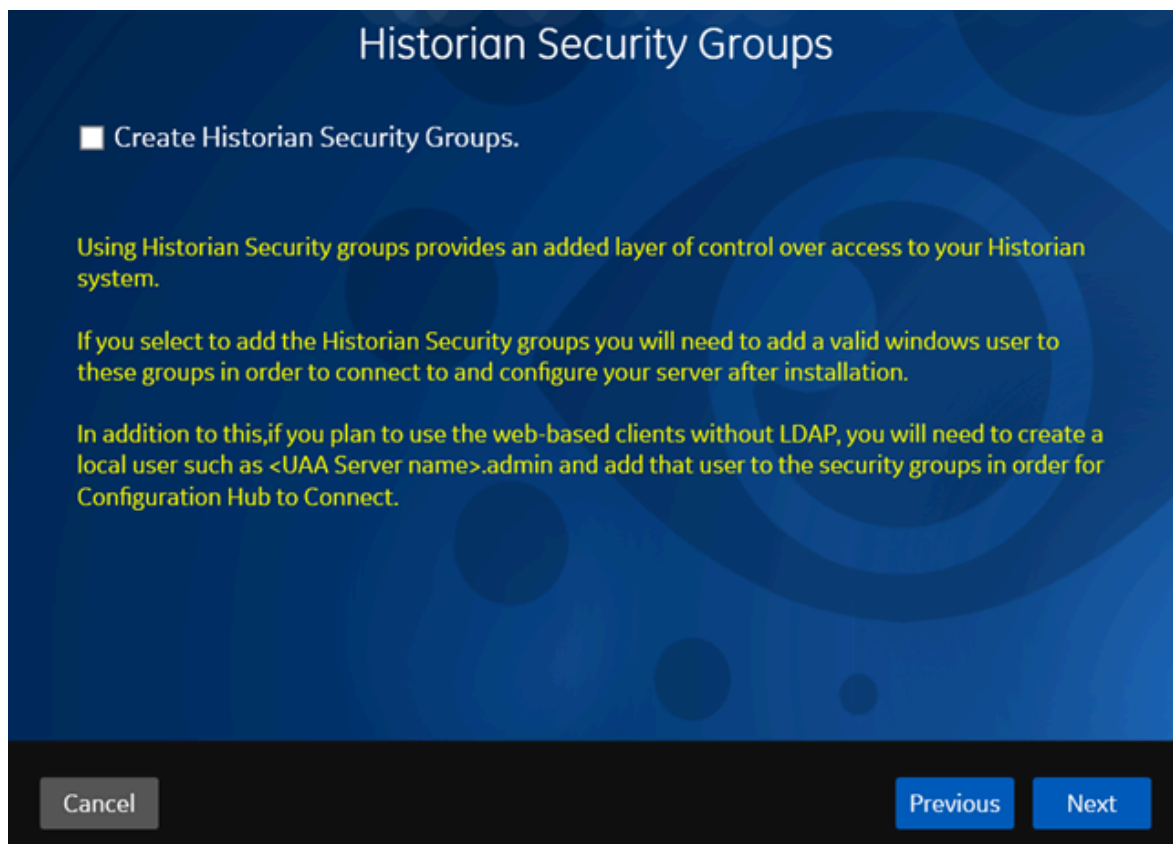
- You can install a Proficy Authentication service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing Proficy Authentication instance. Or, if a Proficy Authentication service is not available, you can install it during Web-based Clients installation.
- If you change the Proficy Authentication server for Web-based Clients later, you must [change the Proficy Authentication server for the Historian server \(on page 89\)](#) as well. You can do so using the Proficy Authentication Configuration tool without the need to install the Historian server again.

9. Select **Next**.

The **Historian Security Groups** page appears.

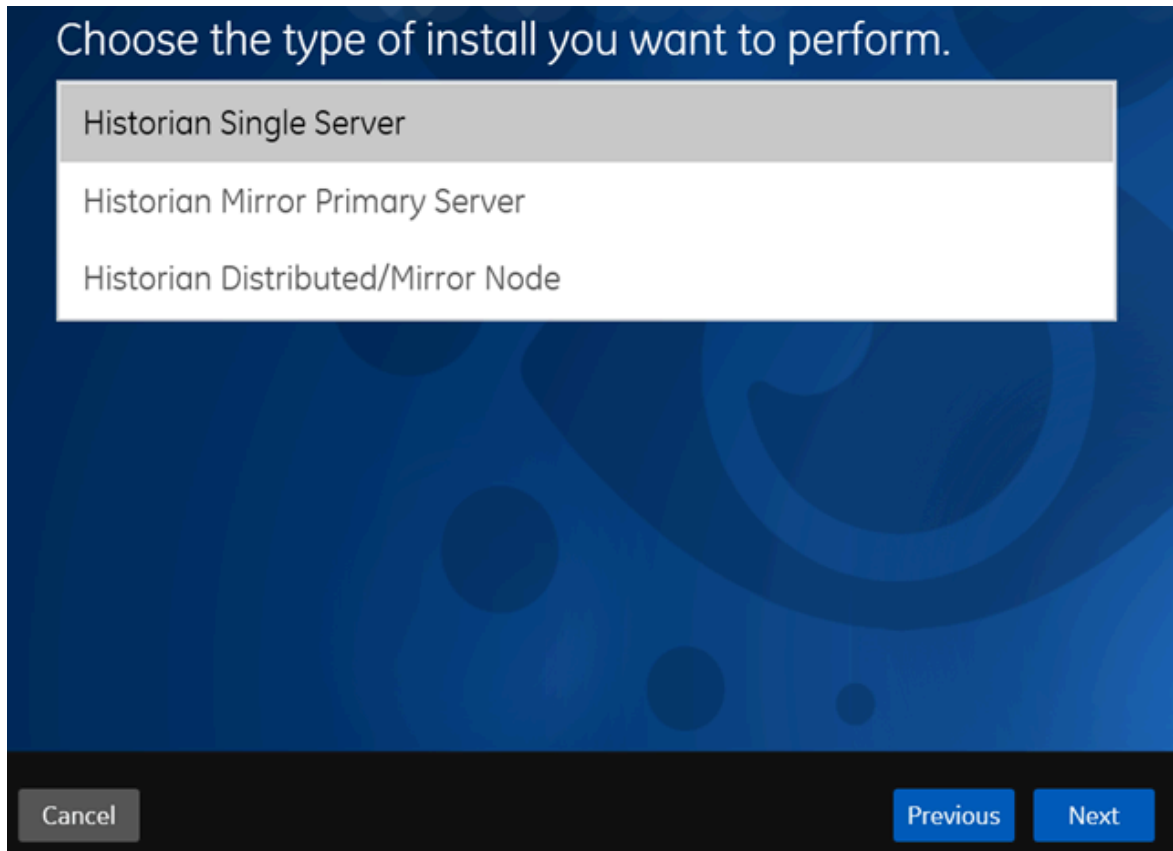
Using Historian security groups provides an added layer of control over access to your Historian system.

By default, the option to create Historian security groups is not selected.



10. If you want the installer to create [Historian security groups \(on page 193\)](#), select the corresponding check box, and then select **Next**.

The **Choose the type of install you want to perform** page appears.



11. Select the type of the Historian server that you want to install, and then select **Next**.
- **Historian Single Server:** This is for a stand-alone Historian system, which contains only one Historian server. This type of system is suitable for a small-scale Historian setup.
 - **Historian Mirror Primary Server:** This is for a horizontally scalable Historian system, which contains multiple Historian servers, all of which are connected to one another. Installing this server will allow you to add machines and distributed/mirror servers to this system.
 - **Historian Distributed/Mirror Node:** This is for a horizontally scalable Historian system. Installing this server will allow you to add this node to a primary server.

The **Ready to Install** page appears.

12. Select **Install**.

The installation begins.

13. When you are asked to reboot your system, select **Yes**.

The Historian server is installed on your machine in the following folder: `<installation drive>:\Program Files\Proficy\Proficy Historian\x64\Server`, and the

following registry path is created: HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\Services.

In addition, the following components are installed:

- **The RemoteCollectorConfigurator utility:** A command-line tool, which allows you to manage collectors remotely. By default, it is located in the C:\Program Files\GE Digital\NonWebCollectorInstantiationTool folder. For instructions on using this utility, refer to About Installing and Managing Collectors Remotely.
- **The Proficy Authentication Configuration tool:** A utility that allows you to specify the Proficy Authentication server details to match with the Proficy Authentication server used by Web-based Clients. By default, it is located in the C:\Program Files\Proficy\Proficy Historian\x64\Server folder. For instructions on using this tool, refer to [Change the Proficy Authentication Server \(on page 89\)](#).

Install the Historian Server at a Command Prompt

- [Set up the Historian environment \(on page 21\)](#).
- If you are changing the role of a Historian server that was previously a distributed/mirror server to any other configuration (single-server or mirror primary server), you must first [uninstall Historian \(on page 229\)](#).
- If you are installing a distributed/mirror server, use the same configuration, license key, installation drive, Proficy Authentication instance, and domain as the primary server.

This topic describes how to install single-server Historian at a command prompt. You can also [install the Historian server using the installer \(on page 46\)](#).

After you install Historian at a command prompt, you can choose to generate a template XML file, which contains the installation parameters and the values that you have provided. You can use this XML file for subsequent installations. Similarly, you can use a template XML file instead of providing command-line arguments.

1. Open Command Prompt, and navigate to the <DVD drive>:\Historian folder (for example, E:\Historian).
2. Run the following command:


```
install.exe <argument>=<value> <flag> HistorianCmd=<installation type>
```

The following table provides a list of installation types that you can enter.

Installation Type	Description
StandAlone	Enter this value if you want to install a stand-alone Historian system.
HistorianCore	Enter this value if you want to install a primary server in a horizontally scalable system.
mirror	Enter this value if you want to install a distributed/mirror server in a horizontally scalable system.

The following table provides a list of arguments that you must enter.

Argument	Description
RootDrive	The drive letter where the Historian server binary files will be installed.
DataPath	The disk path where the Historian data files will be stored.
HistAdministrator-Password	The password for the built-in administrator account.
ActiveUaaBaseUrl	<p>The URL to connect to Proficy Authentication to allow Web-based Clients to access Historian. Only if you want to use Web-based Clients, this parameter is required for user authentication. Proficy Authentication provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including OAuth2.</p> <p>Proficy Authentication details are required if you want to use Web-based Clients.</p> <p>By default, the local hostname and the port number of 443 are considered. If the Proficy Authentication service is on the same machine on which you are installing the Historian server, you can accept the default value. If, however, the Proficy Authentication service is on a different machine or uses a different port number, replace those values in the URL as follows:</p> <pre>https://<local host name>:<port number>/uaa</pre> <p>where:</p>

Argument	Description
	<ul style="list-style-type: none"> ◦ <i><Proficy Authentication server></i> is the name of the machine on which Proficy Authentication is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. ◦ <i><port number></i> is the one that you have specified for the public https port in the TCP Port Assignments page during Web-based Clients installation. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: You can install a Proficy Authentication service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing Proficy Authentication instance. Or, if a Proficy Authentication service is not available, you can install it during Web-based Clients installation. In that case, provide the server name where Proficy Authentication is installed. </div>
CreateHistorianSecurityGroups	Indicates whether you want the installer to create Historian security groups. <p>Using Historian security groups provides an added layer of control over access to your Historian system.</p> Enter true or false. If you enter true: <ul style="list-style-type: none"> ◦ You must add a Windows user to the appropriate group (on page 215) (for example, add an administrative user to the iH Security Admins group). Only then you can configure this server. ◦ If the Historian server and collectors are installed on the same machine, you can skip this step; by default, the machine name of the local Historian server is considered. If, however, they are installed on different machines, you must provide the credentials of the Windows user who can access the Historian server machine. In addition, if security groups are available, add the user to the appropriate group (on page 215) (for example, add an administrative user to the iH Security Admins group). Only then you can access Web-based Clients without LDAP. For more information, refer to Implementing Historian Security (on page 188) .

The following table provides a list of flags that you can use.

Flag	Description
[-q], [-quiet], [-s], [-silent]	Use any of these flags for a silent installation. The installation will then happen in the background (without a UI).
[-passive]	Use this flag for a passive installation. The progress of the installation then appears on your screen.
/t	<p>Use this flag to generate the template file, which will contain all the installation arguments and the values that you have provided for each of them. You can then use this file for subsequent installations.</p> <p>By default, this file is named <code>Template_Historian.xml</code>, and it is placed in the <code>temp</code> folder, defined by the <code>%temp%</code> environment variable. If, however, you want to save the file in another folder as well, enter: <code>/t TemplateOutputDirectory=<path></code></p>
/c TemplateInputFile=<path>	Use this flag to use a template file (instead of providing command-line arguments). However, if you do provide command-line arguments as well, they take precedence over the values in the template.

The Historian server is installed on your machine in the following folder: *<installation drive>*:\Program Files\Proficy\Proficy Historian\x64\Server, and the following registry path is created: `HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\Services`.

In addition, the following components are installed:

- **The RemoteCollectorConfigurator utility:** A command-line tool, which allows you to manage collectors remotely. By default, it is located in the C:\Program Files\GE Digital\NonWebCollectorInstantiationTool folder. For instructions on using this utility, refer to Remote Collector Management.
- **The Proficy Authentication Configuration tool:** A utility that allows you to specify the Proficy Authentication server details to match with the Proficy Authentication server used by Web-based Clients. By default, it is located in the C:\Program Files\Proficy\Proficy Historian\x64\Server folder. For instructions on using this tool, refer to [Change the Proficy Authentication Server \(on page 89\)](#).

While installing the Historian server, if you have allowed the installer to create Historian security groups, create a local Windows user with the format <Web-based Clients server name>.admin, and [add the user to the ihSecurityAdmins group \(on page 215\)](#).

This user will log in to Web-based Clients.

Alternatively, you can create Proficy Authentication users in an external Proficy Authentication and map their security groups. For information, refer to [About Proficy Authentication Groups \(on page 158\)](#).

Depending on whether the Historian server will use local or domain security groups, select the appropriate option in Historian Administrator.

Post Installation Steps for Configuring Certificate-based Security

Overview of the Certificate-based Security in Historian

Historian implements certificate-based security to strengthen the authentication mechanism and build trusted connections among the core Historian services. The Mutual Transport Layer Security (MTLS) protocol is used to build trusted connections among the core Historian services.

The core Historian services include the:

- Data Archiver
- Client Manager
- Configuration Manager
- Diagnostic Manager

MTLS Configuration

**Important:**

When you install Historian, you are presented with three install types: **Historian Single Server**, **Historian Mirror Primary Server**, and **Historian Distributed/Mirror Node**. The MTLS protocol and certificate-based security is enabled by default for all install types. If you are installing a **Historian Single Server** or the **Historian Mirror Primary Server**, the security settings for the certificates will be automatically configured by the installer. If you are installing a **Historian Distributed/Mirror Node**, you must configure the security settings manually after installation.

There are two command line utilities provided with Historian that you use to configure or enable the certificate-based authentication. These tools generate the necessary certificate files that are used in MTLS handshaking. After configuring the certificate, you need to restart the Historian services manually.

The following sections describe how to configure your security settings:

- [Install Certificates for Proficy Historian \(on page 58\)](#)
- [Install Proficy Historian Certificates on Different Computers \(on page 66\)](#)

MTLS Binaries

To support MTLS, the Historian install media includes the following files. These files are located in the MTLS folder in the Proficy Historian install folder:

- CreateRootCertificate.exe
- MTLSCertificatesInstall.exe
- openssl.exe
- legacy.dll
- libcrypto-3-x64.dll
- libssl-3-x64.dll
- openssl.cnf

CreateRootCertificate.exe and **MTLSCertificatesInstall.exe** are the two command-line utilities for generating the certificates. The other binaries are the dependent components.

Location of MTLS Binaries

The following figure shows an example of the binaries folder for MTLS feature, when Proficy Historian 2023 is installed in "C" drive:

This PC > Windows (C:) > Program Files > Proficy > Proficy Historian > MTLs

Name	Date modified	Type	Size
CreateRootCertificate.exe	12/15/2022 11:41 AM	Application	22 KB
MTLSCertificatesInstall.exe	12/15/2022 11:41 AM	Application	37 KB
openssl.exe	3/15/2022 9:20 PM	Application	700 KB
legacy.dll	3/15/2022 9:20 PM	Application exten...	152 KB
libcrypto-3-x64.dll	3/15/2022 9:20 PM	Application exten...	5,008 KB
libssl-3-x64.dll	3/15/2022 9:20 PM	Application exten...	754 KB
openssl.cnf	3/15/2022 9:20 PM	CNF File	13 KB

Steps to Install Proficy Historian Certificates

Install Certificates for Proficy Historian

This topic describes how to install root certificates and the certificates for core services, for use with the MTLs feature for Proficy Historian.

Installing Root Certificates



Important:

When you install Historian, you are presented with three install types: **Historian Single Server**, **Historian Mirror Primary Server**, and **Historian Distributed/Mirror Node**. The MTLs protocol and certificate-based security is enabled by default for all install types. If you are installing a **Historian Single Server** or the **Historian Mirror Primary Server**, the security settings will be automatically configured by the installer. However, if you are installing a **Historian Distributed/Mirror Node**, you must configure the security settings manually after installation. Use the following steps to configure your security settings.

After installing the Historian Distributed/Mirror Node, you need to generate root certificate. Use the `CreateRootCertificate.exe` utility in the MTLs folder from the Historian install from a command prompt with **Administrator privileges**, as described in the following steps.

1. Right-click the Command Prompt, and select **Run as Administrator**.
2. Navigate to the MTLs folder in the Historian installed path. For example:

```
cd C:\Program Files\Proficy\Proficy Historian\MTLs
```

3. Run the `CreateRootCertificate.exe` command using the following arguments:

Argument	Description
EnableMTLS	<p>Specifies whether MTLS is enabled. If you do not specify a value, MTLS feature is enabled by default (and set to 0 by default):</p> <ul style="list-style-type: none"> ◦ 0 – MTLS feature is disabled ◦ 1 – MTLS feature is enabled <p>For example, if you want to disable the certificate-based security, simply pass “0” to the tool.</p>
Password	<p>Specifies the word or phrase that you use to protect your certificate. The Password argument is mandatory, whereas Number of Days is optional. An example Passphrase is: P@55w0rd.</p>
The Number of Days	<p>Optional. Specifies the Number of Days for the root certificate to be valid. After the specified days, the certificate validity expires.</p> <p>If you do not pass any value for Number of Days, the setting defaults to 365 days. For example, if the Number of Days is 3650, the certificate is valid for 10 years from the generated date.</p>

**Note:**

If you fail to pass any values to this command-line, the command will fail to create the root certificate.

The following is an example of the command-line. In this example, MTLS is enabled, the passphrase is P@55w0rd, and the certificate will be valid for 3650 days (10 years):

```
C:\Program Files\Proficy\Proficy Historian\MTLS CreateRootCertificate.exe 1 P@55w0rd 3650
```

4. After executing `CreateRootCertificate.exe`, locate the root keys generated in the same MTLS folder:

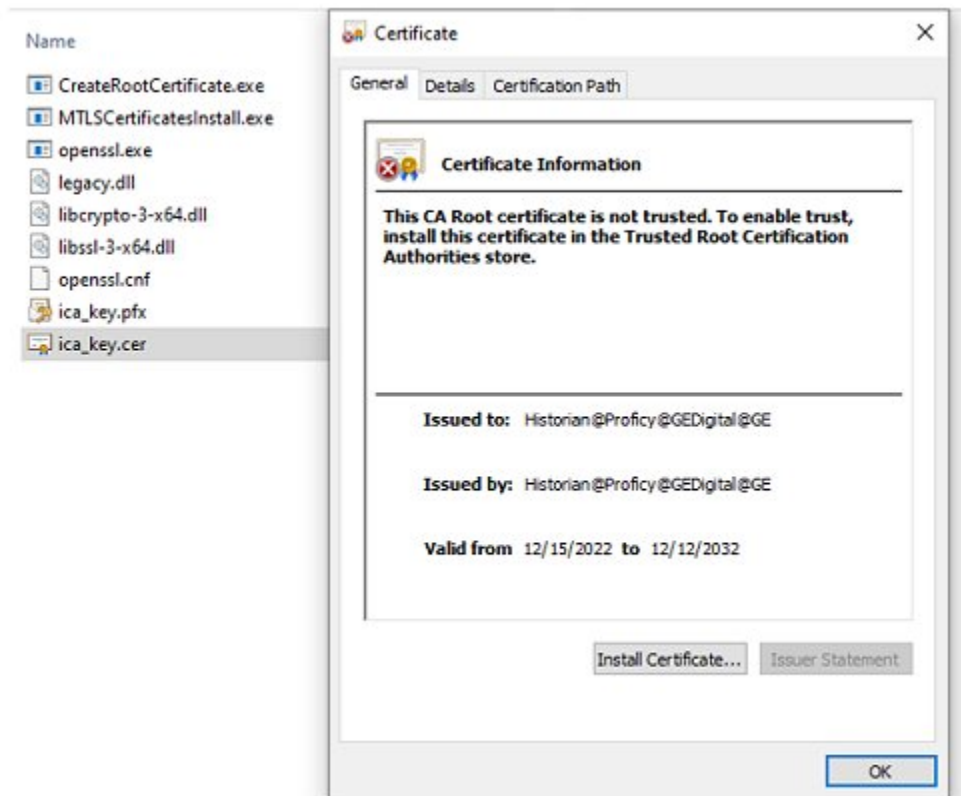
- **ica_key.pfx** – Password protected certificate that contains the private key to sign the core services certificates.
- **ica_key.cer** – Root certificate contains the public and different attributes of the certificate.

The following figure shows examples of the root certificates.

Name	Date modified	Type	Size
CreateRootCertificate.exe	12/15/2022 5:48 PM	Application	168 KB
MTLSCertificatesInstall.exe	12/15/2022 1:38 PM	Application	212 KB
openssl.exe	3/15/2022 9:20 PM	Application	700 KB
legacy.dll	3/15/2022 9:20 PM	Application exten...	152 KB
libcrypto-3-x64.dll	3/15/2022 9:20 PM	Application exten...	5,008 KB
libssl-3-x64.dll	3/15/2022 9:20 PM	Application exten...	754 KB
openssl.cnf	3/15/2022 9:20 PM	CNF File	13 KB
ica_key.pfx	12/15/2022 5:50 PM	Personal Informati...	3 KB
ica_key.cer	12/15/2022 5:50 PM	Security Certificate	2 KB

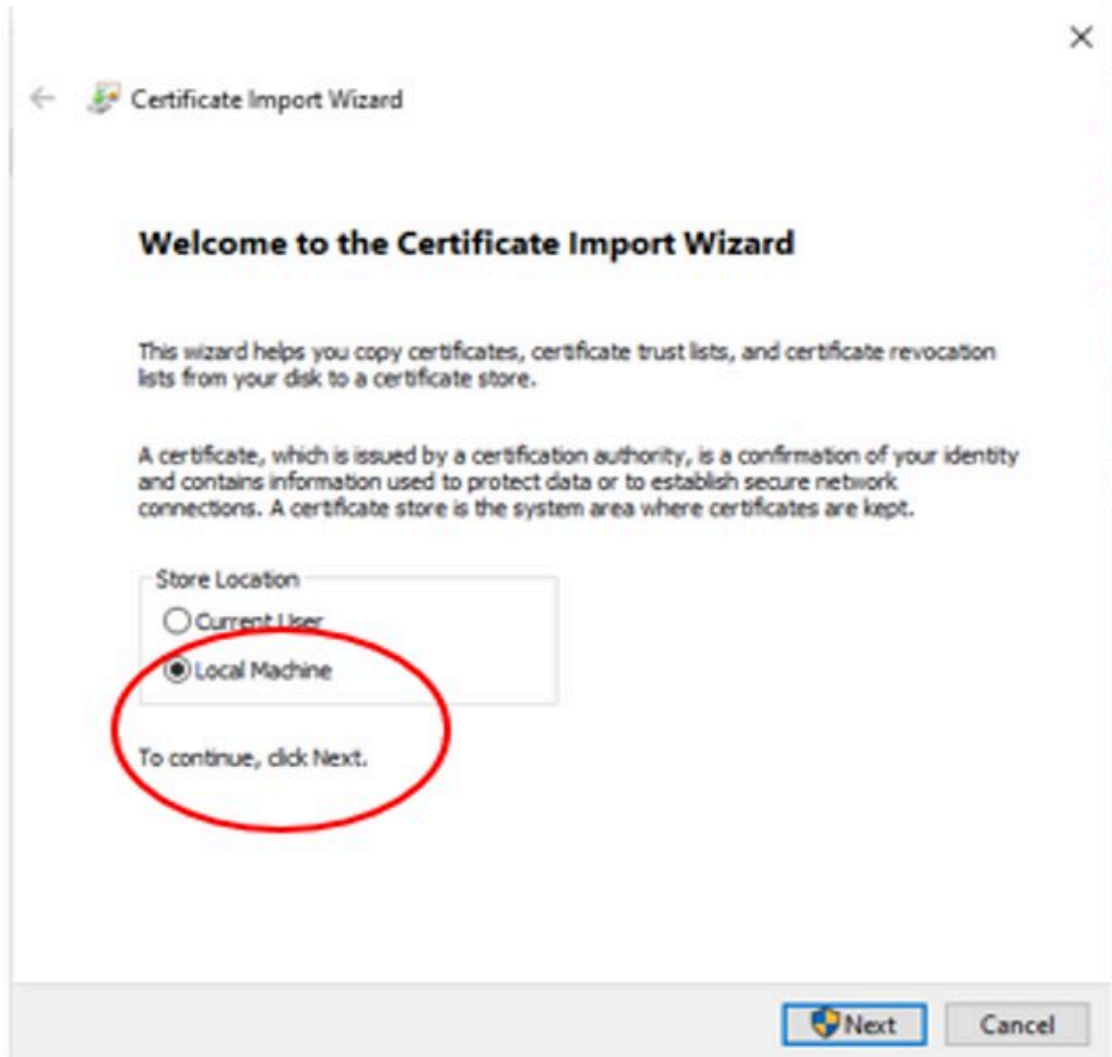
After generating the root certificate, this certificate needs to be added to the “Trusted Root Certification Authorities” certificate store on the Local Machine.

5. Double-click the `ica_key.cer` file. The certificate dialog appears as shown in the following figure.

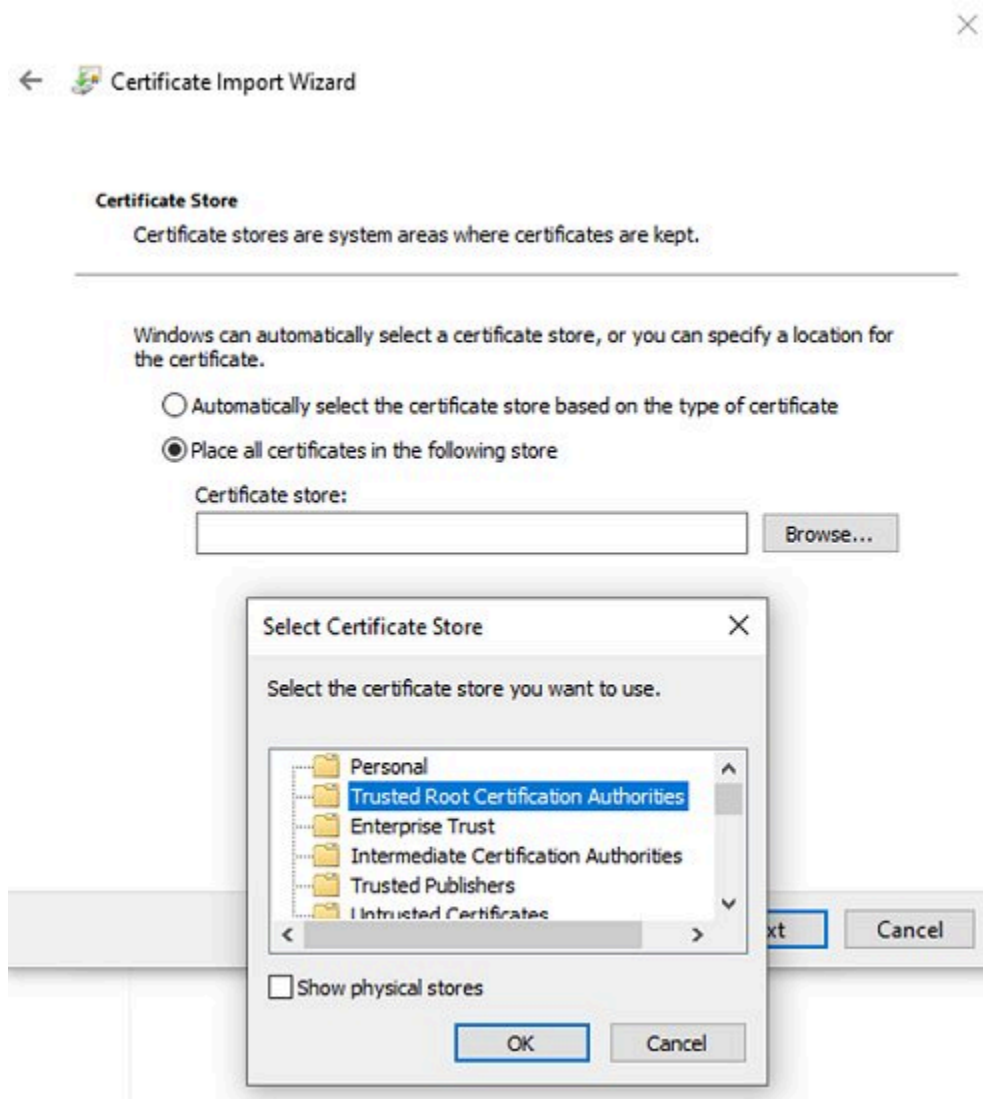


6. Select **Install Certificate** to launch the Certificate Import Wizard.

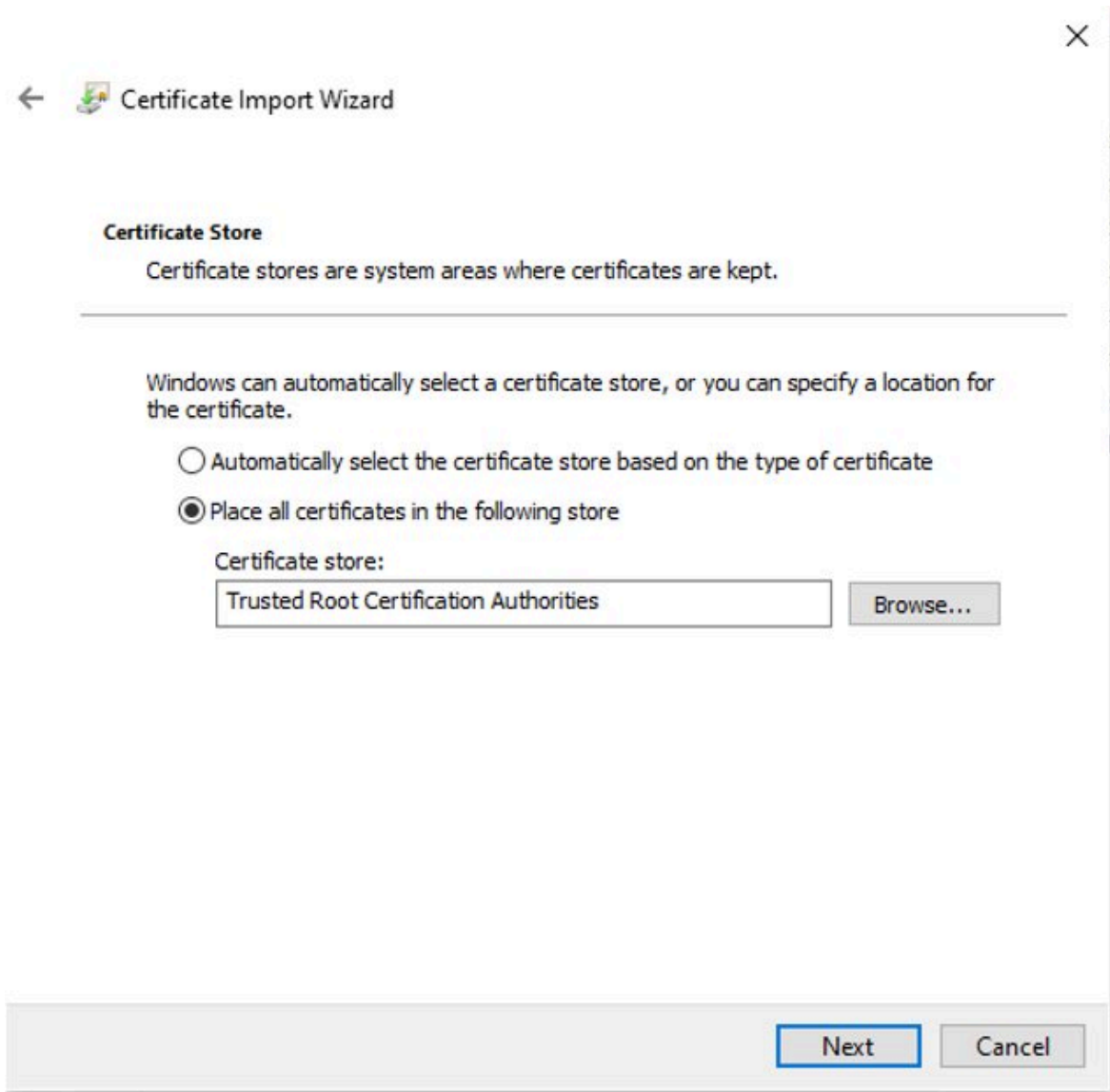
7. Click **Next** to continue. The Certificate Import Wizard appears as shown in the following figure.



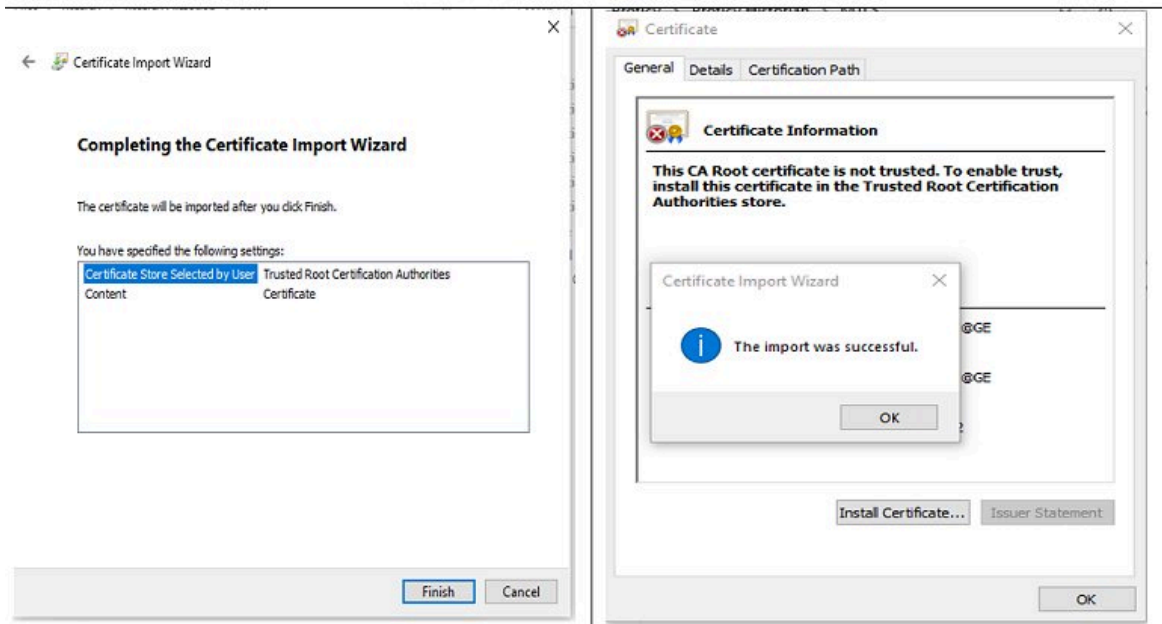
8. Select **Local Machine** and click **Next** to continue. The following screen appears.



9. Select **Place all certificates in the following store**, and click **Browse** to display the list of stores from where Trusted Root Certification Authorities can be selected.
10. Select the **Trusted Root Certification Authorities**, and click **OK**. The following dialog box appears.



11. Click **Next** to continue. The Completing the Certificate Import Wizard appears.



12. Click **Finish** to add the certificate to the **Trusted Root Certification Authorities**. When the import succeeds, the “The import was successful” message appears.


Installing Certificates for Core Services


For generating certificates for core service, run the `MTLSCertificatesInstall.exe` utility from the command prompt with Administrator privileges.

1. Launch from the command prompt with Administrator privileges. For example:

```
C:\Program Files\Proficy\Proficy Historian\MTLS\MTLSCertificatesInstall.exe P@55w0rd 3650
```

The `MTLSCertificatesInstall.exe` utility takes the following arguments:

Argument	Description
Password	Specifies the word or phrase that you use to protect your certificate. The Password argument is mandatory, whereas Number of Days is optional. An example Passphrase is: P@55w0rd. <div data-bbox="862 1713 1425 1862" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: The same Password used for creating the root certificate needs to be used </div>

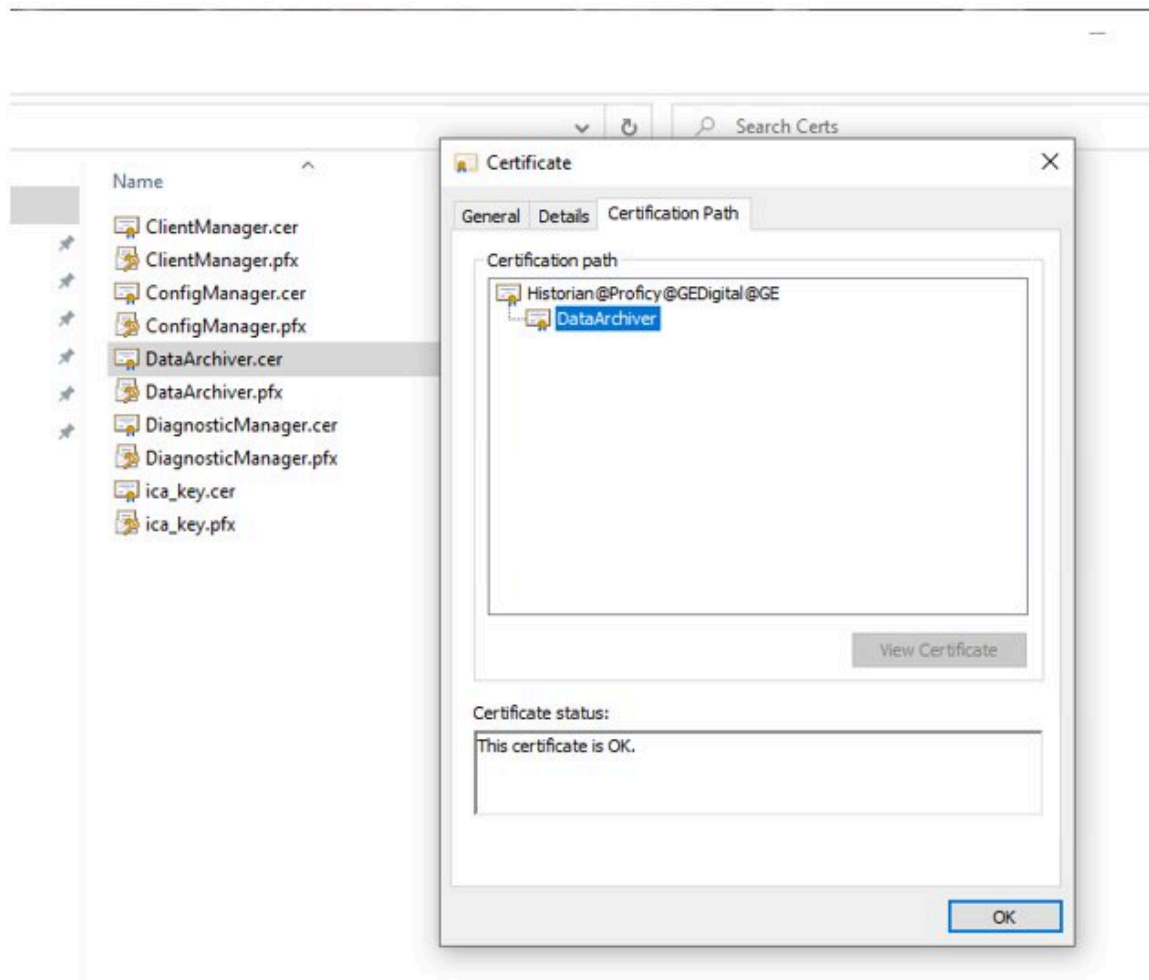
Argument	Description
	 here. This is so that the Password will be same while passing the argument between executables. The MTLSCertificateInstall.exe utility uses this password to open the root certificate private key (ica_key.pfx) and sign the core services certificates.
The Number of Days	<p>Optional. Specifies the Number of Days for the root certificate to be valid. After the specified days, the certificate validity expires.</p> <p>If you do not pass any value for Number of Days, the setting defaults to 365 days. For example, if the Number of Days is 3650, the certificate is valid for 10 years from the generated date.</p>

For each service, two certificates will be generated as shown in the following figure:

Program Files > Proficy > Proficy Historian > MTLS

Name	Date modified	Type	Size
CreateRootCertificate.exe	12/15/2022 5:48 PM	Application	168 KB
MTLSCertificateInstall.exe	12/15/2022 1:38 PM	Application	212 KB
openssl.exe	3/15/2022 9:20 PM	Application	700 KB
legacy.dll	3/15/2022 9:20 PM	Application exten...	152 KB
libcrypto-3-x64.dll	3/15/2022 9:20 PM	Application exten...	5,008 KB
libssl-3-x64.dll	3/15/2022 9:20 PM	Application exten...	754 KB
openssl.cnf	3/15/2022 9:20 PM	CNF File	13 KB
ClientManager.pfx	12/15/2022 6:54 PM	Personal Informati...	3 KB
ConfigManager.pfx	12/15/2022 6:54 PM	Personal Informati...	3 KB
DataArchiver.pfx	12/15/2022 6:54 PM	Personal Informati...	3 KB
DiagnosticManager.pfx	12/15/2022 6:54 PM	Personal Informati...	3 KB
ica_key.pfx	12/15/2022 5:50 PM	Personal Informati...	3 KB
ClientManager.cer	12/15/2022 6:54 PM	Security Certificate	2 KB
ConfigManager.cer	12/15/2022 6:54 PM	Security Certificate	2 KB
DataArchiver.cer	12/15/2022 6:54 PM	Security Certificate	2 KB
DiagnosticManager.cer	12/15/2022 6:54 PM	Security Certificate	2 KB
ica_key.cer	12/15/2022 5:50 PM	Security Certificate	2 KB

2. Double-click each service .cer file as shown in the following figure, and check whether each generated certificate has a valid root certificate chain.



3. After all required certificates are generated, restart the core Historian services. Without valid certificates, core services cannot establish connections to each other.

Install Proficy Historian Certificates on Different Computers

Distributed and Mirror Setups

For MTLS certificates for Historian, be aware of the following steps when working with distributed/mirror setups:

- You will need to generate root certificate on one machine and copy the certificate to all machines that are part of distributed or mirror network. For steps on how to generate the root certificate on the first machine, see the [Install Certificates for Proficy Historian \(on page 58\)](#) topic.
- These root certificates need to be copied into the MTLS folder of Proficy Historian install path on all machines.
- Add the root certificate to the “Trusted Root Certification Authorities” store on all machines.

- Core service certificates can be generated separately on each machine.
- The same password that was provided while creating the original root certificate, needs to be used for creating core service certificates across all of the machines.
- Primarily in this setup, root certificates are common across the machines. Core service certificates will be created separately for each machine. However, the same password that was provided to create the root certificate will be used across machines while creating core service certificates.
- The procedure to create the core service certificates is same as mentioned in the [Install Certificates for Proficy Historian \(on page 58\)](#) topic.

Cluster Nodes

Generate a root certificate and certificates for core services separately on each cluster node that is part of the cluster environment.

Existing Root Certificates

If you want to use existing root certificates for MTLS support with Historian, be aware that:

- You can use your existing root certificates for signing the *core service* certificates.
- To use existing root certificates, follow the requirements below (instead of generating the certificate through the CreateRootCertificate.exe). You can choose to use your existing root certificates if above criteria matches the list below.

Requirements for Using Existing Root Certificates:

- Certificates must be in X.509 standard.
- You must have .cer and .pfx format certificates that have public and private keys respectively, already generated.
- The .pfx files need to be password protected.
- The following attributes or subjects needs to be set in the file:

Attribute	Description	Setting
CN	Common Name	CN = Historian@Proficy@GEDigital@GE
OU	Organization Unit	OU = MFG
O	Organization	O = ProficyHistorian
L	Local Name	L = HYD

Attribute	Description	Setting
S	State or Province	S = TG
C	Country Name	C=IN

- Instead of generating the root certificates from `CreateRootCertificate.exe`, you can choose to use your own root certificates if the above criteria matches.
- Use the `MTLSCertificatesInstall.exe` utility for generating all the core service certificates.

Root Certificates on Microsoft Windows 7 Machines



Note:

These steps only apply to versions of Historian that support Microsoft Windows 7 (Historian 7.0 - Historian 7.2).

To generate a root certificate on a Windows 7 machine, do the following:

1. From a command prompt enter `mmc.exe`. The Windows MMC appears.
2. On the **File** menu, select **Add/Remove Snap-in**.
3. Click **Add**, and then double-click **Certificates** and then select **Computer Account**.
4. In the Select Computer screen, select **Local Computer**.
5. Click **Finish**.
6. Click **OK**.
7. With the snap-in now on the local computer, import the certificate into "Certificates (Local Computer) > Trusted Root Certification Authorities" folder:
 - a. In the Certificates folder in the navigation pane, browse to the **Certificates (Local Computer) > Trusted Root Certification Authorities** folder.
 - b. From the **Actions** menu, click **All Tasks**. The Certificate Wizard appears.
 - c. Click **Next**.
 - d. On the next screen, navigate to the folder where the **ica_key.cer** certificate file resides. By default this path is: `InstallationDrive:\Program Files\Proficy\Proficy Historian\MTLS`.
 - e. Select the **ica_key.cer** certificate file, and click **Next**.
 - f. Select **Place All Certificates in the following store**, and then browse and select the **Trusted Root Certification Authorities** store.
 - g. Click **Next**. The final summary screen appears.
 - h. Click **Finish**. A message appears when the import is complete.
 - i. Click **OK**.
 - j. Before closing the MMC, **Save** your settings.

Upgrade Scenarios when Working with Historian Server Certificates

Be aware of the following when upgrading your Historian:

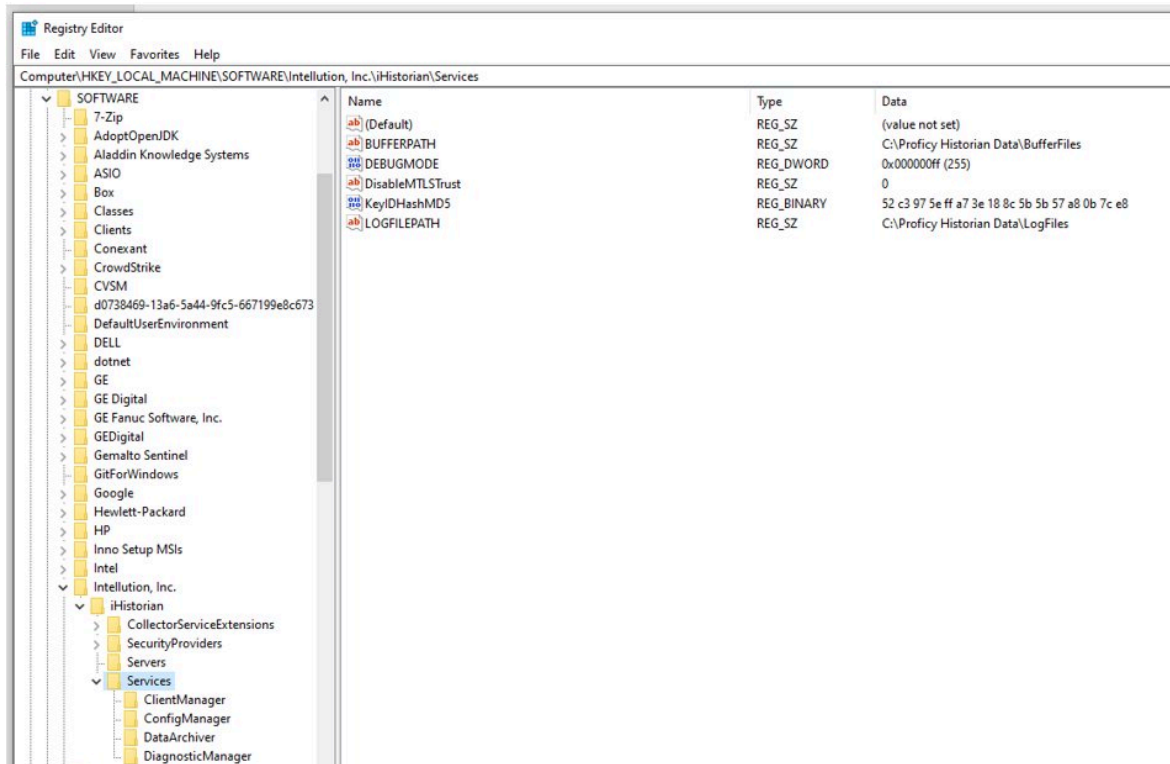
- By default, certificate-based security is enabled. Your configuration for certificates is automatic, unless you are installing or upgrading a distributed/mirror node. If you do not configure your certificates in this scenario, your Historian services may not start when you go to run it for the first time.
- You will need to regenerate the certificates if you uninstall the existing version and reinstall any version that supports certificate-based security.
- You will need to regenerate the certificates for Historian in-place upgrades that support certificate-based security.
- You will NOT need to regenerate the certificates for SIM over SIM upgrades that support the MTLs feature.

Troubleshooting Historian Server Certificates

Be aware of the following when working with certificates in Historian:

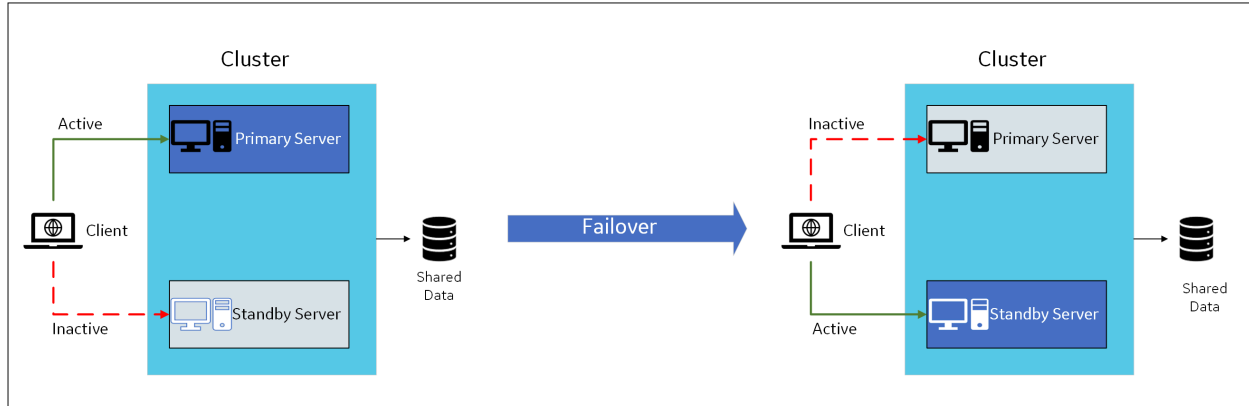
- When you install Historian, you are presented with three install types: **Historian Single Server**, **Historian Mirror Primary Server**, and **Historian Distributed/Mirror Node**. The MTLs protocol and certificate-based security is enabled by default for all install types. If you are installing a **Historian Single Server** or the **Historian Mirror Primary Server**, the security settings will be automatically configured by the installer. However, if you are installing a **Historian Distributed/Mirror Node**, you must configure the security settings manually after installation.
- You will need to follow the same procedure for installing certificates when certificates expire in the future.
- Prior to adding any new root certificate to the “Trusted Root Certification Authorities” store, it’s a better practice to remove an existing root certificate from the store first.
- After the root certificates are added to the “Trusted Root Certification Authorities,” all core services need to be restarted.
- If the MTLs authentication fails due to a mismatch in certificates, improperly generated certificates, expired certificates, or any issue related certificates, it will not cause the core Historian Services to stop. These services will be in running state, but the trusted connections among these services will fail. In this scenario, sometimes client tools will not be able to connect to the services. Sometimes client tools connect to Client Manager but cannot do any operations on Historian server. They simply show the “Not Connected” error.
- After trusted connections among core Historian services succeed, they will be in the same trusted state until these services are stopped or restarted.

- It is strongly recommended to provide same expiration date (in the Number of days field) for the root and all other core services certificates.
- If you forget to install the certificates, some of your core Historian services may not start after you complete your Historian install or upgrade.
- To see any specific errors that may be caused by certificate-based security, you need to enable full debugging by adding the "FF" hexadecimal value to the DEBUGMODE registry as shown in the following figure.



Set Up High Availability of the Historian Server

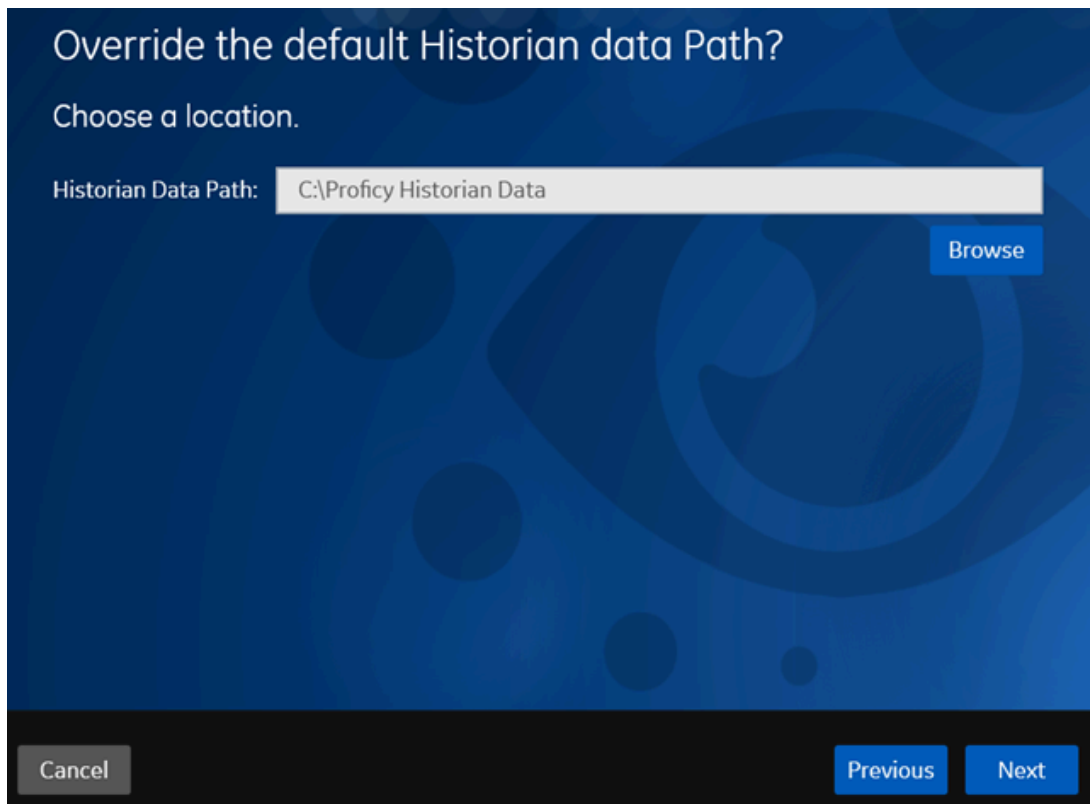
In a cluster environment, multiple servers are installed, which share the same data. Each of these servers is called a node. One of them acts as the primary server, while the others are standby servers. If the primary server is down, one of the standby servers is used.



Historian works with Microsoft Failover Cluster Manager to ensure high availability of the server.

1. Ensure that your network is enabled for multicast traffic.
2. Create a shared drive on your network that all the servers in the cluster can access, and create a database folder in that drive.
3. On each node that you want to add to the cluster:

- a. [Install the Failover Clustering feature.](#)
- b. [Install the Historian server \(on page 46\).](#) During the installation, in the **Historian Data Path** field, enter the path to the folder on the shared drive that you have created.



4. If you are upgrading the Historian server on a passive node, an error message may appear behind the installer screen, stating that the Archives directory is not created. You can ignore this message, or you can make the node active before upgrading the Historian server.

1. If you have upgraded the Historian server, on all the cluster nodes:
 - a. Right-click the cluster, and then select **Properties > Resource Types**.
 - b. If the user-defined resource types are not available, select **Add**.
 - c. Select *<Installation folder of the Historian server>/x64/Server/ Historian.dll* as the resource DLL path with Historian and AlarmArchiver as both the resource type names and display names.

The Historian servers are now part of the cluster, thus achieving high availability. The remaining steps are required only for first-time installation of the Historian server (not upgrade).

2. Access the primary node of the cluster.
3. [Create a failover cluster.](#)
4. [Add a storage to the failover cluster.](#)

5. Add user-defined resource types, Historian and AlarmArchiver, to the cluster. These resources are created when you install the Historian server.
 - a. Right-click the cluster, and then select **Properties > Resource Types**.
 - b. If the user-defined resource types are not available, select **Add**.
 - c. Select `<Installation folder of the Historian server>/x64/Server/ Historian.dll` as the resource DLL path with Historian and AlarmArchiver as both the resource type names and display names.
6. Select **Roles > Create Empty Role**.

A role is created.
7. Add the Historian application to the cluster:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Resource > Historian**.
 - c. Follow the on-screen instructions to add the new Historian resource to the role.
8. Add a client access point to the role:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Resource > Client Access Point**.
 - c. Follow the on-screen instructions to add a client access point to the role.
9. Add a storage to the role:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Storage**.
 - c. Follow the on-screen instructions to add the storage that you have created in step 3. You can use a storage only once.
10. Add the following dependencies to the Historian resource:
 - a. Double-click the Historian resource.

The **Historian Properties** window appears.
 - b. Select **Dependencies**.
 - c. Select **Insert**, and add the following dependencies using the AND operation.
 - Client access point
 - IP address
 - Storage
11. Add the Alarm Archiver resource to the cluster:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Resource > Alarm Archiver**.

- c. Follow the on-screen instructions to add the alarm archiver resource to the role.
 - d. Double-click the Alarm Archiver resource.
The **Alarm Archiver Properties** window appears.
 - e. Select **Dependencies**.
 - f. Select **Insert**, and then add the Historian service as a dependency. You do not need to add the cluster disk and IP address as dependencies.
12. Add generic services.
- a. In the **Summary** section of the Historian role, right-click the Client Manager resource, and then select **Properties > Dependencies**.
 - b. Add the IP address as a dependency, and then select **Apply**.
 - c. Select **General**, select the **Use Network Name for Computer Name** check box, and then select **OK**.
13. Repeat the previous step for the following services:
- Configuration Manager
 - Diagnostics Manager
 - Historian Embedded PostgreSQL Database
 - Historian Embedded Tomcat Container
 - Historian Indexing Service

The services appear under the Historian role.

Historian	
Name	Status
Storage	
+ Cluster Disk 2	Online
Server Name	
+ Name: HistClust7	Online
Roles	
+ Historian Client Manager(x64)	Online
+ Historian Configuration Manager(x64)	Online
+ Historian Diagnostics Manager(x64)	Online
+ Historian Embedded PostgreSQL Database	Online
+ Historian Embedded Tomcat Container	Online
+ Historian Indexing Service	Online
Other Resources	
+ New Historian	Online

14. Select the Historian role, and then in the **Actions** section, select **Start Role**.

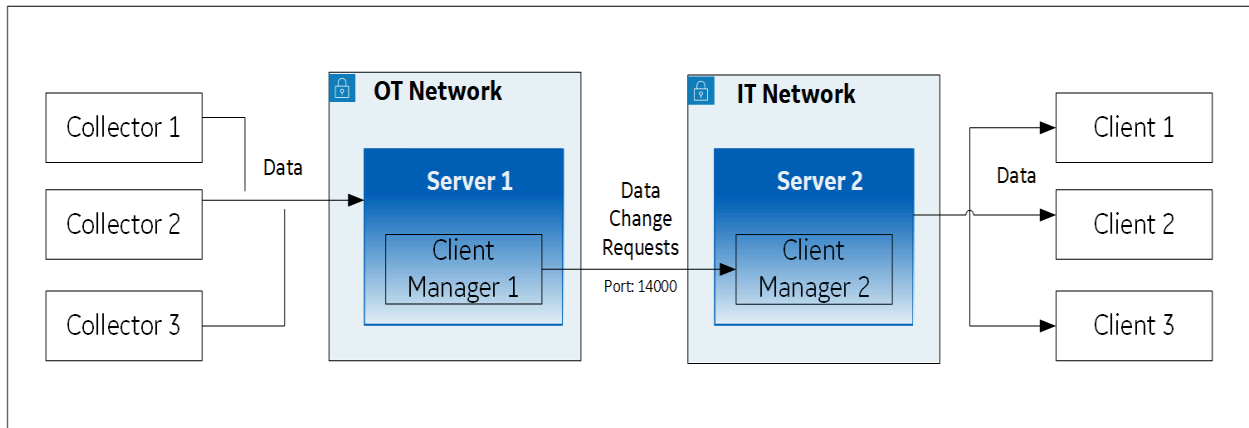
The Historian servers are now part of the cluster, thus achieving high availability.

Set Up a Mirror of Mirror

1. [Install Historian server \(on page 46\)](#) on each machine that you want to use in the mirror of mirror setup.
2. Set up Configuration Hub ([on page](#)) on each machine that you want to use in the mirror of mirror setup.
3. Add a system ([on page](#)). The server that you specify while adding the system serves as the primary server for the system.
4. Create data stores ([on page](#)) in the primary server in the public/IT network with the same name as the data stores in the primary server in your organization network.

You can set up a mirror of the Historian server in a network different from that of your organization. When you do so, any tag/data update requests to the Historian server can be routed to the public and IT network instead of your organization's network.

Single-Node Setup: The following image shows two networks - OT and IT - with a Historian server installed in each network. These networks communicate using port 14000.



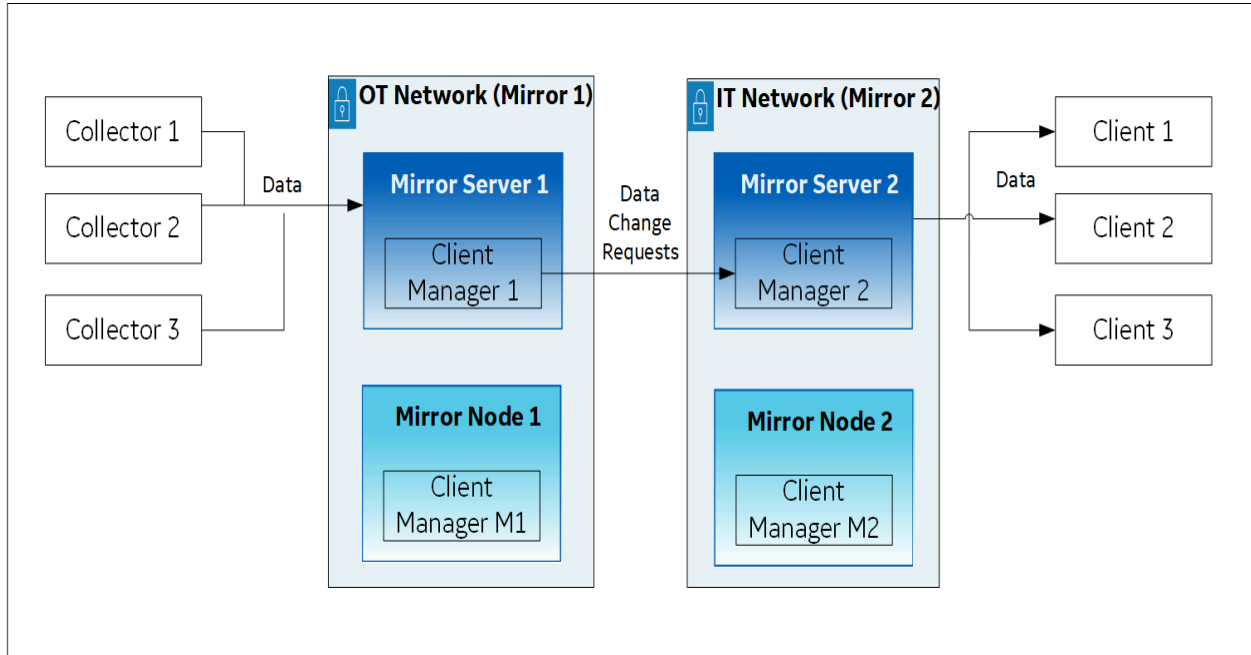
In this setup:

1. Server 1 is the primary server in the OT network; it stores data from collectors.
2. Server 2 is the primary server in the IT network; it is connected to clients.
3. When a tag/data is created, updated, or deleted, Client Manager 1 communicates the same with Client Manager 2 (installed with Server 2 in the IT network).
4. The change in the tag/data is replicated in Server 2 (that is, data is created, updated, or deleted accordingly).
5. The latest data is retrieved from Server 2 using the clients.

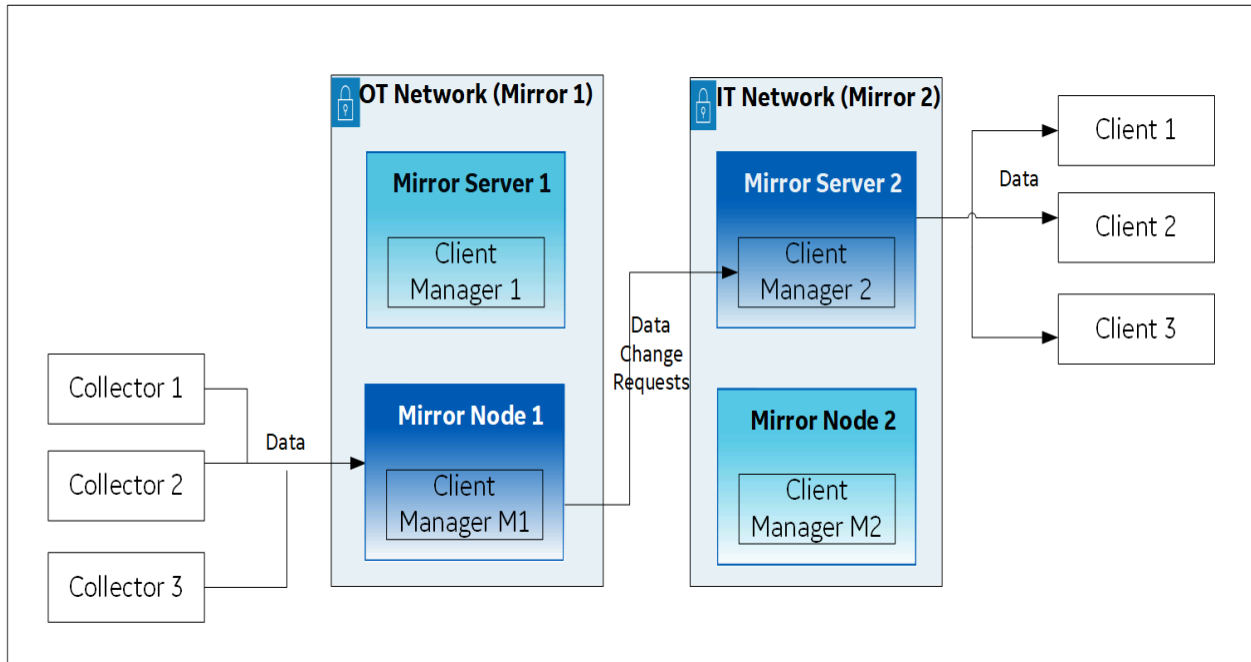
Mirror Setup: The following image shows two mirrors:

- Mirror 1 includes Mirror Server 1 and Mirror Node 1, which is a backup/standby node for Mirror Server 1; both these machines are in the OT network.
- Mirror 2 includes Mirror Server 2 and Mirror Node 2, which is a backup/standby node for Mirror Server 2; both these machines are in the IT network.

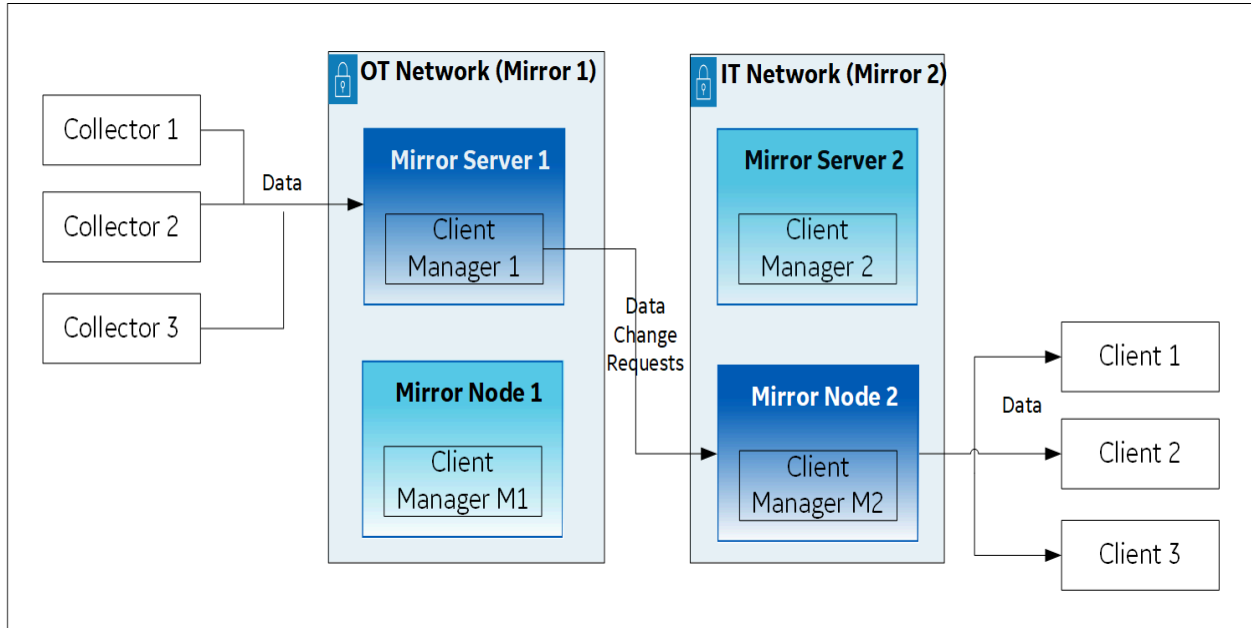
Client Manager 1 in Mirror Server 1 communicates with Client Manager 2 in Mirror Server 2.



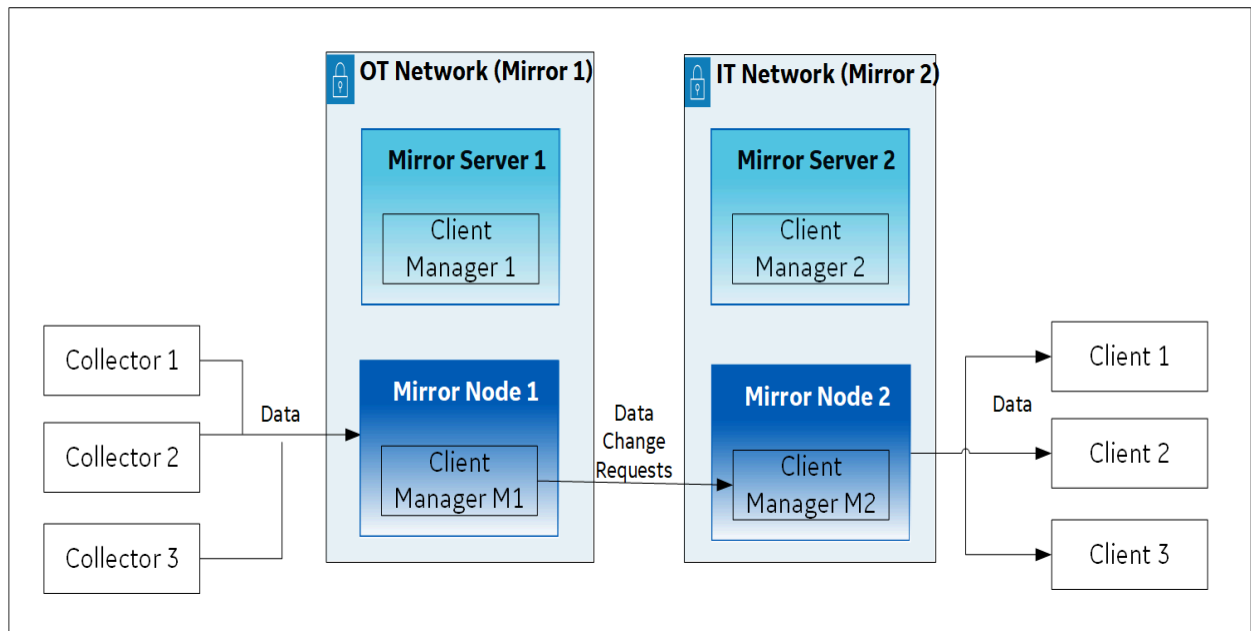
If Mirror Server 1 goes down, Client Manager M1 in Mirror Node 1 communicates with Client Manager 2 in Mirror Server 2.



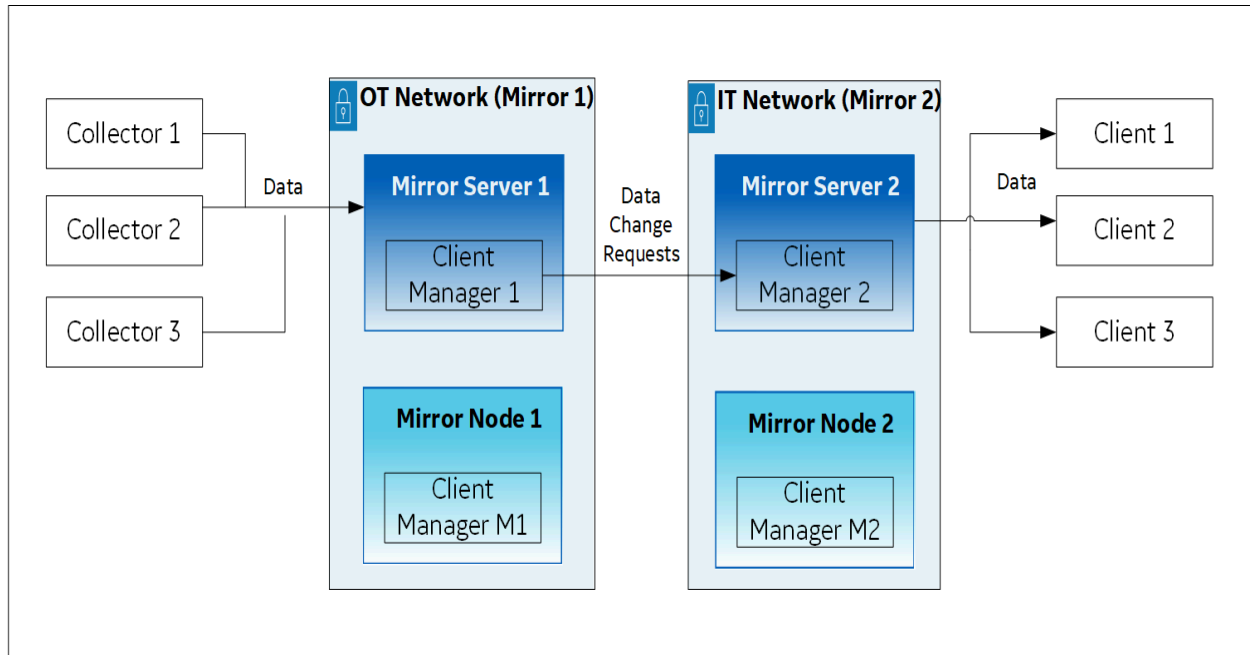
Similarly, if Mirror Server 2 goes down, Client Manager 1 in Mirror Server 1 communicates with Client Manager M2 in Mirror Node 2.



If both Mirror Server 1 and Mirror Server 2 are down, Client Managers M1 and M2 communicate with each other.



If Mirror Server 1 and/or Mirror Server 2 are available, the connection is re-established using these primary servers.



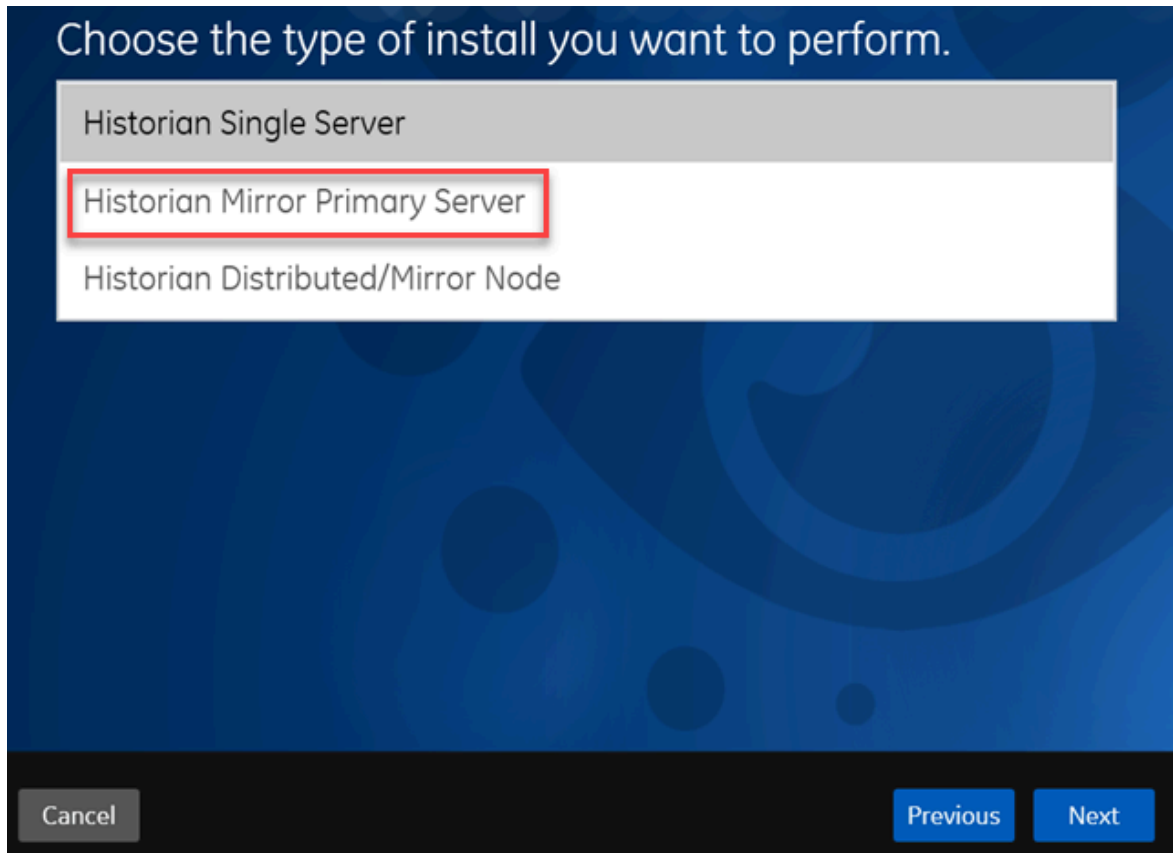
Thus, you can choose to always retrieve data from either Mirror Server 2 or Mirror Node 2. In addition, the store-and-forward functionality is available (in case Client Managers are not yet connected).

This topic describes how to set up a mirror of mirror for the configuration described in the preceding example. It includes the following high-level steps:

1. Installing the Historian server on all the machines
2. Setting up mirror 1
3. Setting up mirror 2
4. Setting up a mirror of mirror

Installing the Historian server

1. On the machines designated as the mirror primary servers (Mirror Server 1 and Mirror Server 2 in the example), [install the Historian server \(on page 46\)](#). During the installation, select **Historian Mirror Primary Server** on the **Choose the type of install you want to perform** page.



2. On the machines designated as mirror nodes (Mirror Node 1 and Mirror Node 2 in the example), [install the Historian server \(on page 46\)](#). During the installation, select **Historian Distributed/Mirror Node** on the **Choose the type of install you want to perform** page.

Set up Mirror 1:

3. On the mirror primary server in your organization's network (Mirror Server 1 in the example), access Configuration Hub [\(on page 46\)](#).
4. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.
A list of systems appears in the main section.
5. Expand Mirror Server 1.
A list of servers in the system appears.
6. Select **+**.

Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...	Out Of
	Connected	43.3	0.5	0.45	0	0	0
	Not Connected	NA	NA	NA	NA	NA	NA

The **Add Server Machine: <system name>** window appears.

- Enter the host name or IP address of the mirror node in your organization's network (Mirror Node 1 in the example), and then select **Add**.

The distributed server is added to the system. A distributed location is added in the server.

- Right-click Mirror Node 1, and then select **Browse Locations**.

Machine Name	STATUS	Archive Compre...	Write Cache Hit R...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...
torsc-collectorsclient		5.5	0.5	0.33	0	0
collectorsclien6		NA	NA	NA	NA	NA

A list of distributed locations in the system appears.

- Select **Mirror Locations**.

A list of mirror locations in the system appears.

- In the upper-right corner of the main section, select **+**.

The **Add Mirror Location** window appears.

- Provide values as described in the following table.

Field	Description
MIRROR LOCATION NAME	Enter a name for the mirror location. A value is required and must be unique for the system.

Field	Description
SERVER MACHINES	Select the servers that you want to add to the mirror group (Mirror Server 1 and Mirror Node 1 in this example). This box contains a list of all the servers in the system. You must add minimum two servers to a mirror location.

12. Select **Add**.

Mirror Node 1 is created.

13. Right-click the system name, and then select **Add Data Store**.

The **Add Data Store: Mirror Node 1** window appears.

14. Enter values as described in the following table.

Field	Description
DATA STORE NAME	Enter a unique name for the data store. A value is required. You can use all alphanumeric characters and special characters except / \ * ? < > You must provide the same name for the mirror setup in the IT network (mirror 2 in the example).
DESCRIPTION	Enter a description for the data store.
Set as default data store for the system	Select this check box if you want to set this data store as the default one. A default data store is the one that is considered if you do not specify a data store while adding a tag. You can set only one data store as default.

15. Select **Add**.

Mirror 1 is configured.

Set up Mirror 2:

16. On the mirror primary server in the IT network (Mirror Server 2 in the example), access Configuration Hub (*on page*).

17. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

A list of systems appears in the main section.

18. Expand Mirror Server 2.

A list of servers in the system appears.

19. Select **+**.

System	Historian Server						
Filter	Filter						
<div style="border: 1px solid #0070C0; padding: 5px;"> + </div>							
SERVERS							
Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...	Out Of
	Connected	43.3	0.5	0.45	0	0	0
	Not Connected	NA	NA	NA	NA	NA	NA

The **Add Server Machine: <system name>** window appears.

- Enter the host name or IP address of the mirror node in your organization's network (Mirror Node 2 in the example), and then select **Add**.

The distributed server is added to the system. A distributed location is added in the server.

- Right-click the system name, and then select **Browse Locations**.

System	Historian Server						
Filter	Filter						
<div style="border: 1px solid #0070C0; padding: 5px;"> + </div>							
SERVERS							
Machine Name	STATUS	Archive Compre...	Write Cache Hit ...	CONSUMPTION R...	Read Thread Usa...	Write Thread Usa...	Out Of
torsc-collectorsclient		5.5	0.5	0.33	0	0	
collectorsclien6		NA	NA	NA	NA	NA	NA

- View System Performance
- Set as Default System
- Add Server
- Browse Collectors
- Browse Tags
- Browse Locations
- Browse Clients
- Delete
- Browse Model

A list of distributed locations in the system appears.

- Select **Mirror Locations**.

A list of mirror locations in the system appears.

- In the upper-right corner of the main section, select **+**.

The **Add Mirror Location** window appears.

- Provide values as described in the following table.

Field	Description
MIRROR LOCATION NAME	Enter a name for the mirror location. A value is required and must be unique for the system.

Field	Description
SERVER MACHINES	Select the servers that you want to add to the mirror group (Mirror Server 2 and Mirror Node 2 in this example). This box contains a list of all the servers in the system. You must add minimum two servers to a mirror location.

25. Select **Add**.

Mirror Node 2 is created.

26. Right-click Mirror Node 2, and then select **Add Data Store**.

The **Add Data Store: Mirror Node 2** window appears.

27. Enter values as described in the following table.

Field	Description
DATA STORE NAME	Provide the same name that you provided while setting up mirror 1.
DESCRIPTION	Enter a description for the data store.
Set as default data store for the system	Select this check box if you want to set this data store as the default one. A default data store is the one that is considered if you do not specify a data store while adding a tag. You can set only one data store as default.

28. Select **Add**.

Mirror 2 is configured.

Set up Mirror of Mirror:

29. Access Configuration Hub in the primary server in the OT network (Mirror Server 2).

30. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

A list of systems appears in the main section.

31. Expand Mirror Server 1.

A list of servers in the system appears.

32. Select .

The **Add Server Machine: <system name>** window appears.

33. Enter the host name or IP address of the mirror server in the IT network (Mirror Server 2 in the example), select the **Set as Mirror of Mirror** check box, and then select **Add**.

The distributed server is added to the system. A distributed location is added in the server.

34. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Systems**.

A list of systems appears in the main section.

35. Expand Mirror Server 1.

A list of servers in the system appears. In the example, Mirror Server 1, Mirror Node 1, and Mirror Server 2 appear.

A mirror of mirror is configured with one primary node and one mirror node each in the OT and IT networks. As needed, you can add more mirror nodes in each network.

Upgrade the Historian Server

If any Historian applications or components are open, close them before upgrading the Historian server.

If you are upgrading from either Historian 6.0 Enterprise or previous releases of Historian 7.2 (including any of the service packs), both Client Manager and Configuration Manager services will be removed. However, this will have no impact on your data or use of Historian unless you intend to use a distributed system.

[Install the Historian server \(on page 44\).](#)

The Historian server is upgraded to the latest version.

About Historian Log Files

Historian creates the following types of log files:

- **The .IHA files:** These files contain data about archives. They are created by the Historian server after data collection begins. By default, these files are located in the `C:\Historian Data\Archives` folder.
- **The .IHC files:** These files contain data about Historian configuration. They are created by the Historian server. By default, these files are located in the `C:\Historian Data\Archives` folder.

There are two types of .IHC files:

- `*CentralConfig.ihc`: This is the master configuration file used by Configuration Manager.
- `*config.ihc`: This is used by the data archiver and is generated from `*CentralConfig.ihc`. This is to maintain consistency between Historian versions.
- **The .LOG files:** These files contain logging data (such as events, warnings, and errors). They are created by the archiver and the collectors. By default, they are located in the `C:\Historian Data\LogFiles` folder.
- **The .SHW files:** These files contain configuration data. They are created by the archiver and the collectors. By default, they are located in the `C:\Historian Data\LogFiles` folder.

FAQs on Installing Historian in a Distributed Environment

- What happens when a node that was down is up and running? Is the data written to one node synchronized with another?

There is no automatic synchronization. If a node is down, the information to be written is buffered by Client Manager, or if Client Manager is down, it is buffered by the collector. When the node is up and running, data is written to the data archiver.

- There is only one Configuration Manager on the primary node. Can I still configure if the primary node is down?

No. If the Configuration Manager is not available, you can read the configuration (because this information is stored in the collectors), but you cannot edit or modify the configuration.

- Is Configuration Manager a single point of failure?

Yes. If the primary node is down, you cannot edit the configuration. However, since information about the configuration is stored in the registry of each client, the information is still available as read-and-write-only when the primary node is down.

If the Configuration Manager service is down, you cannot query tags and data in a horizontally scalable system. However, you can query tags and data in the following scenarios:

- The Historian system contains only one node, which is installed as the primary mirror Historian server.
 - The Historian system contains only one mirror location, and there are no data stores in the distributed locations.
- What happens if a node crashes in the middle of a read/write request?

The operation continues to function in the same way as in prior releases. Client Manager holds a copy of the message request; therefore, once the node is up and running, the write operation is resumed. However, read requests will fail.

- The server where my primary node is installed is down. What is the expected behavior?

The Web Admin console and Trend Client will not be available; you can access tag configuration using Historian Administrator, but you will not be able to edit tag configuration. All other existing clients continue to work as expected, with the ability to collect and store data, search for tags, trend and report on tag information. A new user connection with default Historian server set to primary must connect to the primary node to get information about all the nodes before it gains the ability to automatically failover when the primary node is down.

- Client Manager on the primary node is down, but the server is running. What is the expected behavior?

The Web Admin console and Trend Client, along with all other existing clients, will work as expected with the ability to do configuration changes, collect and store data, search for tags, trend and report on tag information. A new user connection with default Historian server set to primary must connect to the primary node to get information about all the mirrors before it gains the ability to automatically failover when the primary node is down.

- One of the data archivers is down, but at least one is active. What is the expected behavior?

The system should continue to function as designed. The Web Admin console, Trend Client, Historian Administrator, as well as other clients continue to work as expected, with the ability to collect and store data, search for tags, trend and report on tag information.

- If there are calculated tags in a distributed environment, are the calculations done on all nodes?

Yes.

- Are Historian tag statistics created independently? Can they be different between different nodes?

Yes. These are queries, not tags, to a specific data archiver. As writes are independent, one data archiver may be ahead of another, so the statistics may vary slightly.

- How do we ensure that the data is consistent across data archivers?

Tag information is consistent; there is only one tag. The time stamp and value are sent to all the nodes.

- Are there specific log files that I should be looking for to help diagnose issues with failure modes?

No changes were made to the logs for data archiver; however, there are new log files for Client Manager and Configuration Manager.

- There are now two *.ihc files: *config.ihc and *CentralConfig.ihc. What is the difference between the two?

*CentralConfig.ihc is the master configuration file used by Configuration Manager. The *config.ihc file is used by the data archiver and is generated from *CentralConfig.ihc. This is to maintain consistency between Historian versions.

- With mirroring, is Microsoft Cluster Server still supported? What is the recommended approach?

Mirroring is offered as a substitute to Microsoft Cluster Server. Mirroring provides high availability for locations. Microsoft Cluster Server has not been tested or validated to date with Historian systems.

- Should I install SQL server in a distributed environment?

No. SQL server is only required for the Historian Alarms and Events database.

- How does mirroring work with Historian Alarms and Events SQL logging?

There is still an alarm archiver; it does not go through Client Manager, so it connects with SQL as earlier.

- How does Historian Alarms and Events fit with their syncing?

There is one database, so everyone talks to the same SQL database. You can cluster the database, but that is separate from mirroring.

- How does mirroring work in a workgroup environment or non-domain?

Mirroring is not supported in Workgroups.

- Are there any issues when making changes in Historian Administrator and a mirrored system?

You must establish a mirror using the Historian Configuration Hub, but compatibility with all APIs has been maintained. Therefore, you can make tag changes in either the Web Admin or the VB Windows Admin, and those changes will show up in both Admins.

- Are there any plans to add more than three mirrors?

No performance benefits have been seen beyond three mirrors.

- Do redundant collectors behave differently in a distributed environment?

No.

- Are there any conflicts when using port 14000 for Historian to Historian communications (for example, Site to Corporate)?

No. Client Manager is now on port 14000, data archiver is on port 14001, and Configuration Manager is on port 14002.

- If load balancing uses round robin reads, does the cache need to be loaded separately on both machines, and will it decrease performance?

It does require more memory. Client Manager decides where to send the messages, and it knows about the configuration. There is some overhead, but it is overcome by having multiple data archivers to service multiple requests. That is why there is a 1.5X improvement with two mirrors, instead of 2X.

- Are there any additional considerations if a distributed system is used with other GE applications such as Workflow or Plant Applications?

No. It still looks like one Historian to other applications.

- Is the store-and-forward feature also used in a distributed environment?

Yes. This is a feature of the collector. Once the message is sent to Client Manager, it is done. If the Client Manager cannot reach one of the data archivers, it buffers the request until the archiver is available.

- In a distributed environment, do existing queries and reports work the same?

Yes. Everything works the same as it did before. It sees it as a single Historian and communicates over the same ports through the same API.

- Does the Historian OPC Classic HDA server still work in a distributed environment?

Yes.

- If data is being written to two data archivers, does this double the traffic from the collector?

No. It does not double traffic from the collector; it sends a single message to Client Manager. The traffic is doubled between the Client Manager and the two data archivers.

Change the Proficy Authentication Server

[Install Web-based Clients \(on page 104\)](#), specifying the details of the new Proficy Authentication server.

The Historian server and Web-based Clients must always point to the same Proficy Authentication server. Only then you can access Web-based Clients (such as Configuration Hub, Trend Client, the Web Admin console, and REST APIs). Therefore, if you have changed the Proficy Authentication server used by Web-based Clients, the Historian server must point to the same Proficy Authentication server.

This topic describes how to update the Proficy Authentication server details for the Historian server without the need to reinstall it.

1. Access the `UAAConfiguration.exe` file. By default, it is located at `C:\Program Files\Proficy\Proficy Historian\x64\Server`.

The **Proficy Authentication Configuration tool** window appears, displaying the Proficy Authentication server name and port number that you specified while installing the Historian server.

2. In the **Proficy Authentication server name** and **Public https port** fields, provide the values of the Proficy Authentication server used by Web-based Clients.

3. Select **Test**.

The test results appear. Only if the connection test is successful, you can modify the details.

4. Select **Configure**.

The Proficy Authentication server and port number details are updated for the Historian server.

The changes are reflected as soon as you refresh the browser in which you have opened any of the Web-based Clients components (such as Configuration Hub, the Web Admin console, Trend Client).

If testing the connection fails, try these steps:

- Verify that you can ping the Proficy Authentication server. If you cannot ping the Proficy Authentication server, add the IP address and the server name in the `hosts` file located in `C:\Windows\System32\drivers\etc`.
- Ensure that the following services are running on the Proficy Authentication server machine:
 - GE Operations Hub Httpd Reverse Proxy
 - GE Operations Hub Proficy Authentication Tomcat Web Server
- Verify that the Proficy Authentication server details provided during Web-based Clients installation match the ones you have specified in the Proficy Authentication Configuration tool.

Alarms and Events

Install Alarms and Events

- You must install Historian Alarms and Events on the same machine as the data archiver.
- If you have chosen to connect Historian to a remote SQL server, the following conditions must be satisfied:
 - The Historian Alarm Archiver service must be run on a user account that has privileges to log in to the SQL server using Windows authentication.
 - The default backup path, which you can set on the Archive page, must be a shared directory that is accessible to both the Historian Data Archiver and the remote SQL server. It is recommended that this shared directory be placed on the same computer as the Historian Data Archiver service.

1. Run the `InstallLauncher.exe` file.

2. Select **Install Alarms and Events**.

The **Alarms and Events Archiver** page appears.

Proficy Historian Setup Maintenance

Alarm and Event Archiver
Specify SQL server database details for archiver.

The Alarm and Event archiver require access to SQL Server.

Server Name

Database Name

Use Windows Authentication

Admin User Password

InstallShield

< Back Next > Exit

3. If needed, change the values in the **Server Name** and **Database Name** fields to provide the name of the SQL server and the name of the database where the alarms and events data is archived.
4. If you want to use the SQL server credentials, clear the **Use Windows Authentication** check box, and then enter the SQL server login credentials in the **Admin User** and **Password** fields. If you want to use Windows authentication, select the **Use Windows Authentication** check box. When you do so, the **Admin User** and **Password** fields are disabled.
5. Select **Next**.
6. When prompted to restart your system, select **Yes**.

Historian Alarms and Events is installed in the following folder: *<installation drive>*:
 \Program Files\Proficy\Proficy Historian\x86\Server, and the following registry path is created: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ Intellution, Inc.
 \iHistorian\Services\AlarmArchiver

7. To verify that the Alarms service has started, access the **Services** window, and check the status of the Historian Alarm Archiver service.

If the **Startup Type** field is set to **Automatic**, the service is started automatically when the system is started or restarted.

Upgrade Alarms and Events

- If Alarms and Events were installed prior to Historian 7.0, you must install them separately.
- If you want to upgrade from Historian 4.5, since the database schema are different, if you select the same database name that is pre-populated by default, you will get an error message: `Later or Higher version of Alarms and Events database is already installed. Hence, you cannot proceed further.` You need to enter a different database name and then proceed with the upgrade.

[Install Alarms and Events \(on page 90\).](#)

Alarms and Events are upgraded to the latest version.

About Installing Historian Data Collectors

When you install collectors, the required binaries are downloaded. In addition, if iFIX/CIMPLICITY are installed on the same machine as the collectors, instances of the following collectors are created:

- The iFIX collector
- The iFIX Alarms & Events collector
- The OPC Classic Data Access collector for CIMPLICITY
- The OPC Classic Alarms and Events collector for CIMPLICITY

If an iFIX collector instance created in version 9.0 exists, after you upgrade collectors, another instance of the iFIX collector is created. Because of this, the Remote Collector Manager (RCM) will not work correctly. Therefore, if you want to use RCM, you must delete one of the instances. If needed, you can manually create another instance of the iFIX collector using Configuration Hub or the RemoteCollectorConfigurator utility. This is applicable to the iFIX Alarms and Events collector as well.



Note:

If you want to upgrade collectors earlier than version 7.1, additional registries that you create manually are deleted. Therefore, we recommend that you back them up, uninstall the collectors, and then install the latest version.

Install Collectors Using the Installer

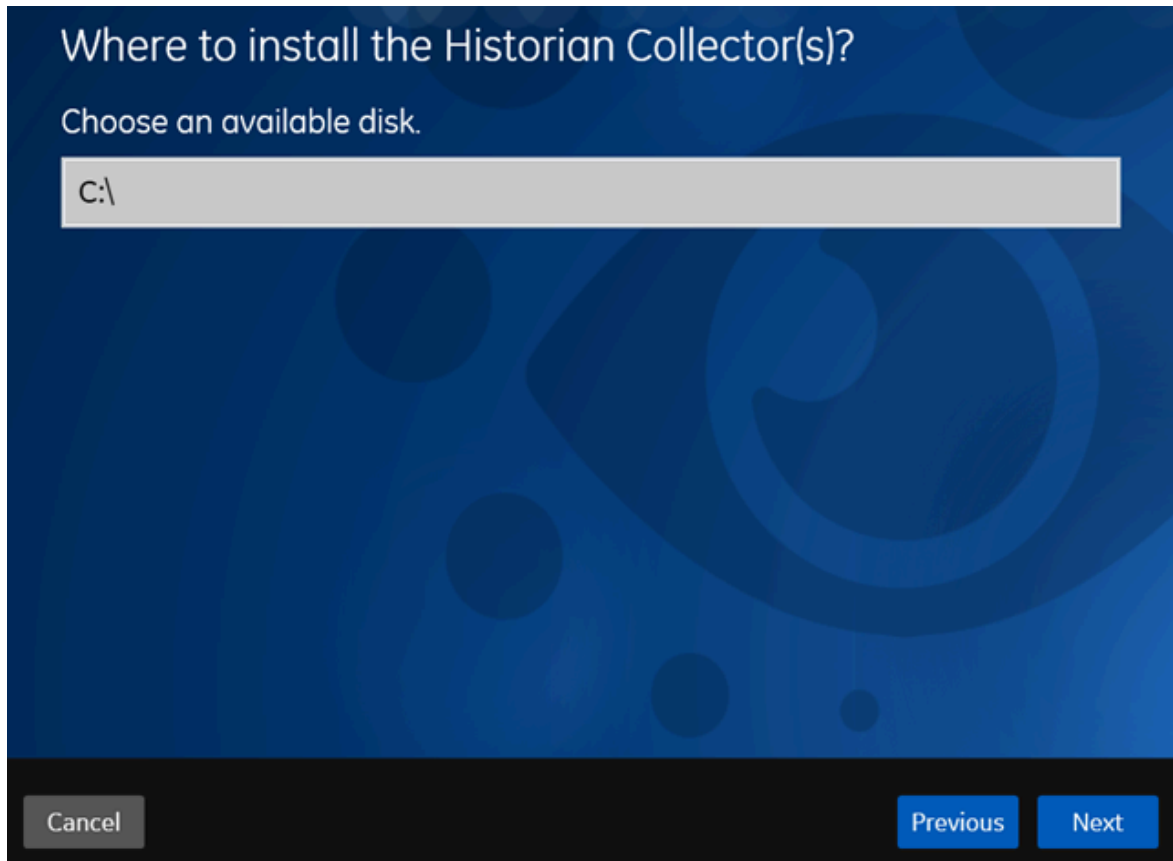
After you install collectors, the following artefacts will be available:

- **Executable files:** These files are required to add a collector instance.
- **Instances of the following collectors:**
 - The iFIX collector
 - The iFIX Alarms & Events collector
 - The OPC Classic Data Access collector for CIMPLICITY
 - The OPC Classic Alarms and Events collector for CIMPLICITY

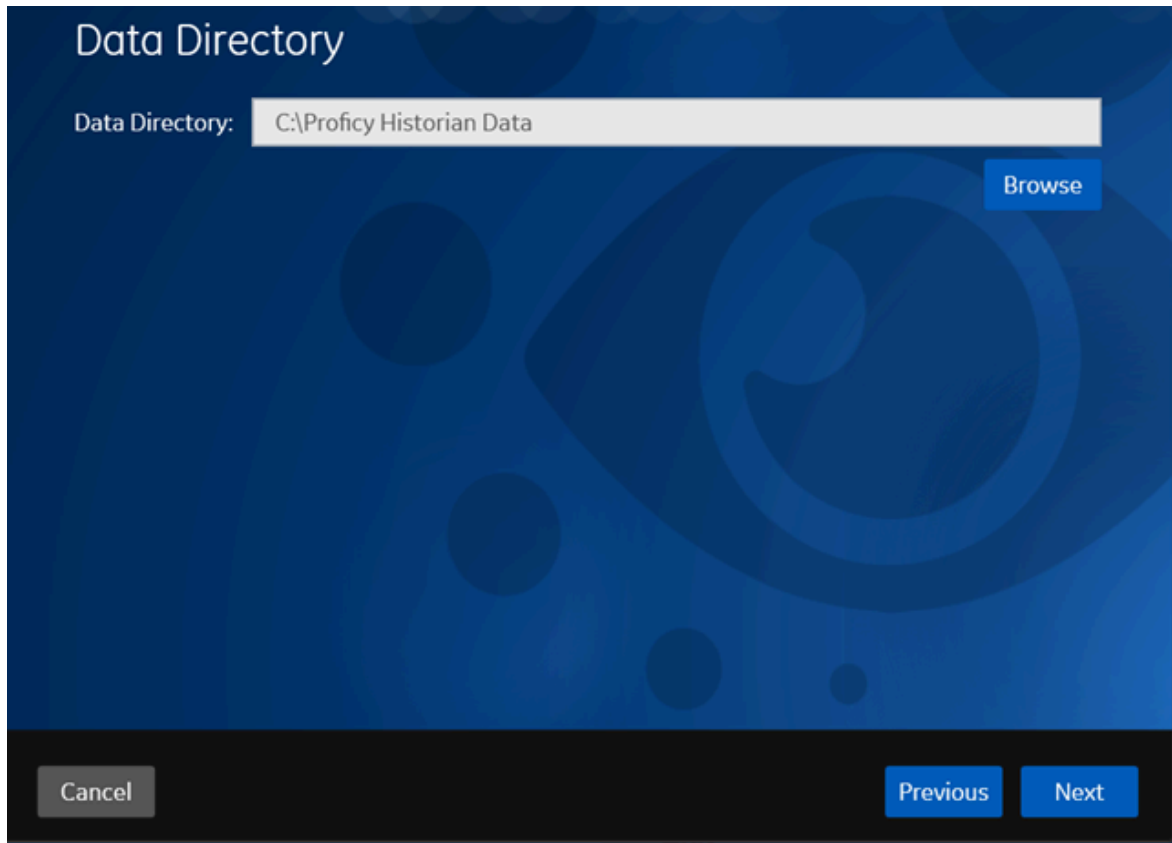
These instances will be created only if iFIX and/or CIMPLICITY are installed on the same machine as the collectors.

- **The Remote Collector Management agent:** Provides the ability to manage collectors remotely.

1. Run the `InstallLauncher.exe` file.
2. Select **Install Collectors**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box, and then select **Next**.
The default installation drive appears.



5. If needed, modify the installation drive, and then select **Next**.
The data directory page appears.



6. If needed, change the folder for storing the collector log files, and then select **Next**.
The destination Historian server page appears.

Historian Server Details

Provide a valid windows user of the default Historian server to which the Remote Collector Manager will connect.

Historian Server:

User Name:

Password:

Confirm Password:

Note: If the Historian server and collectors are installed on the same machine, you need not provide the details; by default, the machine name of the local Historian server is considered. If, however, they are installed on different machines, you must provide the credentials of the Historian server user. If the password changes, you must reinstall Remote Management Agents to reset the password.

7. Provide the credentials of the Windows user account of the destination Historian server to which you want Remote Management Agent to connect.

These details are required for Remote Collector Manager to connect to Historian to manage the collectors remotely. If are installing collectors on same machine as the Historian server, and if strict collector authentication is disabled, you need not provide these details; by default, the machine name of the local Historian server is considered. If, however, they are installed on different machines, or if strict collector authentication is enabled, you must provide the credentials of the Historian server user.

8. Select **Next**.

A message appears, stating that you are ready to install collectors.

9. Select **Install**.

The installation begins.

10. When you are prompted to reboot your system, select **Yes**.

The collector executable files are installed in the following folder: `<installation drive>:\Program Files (x86)\GE Digital\<collector name>`. The iFIX collectors are installed in the following folder: `C:\Program Files\GE\iFIX`. The following registry paths are created:

- `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ GE Digital\iHistorian\Services\<collector type>`
- `HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\iHistorian\Services\<collector type>`

In addition, if iFIX and/or CIMPLICITY are installed on the same machine as the collectors, instances of the following collectors are created:

- The iFIX collector
- The iFIX Alarms & Events collector
- The OPC Classic Data Access collector for CIMPLICITY
- The OPC Classic Alarms and Events collector for CIMPLICITY

Installing a Collector at a Command Prompt

After you install collectors and Remote Management Agent, the following artefacts will be available:

- **Executable files:** These files are required to add a collector instance.
- **Instances of the following collectors:**
 - The iFIX collector
 - The iFIX Alarms & Events collector
 - The OPC Classic Data Access collector for CIMPLICITY
 - The OPC Classic Alarms and Events collector for CIMPLICITY

These instances will be created only if iFIX and/or CIMPLICITY are installed on the same machine as the collectors.

- **The Remote Collector Management agent:** Provides the ability to manage collectors remotely.

Using Configuration Hub, you will then add a collector instance and begin using the collector.

This topic describes how to install collectors at a command prompt. You can also [install them using the installer \(on page 93\)](#).

1. Navigate to the `Collectors` folder in the installation folder.
2. At a command prompt, enter:

```
Collectors_Install.exe -s RootDrive=<value> DestinationServerName=<value> DataPath=<value>
UserName1=<value> Password=<value>
```

Parameter	Description	Default Value
RootDrive	The installation drive for the collectors.	C:\

Parameter	Description	Default Value
DataPath	The folder for storing the collector log files.	C:\Proficiency Historian Data
DestinationServerName	<p>The host name of the destination Historian server to which you want collectors to send data.</p> <p>This is required for Remote Collector Manager to connect to Historian to manage the collectors remotely. If you are installing collectors on the same machine as the Historian server, and if strict collector authentication is disabled, you need not provide the server name; by default, the machine name of the local Historian server is considered. If, however, they are installed on different machines, or if strict collector authentication is enabled, you must provide the credentials of the Historian server user.</p>	local host name
UserName1	The username of the Windows user of the destination Historian server. A value is required only if the destination Historian server and collectors are on different machines.	
Password	The password of the Windows user of the destination Historian server. A value is required only if the destination Historian	

Parameter	Description	Default Value
	an server and collectors are on different machines.	

For example: `Collectors_Install.exe -s RootDrive=C:\ DestinationServerName=myservername
DataPath=C:\Proficy Historian Data UserName=user123 Password=xyz123`

- Restart the machine. If you uninstall a collector or install another one before restarting the machine, an error may occur.

The collector executable files are installed. In addition, if iFIX and/or CIMPLICITY are installed on the same machine as the collectors, instances of the following collectors are created:

- The iFIX collector
 - The iFIX Alarms & Events collector
 - The OPC Classic Data Access collector for CIMPLICITY
 - The OPC Classic Alarms and Events collector for CIMPLICITY
1. Ensure that the Windows user that you have specified while installing collectors is added to the iH Security Admins and iH Collector Admins groups.
 2. [Enable trust for a client certificate for Configuration Hub.](#)
 3. [Enable trust for a self-signed certificate on Chrome \(on page 38\).](#)
 4. [Import an issuer certificate.](#)

You are now ready to use Configuration Hub. To add and manage collector instances, you can use Configuration Hub or Remote Collector Management. For instructions specific to setting up the iFIX collector and the iFIX Alarms and Events collector, refer to [Working with iFIX Collectors](#).

Upgrade Collectors

- If an iFIX collector instance created in version 9.0 exists, after you upgrade collectors, another instance of the iFIX collector is created. Because of this, the Remote Collector Manager (RCM) will not work correctly. Therefore, if you want to use RCM, you must delete one of the instances. If needed, you can manually create another instance of the iFIX collector using Configuration Hub or the RemoteCollectorConfigurator utility. This is applicable to the iFIX Alarms and Events collector as well.
- For collectors earlier than version 7.1, additional registries that you create manually are deleted. Therefore, we recommend that you back them up, uninstall the collectors, and then install the latest version.

[Install the collectors \(on page 92\)](#).

The collectors are upgraded to the latest version.

Client Tools

Install Client Tools

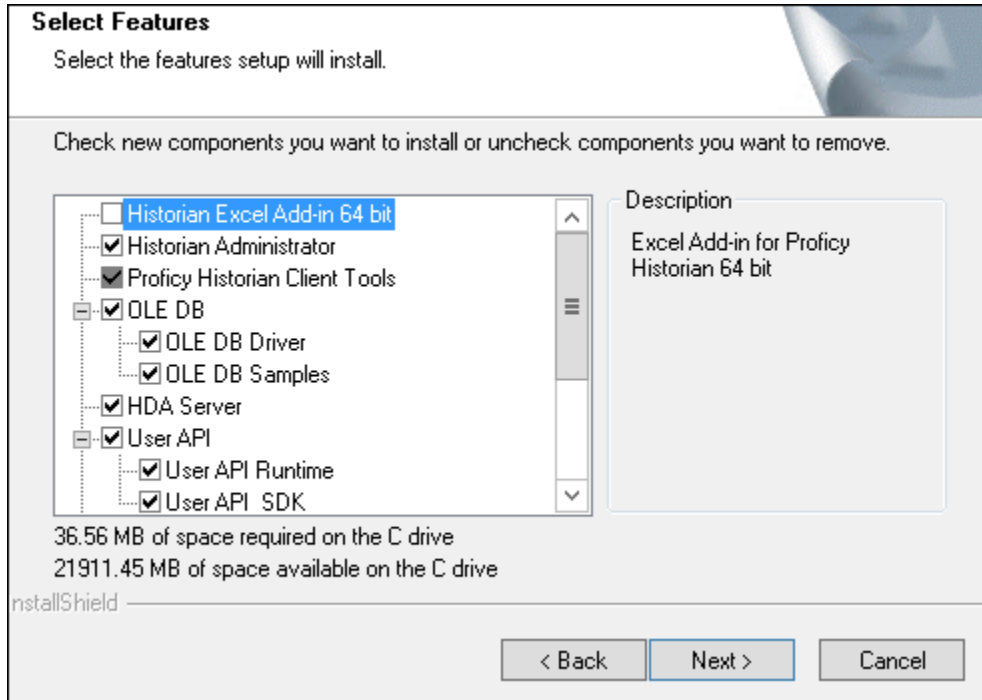
When you install Client Tools, the following components are installed by default:

- Client Tools
- Historian Administrator
- OLE DB provider (driver and samples)
- The OPC Classic HDA server
- User API and SDK
- Historian Client Access API
- Collector Toolkit

This topic describes how to install Client Tools using the installer. You can also [install it at a command prompt \(on page 103\)](#).

1. Run the `InstallLauncher.exe` file.
2. Select **Install Client Tools**.

The **Select Features** page appears, displaying a list of components that you can install with Client Tools.



By default, the check boxes for components such as **Historian Administrator**, **HDA Server**, **OLE DB**, and **User API and SDK** are selected. If you do not want to install them at this time, clear the check boxes. You cannot, however, clear the **Proficy Historian Client Tools** check box.

 **Important:**

If you are reinstalling, you must select all of the previously installed components. If you do not do so, the component will be uninstalled.

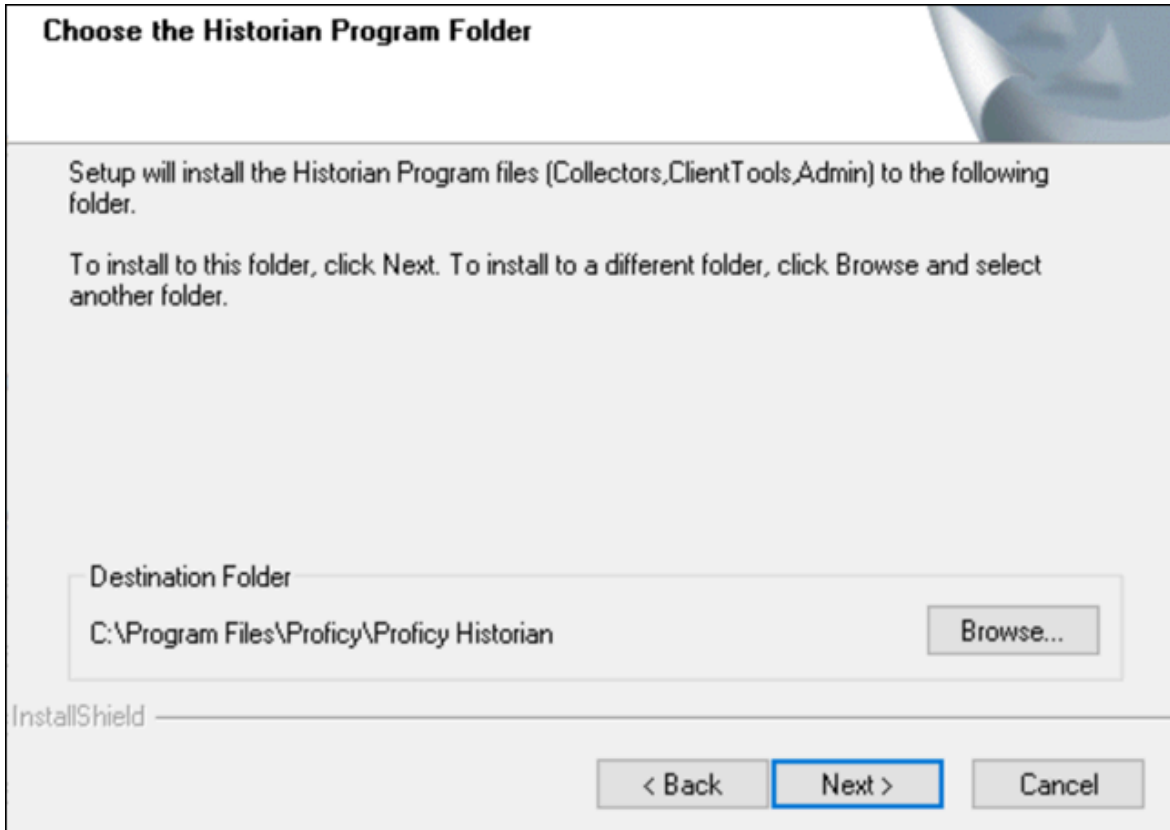
By default, the **Historian Excel Add-in 64-bit** check box is cleared. If you want to install Excel Add-In along with Client Tools installation, select the check box.

 **Note:**

If using certain versions of Windows (like Windows 10 or Windows 2019), you may receive an error message while installing Excel Add-In, stating that some of the DLL files are not registered. You can ignore these messages.

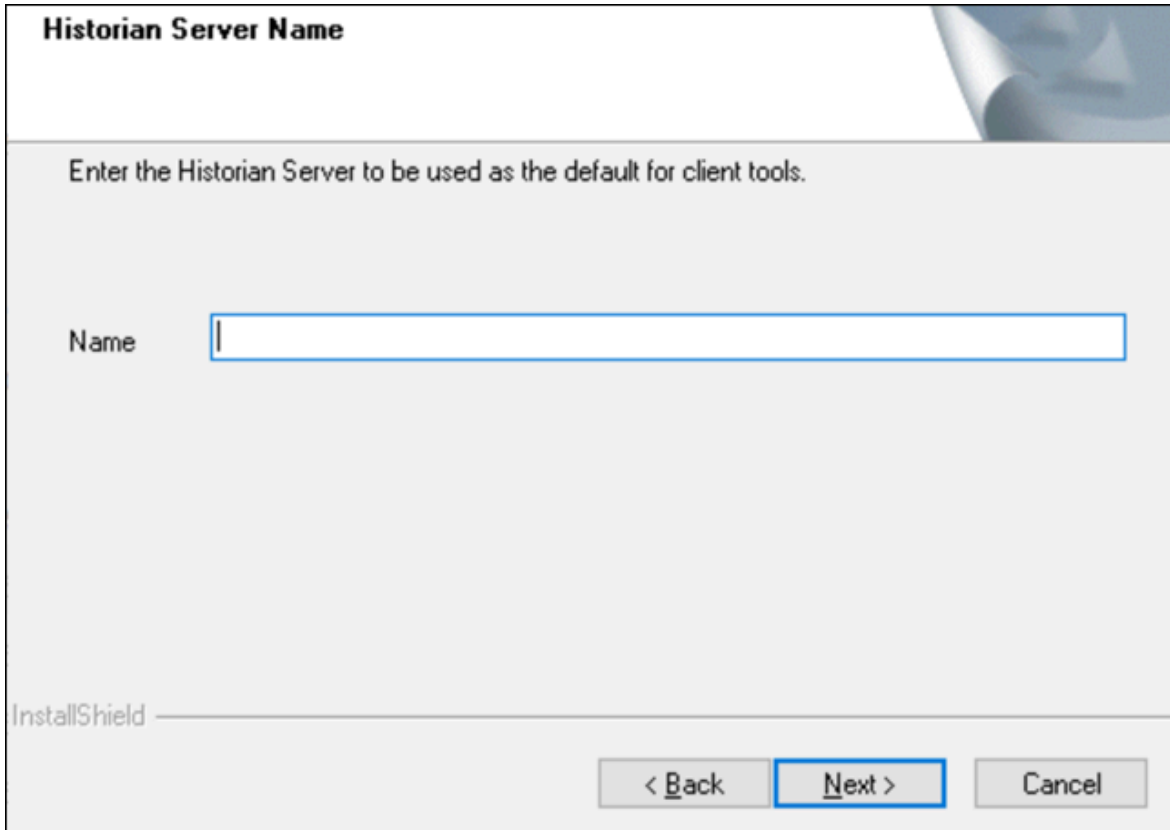
3. Select **Next**.

The **Choose the Historian Program Folder** page appears.



4. As needed, change the destination folder of Client Tools, or leave the default folder, and then select **Next**.

The **Historian Server Name** page appears.



Historian Server Name

Enter the Historian Server to be used as the default for client tools.

Name

InstallShield

< Back Next > Cancel

5. Enter the IP address or the host name of the Historian server that you want to use with Client Tools, and then select **Next**.
6. When you are asked to reboot your system, select **Yes**.

Client Tools, along with the selected components, are installed in the following folder: *<installation drive>:\Program Files\Proficy\Proficy Historian\x86\<tool name>*. If you have selected HDA Server, Microsoft .NET Framework 4.5 and the OPC Core Components 3.00 redistributable are installed as well.

Install Client Tools at a Command Prompt

1. If you want to install Excel Add-In for Historian, install one of the following 32-bit or 64-bit Microsoft® Excel® applications:
 - Microsoft® Excel® 2019
 - Microsoft® Excel® 2016
 - Microsoft® Excel® 2013
 - Microsoft® Excel® 2010

2. [Install Client Tools using the installer \(on page 100\)](#) on a machine. When you do so, a template file named `setup.iss` is created at `C:\Windows`. This file stores the installation options that you have provided. You can then use this template to install Client Tools at a command prompt on other machines.

When you install Client Tools, the following components are installed by default:

- Client Tools
- Historian Administrator
- OLE DB driver and samples
- The OPC Classic HDA server
- User API and SDK
- Historian Client Access API
- Collector Toolkit

1. Copy the `setup.iss` file to the machine on which you want to install Client Tools at a command prompt.
2. In the folder in which you have copied the file, run the following command: `setup.exe /s /sms`
The installer runs through the installation steps.



Note:

If using certain versions of Windows (like Windows 10 or Windows 2019), you may receive an error message, stating that some of the DLL files are not registered. You can ignore these messages.

3. When prompted to reboot your system, select **Yes**.

Client Tools are installed.

If you have installed Excel Add-in, [activate it \(on page 147\)](#).

About Installing Web-based Clients

Using Web-based Clients, you can configure and manage Historian systems and their components using a browser.

When you install Web-based Clients, you can install the following components:

- Configuration Hub: Allows you to manage Historian systems and its components. You can set up stand-alone as well as horizontally scalable systems. You can also add collector instances and manage them.
- Trend Client: Provides access to process and equipment data, allowing you to quickly troubleshoot and make improvements, leading to time and cost savings through the use of trend charts and current value tables.
- The Web Admin console: Allows you to monitor, supervise, archive, retrieve, and control data gathered from Historian systems.
- The Proficy Authentication service (optional): Provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2. You can install Proficy Authentication and Configuration Hub, or you can point to existing Proficy Authentication and Configuration Hub instances.
- Rest APIs: Allow you to query data from a Historian server.

You can install Web-based Clients [using a GUI-based installer \(on page 109\)](#) or [at a command prompt \(on page 125\)](#).

**Important:**

When you install Web-based Clients:

- If you want to reinstall the same version of Web-based Clients, you must uninstall and then install Web-based Clients.
- If, even after installing Web-based Clients, you cannot access a web component, start the GE Operations Hub Httpd Reverse Proxy and the Data Archiver services.

Set Up High Availability of Web-based Clients

1. Ensure that your network is enabled for multicast traffic. To do so, run the following command:

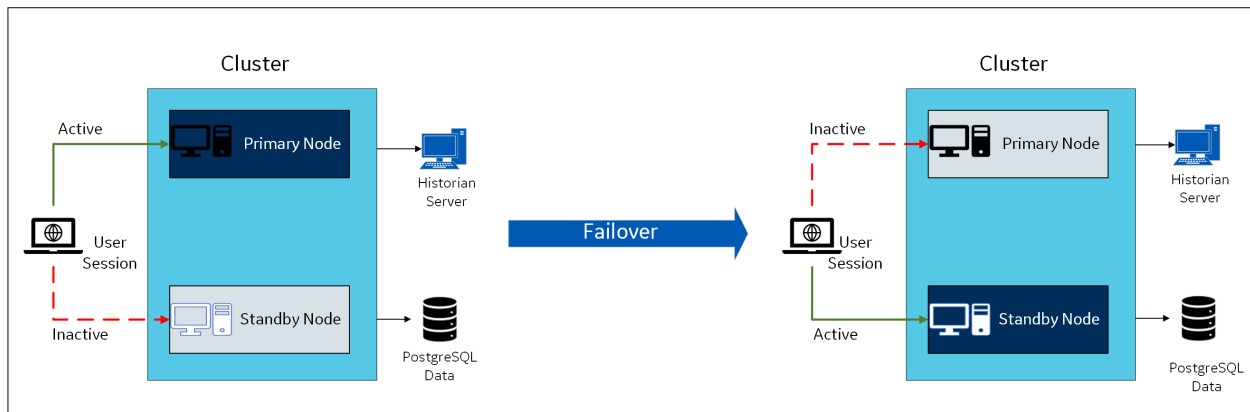
```
netsh <interface name> <IP address> show joins
```

A list of IP multicast groups that have been joined through an interface appears. If you do not specify an interface name, a list of multicast groups for all interfaces appears.

2. Create a shared drive on your network that all the nodes in the cluster can access, and create a folder in that drive.
3. On each node that you want to add to the cluster:

- a. [Install the Failover Clustering feature.](#)
- b. If you want to use an existing Proficy Authentication instance, ensure that all the cluster nodes point to the same Proficy Authentication instance. Note that for *all* the cluster nodes, the Proficy Authentication credentials of the node on which you installed Proficy Authentication *last* will be considered.

In a cluster environment, multiple servers are installed, which share the same data. Each of these servers is called a node. One of them acts as the primary node, while the others are standby nodes. If the primary node is down, one of the standby nodes is used.



When you install Web-based Clients in a cluster environment, the web servers are added to the cluster. You can then achieve high availability of connection between the Historian server and the client applications.

For example, if Configuration Hub on the primary node is unable to connect to the Historian server, the user session on the standby node is activated. Therefore, you will still be able to connect to the Historian server using Configuration Hub installed on the standby node.

The following services are shared between the primary and standby nodes in a cluster:

- Historian Indexing Service
- GE Historian PostgreSQL Database

Historian works with Microsoft Failover Cluster Manager to ensure high availability of Web-based Clients. Using Failover Cluster Manager, you must add these services to the cluster.

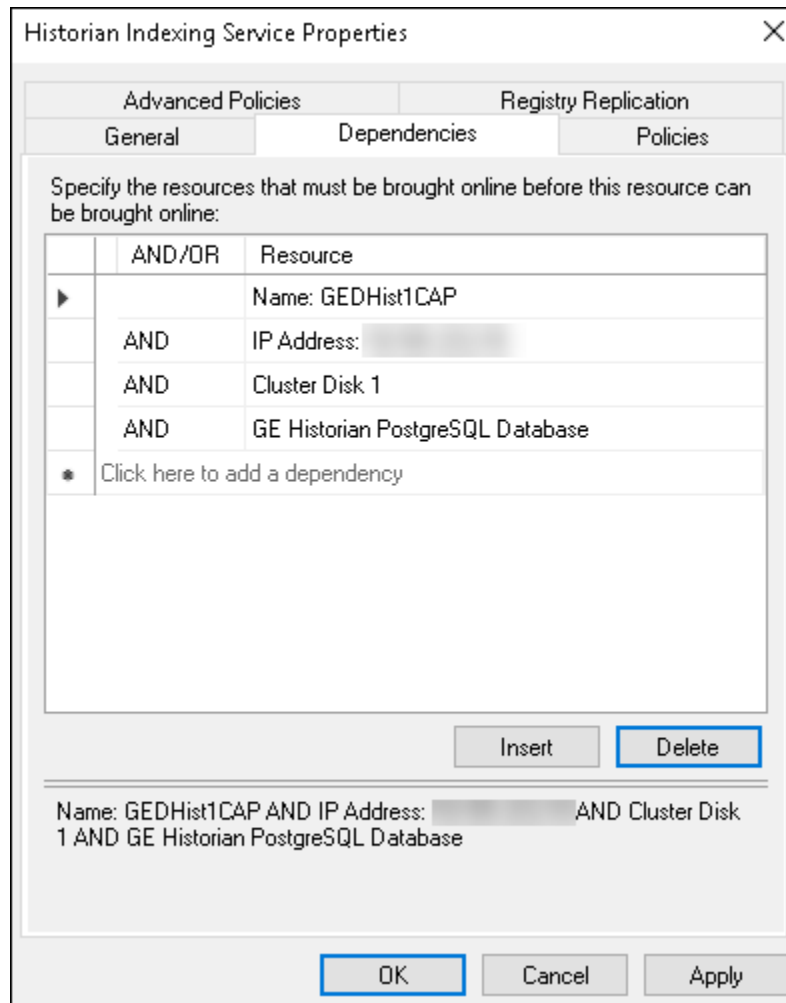
1. Access the primary node of the cluster.
2. [Create a failover cluster.](#)
3. [Add a storage to the failover cluster.](#)
4. Select **Roles > Create Empty Role.**

A role is created.

5. Add a client access point to the role:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Resource > Client Access Point**.
 - c. Follow the on-screen instructions to add a client access point to the role.
6. Add a storage to the role:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Storage**.
 - c. Follow the on-screen instructions to add the storage that you have created in step 3. You can use a storage only once.
7. Add resources to the role:
 - a. Select the role.
 - b. In the **Actions** section, select **Add Resource > Generic Service**.
The **New Resource Wizard** window appears.
 - c. In the list of resources, select **Historian Indexing Service**, and then follow the on-screen instructions to add the service.
8. Perform the previous step to add the GE Historian PostgreSQL Database resource as well.
9. Add the following dependencies for each of these resources:
 - a. Double-click a resource.
The **<resource name> Properties** window appears.
 - b. Select **Dependencies**.
 - c. Select **Insert**, and add dependencies for each resource as described in the following table, using the AND operation.

Resource Name	Dependencies
GE Historian PostgreSQL Database	<ul style="list-style-type: none"> ▪ IP Address ▪ Storage ▪ The network name
Historian Indexing Service	<ul style="list-style-type: none"> ▪ IP Address ▪ Storage ▪ The network name ▪ GE Historian PostgreSQL Database

For example, the following image shows the dependencies added to Historian Indexing Service:



10. Select the role, and then in the **Actions** section, select **Start Role**.

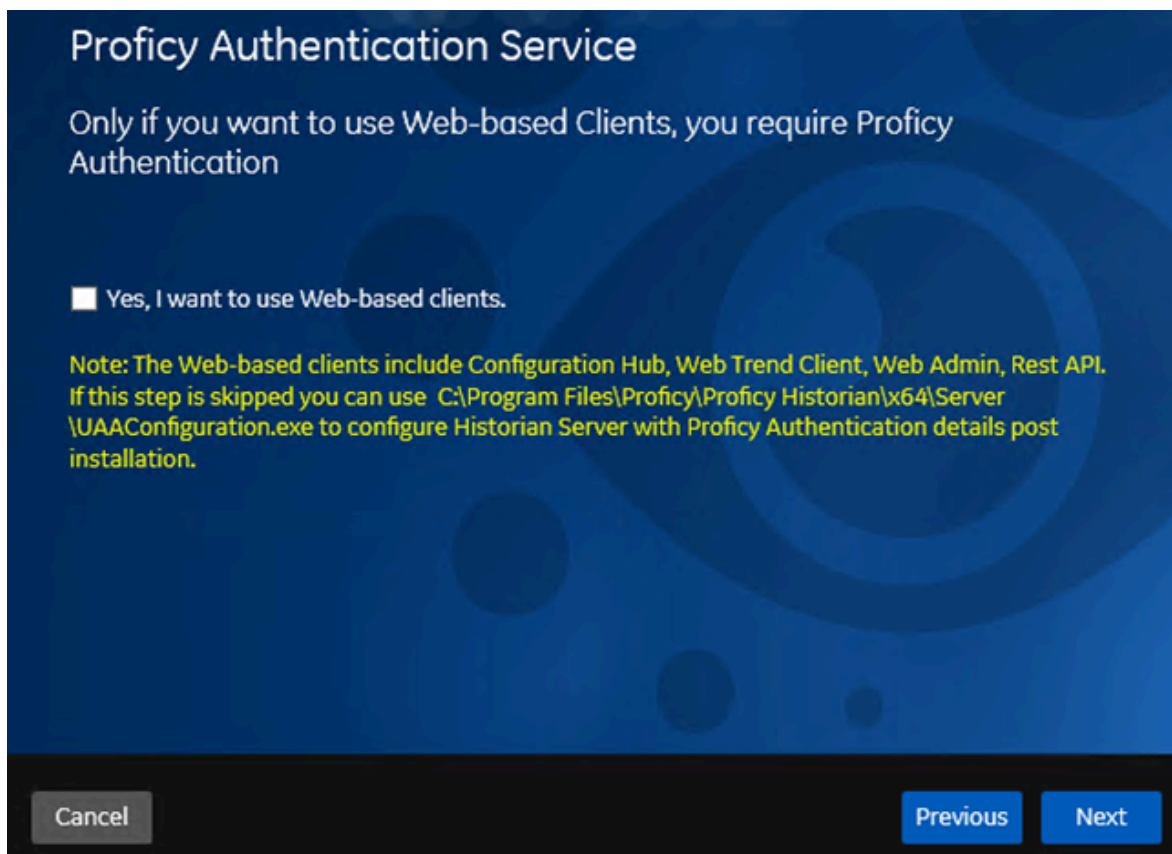
When you later install Web-based Clients and provide the cluster details, Web-based Clients will be part of the cluster, thus achieving high availability.

1. [Install Web-based Clients \(on page 109\)](#). During the installation, select the **Cluster Node** check box, and provide the details.
2. [Import the Proficy Authentication certificate \(on page 136\)](#) into all the cluster nodes. Copy the certificate in the following path from any node in the cluster and paste it in the same folder in all the other nodes: C:\Program Files\GE\Operations Hub\httpd\conf\cert
3. Restart the following services on all the cluster nodes:

- Historian Indexing Service
 - GE Historian PostgreSQL Database
4. On the machine on which you have installed the Historian server, update the URI of the following registry key to point to the cluster FQDN: `HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc\iHistorian\SecurityProvider\OAuth2`

Install Web-Based Clients Using the Installer

1. [Install the Historian server \(on page 46\)](#). During the installation, in the **Proficy Authentication** page, select the **Yes, I want to use Web-based Clients** check box, and provide the Proficy Authentication server name and port number.



2. If you want to use Web-based Clients in a cluster environment, ensure that your network is enabled for multicast traffic, and [set up high availability](#) on each node in the cluster.

This topic describes how to install Web-based Clients using a GUI-based installer.

<https://www.youtube.com/embed/KmIREuZVQW4>

You can also [install Web-based Clients using the command line](#).

During the installation, you can choose to use Web-based Clients in a cluster environment, thus ensuring high availability of connection to the Historian server using the client applications.

1. Run the `InstallLauncher.exe` file.
2. Select **Install Web-based Clients**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box, and then select **Next**.
The **TCP port assignments** page appears.

Field	Description
Public https port:	443
Proficy Authentication http port:	9480
Proficy Authentication database port:	9432
Historian http port:	8070
Historian database port:	8432
Proficy Authentication ldp config service port:	7010
Proficy Authentication security app port:	7011

Note: Public HTTPS port cannot be changed as the Proficy Authentication server already exists on the local machine. It may have been installed with previous versions of Historian Web-based Clients or with other products such as Operations Hub or common components.

5. As needed, change the values for TCP port assignments as described in the following table, and then select **Next**.

Field	Description
Public https port	Port for https protocol communication used by Web-based Clients (through a firewall). The default value is 443. Ensure that this port number matches the one you specify while installing the Historian server. In addition:

Field	Description
	<ul style="list-style-type: none"> ◦ If you will install Operations Hub later on the same machine, the value that you provide in this field is populated while installing Operations Hub. ◦ If you have already installed Operations Hub on the same machine, this field is disabled and populated with the value you have provided while installing Operations Hub.
Proficy Authentication http port	Port for http protocol communication used by the Proficy Authentication service. The default value is 9480.
Proficy Authentication database port	Port for the Proficy Authentication database. The default value is 9432.
Historian http port	Port for the http protocol communication used by Web-based Clients. The default value is 8070.
Historian database port	Port for the PostgreSQL Historian database. The default value is 8432.
Proficy Authentication Idp config service port	Port for the Configuration Hub identity provider service. The default value is 7010.
Proficy Authentication security app port	Port for the Proficy Authentication Configuration tool. The default value is 7011.

The **Fully Qualified Domain Name(s)** page appears.

- If you will install Operations Hub later on the same machine, the value that you provide in the **FQDNs** field is populated while installing Operations Hub.
- If you have already installed Operations Hub on the same machine, the **FQDNs** field is disabled and populated with the value you have provided while installing Operations Hub.

Fully Qualified Domain Name(s).

To allow users to access Historian web applications remotely using fully qualified domain names (FQDN), please list one or more here, separated by semicolons. Otherwise, you may leave this blank.

FQDNs:

6. In the **FDQNs** field, enter the fully qualified domain names, and then select **Next**.

This enables you to access Historian web applications remotely. You can use it to access the Web Admin console using alias names. Enter the values separated by commas.

To access the Web Admin console using any of the following URLs, enter

`Test.abc.ge.com,localhost,127.0.0.1,aliasName`

- [https:// Test.abc.ge.com /historian-visualization/hwa](https://Test.abc.ge.com/historian-visualization/hwa)
- [https:// 127.0.0.1 /historian-visualization/hwa](https://127.0.0.1/historian-visualization/hwa)
- [https:// aliasName /historian-visualization/hwa](https://aliasName/historian-visualization/hwa)
- [https:// localhost /historian-visualization/hwa](https://localhost/historian-visualization/hwa)

! **Important:**

- Do not enter a space between the values.
- You must add the IP address and alias name in the `hosts` file located at `C:\Windows\System32\drivers\etc`. The IP address that you add must be a static or fixed IP address.

Format: `<IP address> <alias name>`



Example: 1.2.3.4 myservername

- FQDN is not supported for Configuration Hub.

The **Cluster Configuration** page appears.

Cluster Configuration

Want to configure this as Cluster Node?

Note: Select above check box if you want to install Web-based Clients in a cluster environment for achieving high availability.

Cancel Previous Next

If, however, you are upgrading Web-based Clients, this page does not appear. In that case, skip the next step.

7. If you want high availability of Web-based Clients, select the **Cluster Node** check box, and enter values as described in the following table.

Field	Description
Historian Database Folder	Provide the database folder in the shared drive that you have created. The default value is C:\ProgramData\GE\OperationsHub. You <i>must</i> change this value.

Field	Description
Cluster FQDN	Enter the client access point of the role for which you have added the resources while setting up high availability (on page 105) .
Multicast Address	If needed, modify the common IP address that all the nodes in the cluster can use. Enter a value between 224.0.0.0 and 239.255.255.255 (or a hostname whose IP address falls in this range). The default value is 228.0.0.4.
Historian Cluster Membership Port	If needed, modify the common port number that all the nodes in the cluster can use. The default value is 45564. This port number, in conjunction with the multicast address, is used to create the cluster.
Historian Cluster Receiver Port	If needed, modify the multicast port number that you want to use for incoming Historian data. The default value is 4000.

8. Select **Next**.

The **Proficy Authentication** page appears, allowing you to choose whether you want to install Proficy Authentication along with Web-based Clients installation or use an existing Proficy Authentication.

Proficy Authentication

Use Existing Proficy Authentication:

Admin client Secret:

Re-enter Secret:

Note: The default Client ID is <admin>. As the admin Client is highly privileged, choose a strong secret and safekeep it.

Note: The username to login to Historian web-based clients is <[redacted].admin>. This is case-sensitive.

- If you want to install Proficy Authentication, clear the **Use External Proficy Authentication** check box. If you want to include Proficy Authentication in the cluster, you must install Proficy Authentication locally on each cluster node.
 - If you want to use an existing Proficy Authentication server, select the **Use External Proficy Authentication** check box. Proficy Authentication is detected if you installed it using a unified installer or Operations Hub, or if Historian uses Proficy Authentication installed remotely from an earlier version.
9. If you want to install Proficy Authentication, enter the **Admin client secret**, re-enter the secret, and then select **Next**.

The admin client secret must satisfy the following conditions:

- Must not contain only numbers.
- Must not begin or end with a special character.
- Must not contain curly braces.



Note:

The format of username for Historian Web-based Clients is <host name>.admin, where <host name> is the machine on which Web-based Clients are installed. And, the default client ID is admin. Both the host name and client ID are case-sensitive.



If, however, the Proficy Authentication server hostname is long, resulting in a username longer than 20 characters, Windows does not allow you to create the user. In that case, you can create a Proficy Authentication user, and then [create the corresponding Windows user](#), using the `uaa_config_tool` utility.


10. Alternatively, if you want to use an external Proficy Authentication service (that is, a Proficy Authentication instance already installed by an external application such as Operations Hub):

a. Select the **Use External Proficy Authentication** check box.

The fields for the external Proficy Authentication service appear.

b. Enter values as described in the following table.

Field	Description
Proficy Authentication	Enter the URL of the external Proficy Authentication server in the following format: <code>https://<Proficy Authentication server name>:<port number></code> , where <code><Proficy Authentication server name></code> is the FQDN or hostname of the machine on which Proficy Authentication is installed. By default, the port number is 443.

Field	Description
Base URL	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: Do not enter a trailing slash character. </div>
Admin Client ID	Enter the client name that you provided while installing the external Proficy Authentication. The default value is admin.
Admin Client Secret	Enter the client secret that you provided while installing the external Proficy Authentication.

c. Select **Test Connection**.

The results of the connection test appear. You cannot proceed until the connection is successful.

11. Select **Next**.

The **Configuration Hub Installation** page appears, allowing you to choose whether you want to install Configuration Hub along with Web-based Clients or use an existing Configuration Hub.

Configuration Hub Installation

Use Existing Configuration Hub:

Install Location:

Plugin-Name:

Server Port:

Container Port:

Client ID:

Client Secret:

Re-enter Secret:

Note: Credentials used here are needed for registering other products with this Configuration Hub. Make sure to save these credentials for future registrations and upgrades to Configuration Hub.

Configuration Hub allows you to add and manage a collector instance remotely. For more information, refer to [About Configuration Hub](#).

If, however, an earlier version of Configuration Hub is available on the same machine, you will be prompted to enter the details of the existing Configuration Hub, and it will be upgraded to the latest version. If that happens, skip the next step.



Important:

By default, Configuration Hub points to the same Proficy Authentication server as the one you provided during the Historian server installation. If you want to install Web-based Clients in a cluster environment, ensure that:

- Configuration Hub does not use the same Proficy Authentication server as that used by the cluster.
- The Proficy Authentication and Configuration Hub details must be the same for all cluster nodes.

12. If you want to install Configuration Hub, ensure that the **Use Existing Configuration Hub** check box is cleared, and then provide values as described in the following table.

Field	Description
Install Location	If needed, modify the installation folder for Configuration Hub.
Plugin Name	If needed, modify the name of the Configuration Hub plugin for Historian. The default value is in the following format: Historian_<host name>. If, however, you are installing Web-based Clients in a cluster environment, the default value is Historian_<cluster name>. You can modify this value, but provide the same value for all the nodes in the cluster.
Server Port	If needed, modify the port number that you want to use for the web server (NGINX). The default value is 5000. If you want to install Web-based Clients in a cluster environment, provide the same value for all the nodes in the cluster.
Container Port	If needed, modify the port number for the Configuration Hub container. The default value is 4890.
Client ID	<p>Enter the username to connect to Configuration Hub. The default value is admin. The value that you enter can contain:</p> <ul style="list-style-type: none"> ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVWXYZ_0123456789) ◦ The following special characters: ><:~!@#%&*?
Client Secret	<p>Enter the password to connect to Configuration Hub. The value that you enter can contain:</p> <ul style="list-style-type: none"> ◦ Must contain at least eight characters. ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVWXYZ_

Field	Description
	VXYZ abcdefghijklmnopqrstuvwxyz_-0123456789) ◦ The following special characters: ><:~!@#\$\$%^&*?
Re-enter Secret	Re-enter the password to connect to Configuration Hub.

13. Alternatively, if you want to use an existing Configuration Hub:

- a. Select the **Use External Configuration Hub** check box. This check box is disabled if an existing Configuration Hub is detected.

The fields for external Configuration Hub appear.

Configuration Hub Installation

Use Existing Configuration Hub:

Plugin-Name:

Server Name:

Server Port:

Client ID:

Client Secret:

Test Connection Status: Test connection with Existing Configuration Hub Server is pending; click Test Connection

Enter the Client ID and Secret that you provided while installing Configuration Hug plugin for Historian to register with existing Configuration Hub.

- b. Provide values as described in the following table.

Field	Description
Plugin Name	If needed, modify the name of the Configuration Hub plugin for Historian. The default

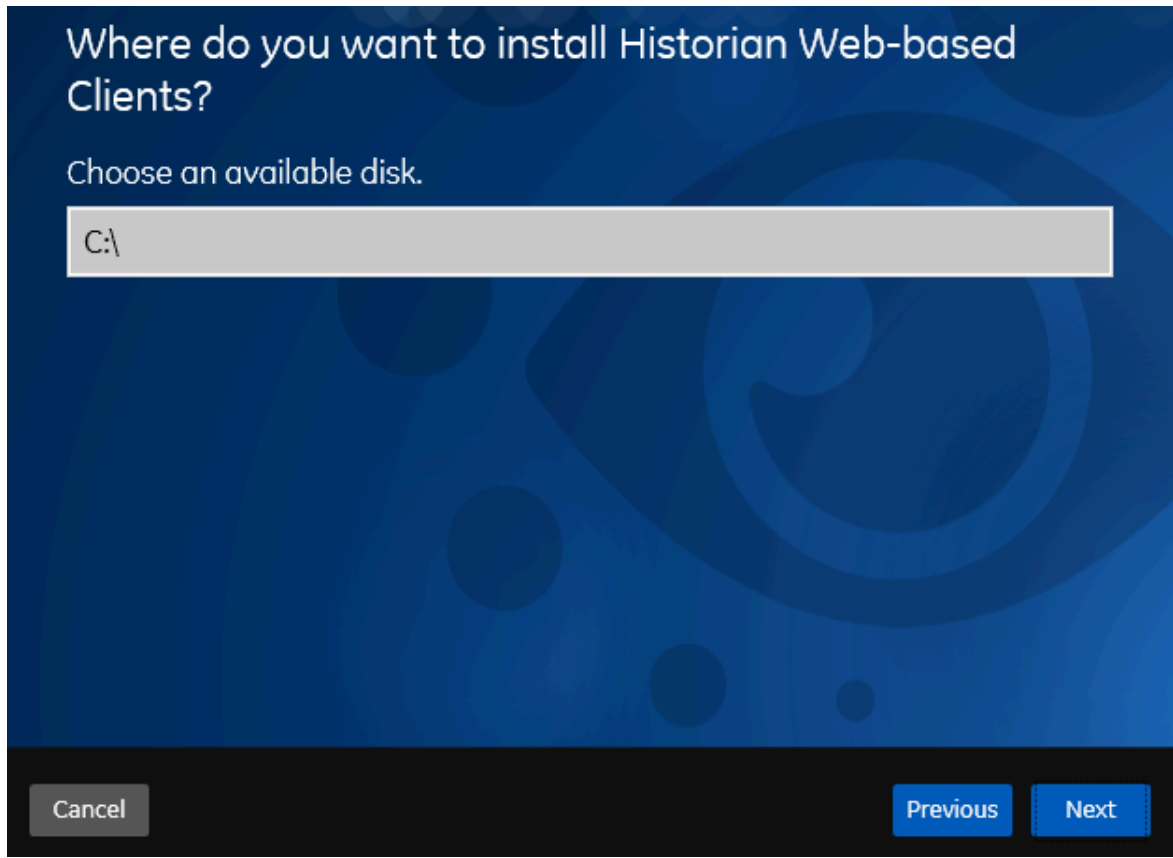
Field	Description
	value is in the following format: Historian_<host name>
Server Name	Enter the server name or the FQDN of the existing Configuration Hub server, as displayed in the address bar of the browser when you access Configuration Hub from the machine where Configuration Hub is installed.
Server Port	If needed, modify the port number that you want to use for the web server (NGINX). The default value is 5000.
Client ID	If needed, modify the username to connect to Configuration Hub. The default value is admin.
Client Secret	Enter the password to connect to Configuration Hub.

c. Select **Test Connection**.

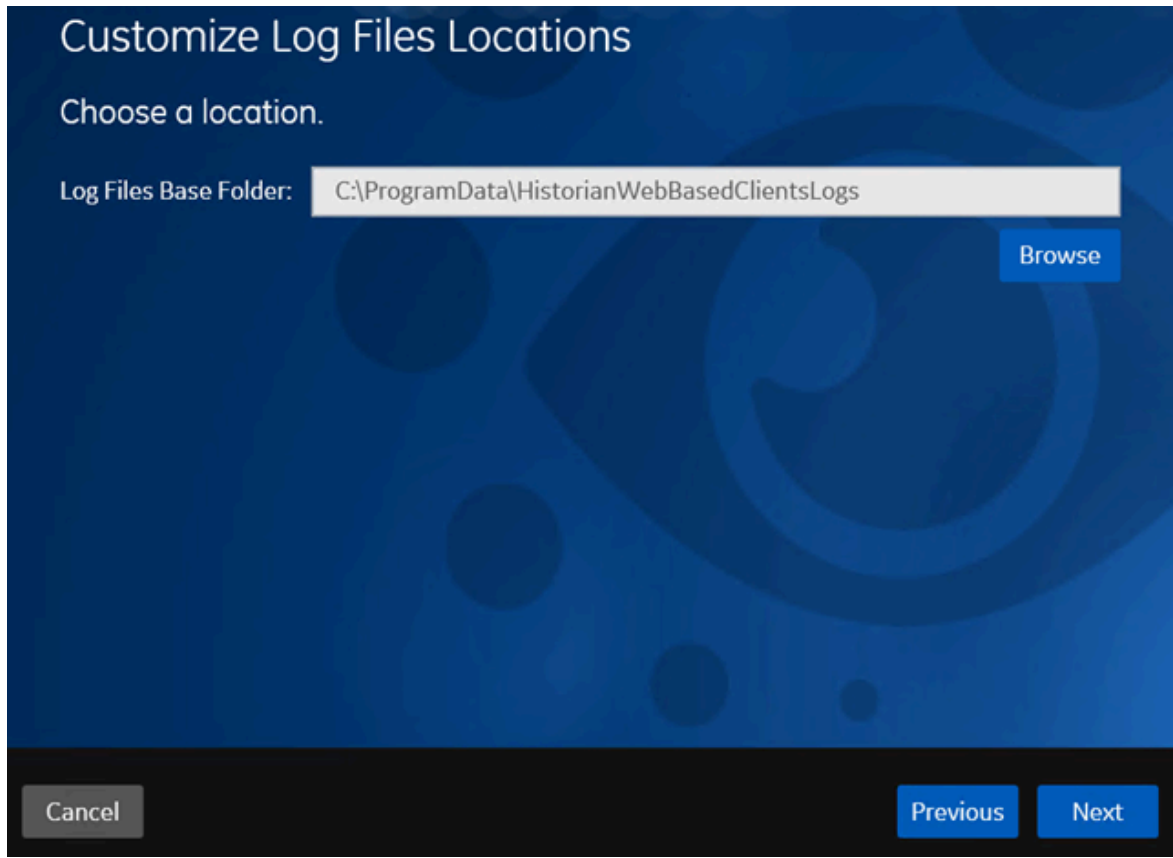
The results of the connection test appear. You cannot proceed until the connection is successful.

14. Select **Next**.

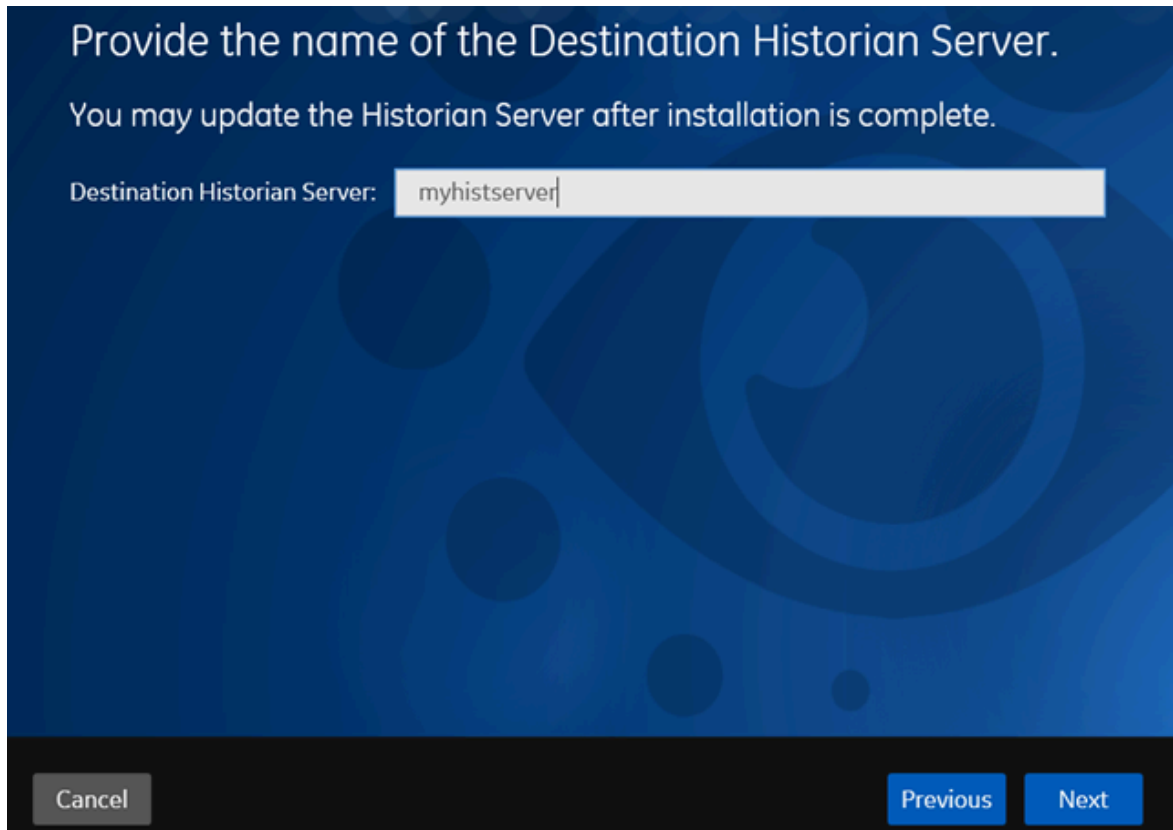
The default installation drive appears.



15. If needed, change the installation drive for Web-based Clients, and then select **Next**.
The log files location page appears.



16. If needed, change the location for log files, and then select **Next**.
The destination Historian server page appears.



17. Provide the name of the destination Historian server to which Web-based Clients are connected by default. When you login to Configuration Hub, the default system will point to this server.



Note:

- Provide the name of either Historian single-server or mirror primary server because the systems in Configuration Hub will be either a stand-alone system or a horizontally scalable system.
- If you want to connect to a remote Historian server, you must disable the **Enforce Strict Client Authentication** and **Enforce Strict Collector Authentication** options using Historian Administrator in the remote server.

18. Select **Next**.

A message appears, stating that you are ready to install Web-based Clients.

19. Select **Install**.

The Web-based Clients installation begins.

20. When you are prompted to reboot your machine, select **Yes**.

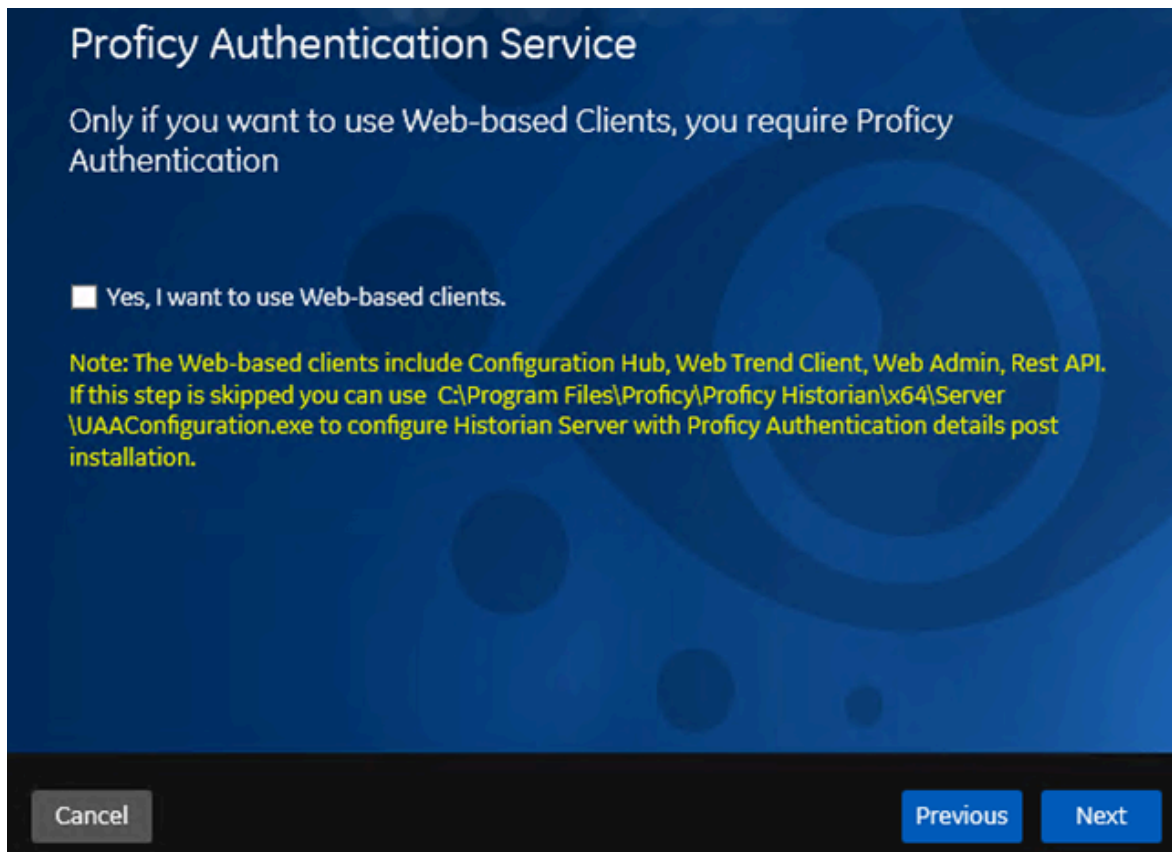
Historian Web-based Clients are installed in the following folder: `<installation drive>:\Program Files\GE`, and the following registry paths are created:

- HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital
- HKEY_LOCAL_MACHINE\SOFTWARE\GE

If you want to use Configuration Hub installed using other products such as iFIX, Plant Applications, and so on, [set up authentication](#) to point to the Proficy Authentication instance.

Install Web-Based Clients at a Command Prompt

1. [Install the Historian server \(on page 46\)](#). During the installation, in the **Proficy Authentication** page, select the **Yes, I want to use Web-based Clients** check box, and provide the Proficy Authentication server name and port number.



2. If you want to use Web-based Clients in a cluster environment, ensure that your network is enabled for multicast traffic, and [set up high availability](#) on each node in the cluster.

This topic describes how to install Web-based Clients at a command prompt. You can also [install Web-based Clients using an installer \(on page 104\)](#).

During the installation, you can choose to use Web-based Clients in a cluster environment, thus ensuring high availability of connection to the Historian server using the client applications.

1. If you want to install Web-based Clients with the default values, run the following command:

```
install.exe /quiet AdminClientSecret=<password> ConfigHubClientSecret=<password>
```

2. If you want to modify the default values, run the following command:


```
install.exe /quiet AdminClientSecret=<password> ConfigHubClientSecret=<password> <parameter>=<value>
```


The following table describes the installation parameters.

Parameter	Description	Default Value
PublicPort	<p>Port for https protocol communication used by Web-based Clients. Ensure that the value for this parameter matches the one you specify while installing the Historian server. In addition:</p> <ul style="list-style-type: none"> ◦ If you will install Operations Hub later on the same machine, the value that you provide for this parameter is populated while installing Operations Hub. ◦ If you have already installed Operations Hub on the same machine, provide the same value that you provided while installing Operations Hub. 	443
UAAHttpPort	Port for http protocol communication used by the Proficiency Authentication service.	9480

Parameter	Description	Default Value
UAADatabasePort	Port for the Proficy Authentication database.	9432
HistorianHttpPort	Port for the http protocol communication used by Web-based Clients.	8070
HistorianDatabasePort	Port for the PostgreSQL Historian database.	8432
EmbeddedWebServerAlternativeNames	<p>The fully qualified domain names to access Historian web applications remotely. You can use it to access the Web Admin console using alias names. Enter the values separated by commas.</p> <p>For example, to access the Web Admin console using any of the following URLs, enter <code>Test.abc.ge.com,localhost,127.0.0.1,aliasName</code></p> <ul style="list-style-type: none"> ◦ https:// Test.abc.ge.com /historian-visualization/hwa ◦ https:// 127.0.0.1 /historian-visualization/hwa ◦ https:// aliasName /historian-visualization/hwa ◦ https:// localhost /historian-visualization/hwa 	

Parameter	Description	Default Value
	<p data-bbox="678 279 873 325">! Important:</p> <ul data-bbox="808 338 1019 1856" style="list-style-type: none"><li data-bbox="808 338 1019 457">◦ Do not enter a space between the values.<li data-bbox="808 470 1019 905">◦ If you have already installed Operations Hub on the same machine, enter the same value that you have provided while installing Operations Hub.<li data-bbox="808 917 1019 1352">◦ If you will install Operations Hub later on the same machine, the value that you provide for this parameter is used while installing Operations Hub.<li data-bbox="808 1365 1019 1856">◦ You must add the IP address and alias name in the <code>hosts</code> file located at <code>C:\Windows\System32\drivers\etc</code>. The IP address that you add	


Parameter	Description	Default Value
	<p> must be a static or fixed IP address.</p> <p>Format: <code><IP address> <alias name></code></p> <p>Example: <code>1.2.3.4 myservername</code></p> <ul style="list-style-type: none"> ◦ FQDN is not supported for Configuration Hub. 	
AdminClientId	The client ID to connect to the Proficy Authentication service.	
AdminClientSecret	<p>The password to connect to the Proficy Authentication service. The password must satisfy the following conditions:</p> <ul style="list-style-type: none"> ◦ Must not contain only numbers. ◦ Must not begin or end with a special character. ◦ Must not contain curly braces. <p>If the password does not satisfy these conditions, the installation may be successful, but Web-based Clients will not work.</p>	Not applicable

Parameter	Description	Default Value
	<p> Note:</p> <p>The format of user-name for Historian Web-based Clients is <host name>.admin, where <host name> is the machine on which Web-based Clients are installed. And, the default client ID is admin. Both the host name and client ID are case-sensitive.</p> <p>If, however, the Proficy Authentication server hostname is long, resulting in a username longer than 20 characters, Windows does not allow you to create the user. In that case, you can create a Proficy Authentication user, and then create the corresponding Windows user, using the uaa_config_tool utility.</p>	
UseExternalUaa	Identifies whether you want to use an external Proficy Authentication service (that is, a Proficy Authentication instance already installed by an external application such as Operations	0

Parameter	Description	Default Value
	Hub). If you want to use external Proficy Authentication, enter 1.	
ActiveUaaBaseUrl	The base URL to connect to external Proficy Authentication. A value is required only if you want to connect to an external Proficy Authentication service. Enter a value in the following format: <code>https://<Proficy Authentication server machine name>:<public https port number></code> . By default, the port number is 443.	
ConfigHubContainerPort	The web server (httpd) port that you want to use for Configuration Hub.	5000
ContainerPort	The port for the Configuration Hub container.	4890
ConfigHubAdminPort	The port for the administration service for Configuration Hub.	4920
ConfigHubInstallFolder	The installation folder for Configuration Hub.	C:\Program Files (x86)\GE\Configuration-Hub
UseExternalConfigHub	Identifies whether you want to use Configuration Hub installed with iFIX or on a remote machine. If you want to use an external Configuration Hub, enter 1.	0
ExternalConfigHubMachine-Name	Enter the server name or the FQDN of the existing Configuration Hub server, as dis-	

Parameter	Description	Default Value
	played in the address bar of the browser when you access Configuration Hub from the machine where Configuration Hub is installed.	
ConfigHubClientID	<p>The username to connect to Configuration Hub. The value that you enter can contain:</p> <ul style="list-style-type: none"> ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPSRTUVWXYZ abcdefghijklmnopqrstuvwxy_0123456789) ◦ The following special characters: ><:~!@#\$%^&*? 	admin
ConfigHubClientSecret	<p>The password to connect to Configuration Hub. The value that you enter can contain:</p> <ul style="list-style-type: none"> ◦ Must contain at least eight characters. ◦ All English alphanumeric characters (ABCDEFGHIJKLMNOPSRTUVWXYZ abcdefghijklmnopqrstuvwxy_0123456789) ◦ The following special characters: ><:~!@#\$%^&*? 	
IsClusterNode	Indicates whether you want to install Web-based Clients in a cluster environment. If you want to install Web-based	0

Parameter	Description	Default Value
	Clients in a cluster environment, enter 1. This is not applicable if you are upgrading Web-based Clients.	
PostgresBaseDir	The folder in the shared drive that you want to use for Historian database if you want to add the Web-based Clients server to a cluster.	C:\ProgramData\GE\Operations Hub
ClusterFQDN	Enter the client access point of the role for which you have added the resources while setting up high availability (on page 105) .	
MulticastAddress	The common IP address that all the nodes in the cluster can use. Enter a value between 224.0.0.0 and 239.255.255.255 (or a hostname whose IP address falls in this range).	228.0.0.4
HistorianClusterMembershipPort	The common port number that all the nodes in the cluster can use. This port number, in conjunction with the multicast address, is used to create the cluster.	45564
HistorianClusterReceiverPort	The multicast port number that you want to use for incoming Historian data.	4000
DataPath	The path to the log files.	C:\ProgramData\HistorianWebBasedClientsLogs
DestinationHistorian	The name of the destination Historian server.	

Parameter	Description	Default Value
	 <p>Note: If you want to connect to a remote Historian server, you must disable the Enforce Strict Client Authentication and Enforce Strict Collector Authentication options using Historian Administrator in the remote server.</p>	

To install Web-based Clients with local Proficy Authentication and local Configuration Hub, run the following command:

```
Install.exe /quiet PublicPort=443 UAAHttpPort=9480 UAADatabasePort=9432 HistorianHttpPort=8070
HistorianDatabasePort=8432 AdminClientId=admin AdminClientSecret=abc
ConfigHubContainerPort=5000 ContainerPort=4890 ConfigHubInstallFolder="C:\Program Files
(x86)\GE\ConfigurationHub"
ConfigHubClientID=admin ConfigHubClientSecret=xyz
DataPath="C:\ProgramData\HistorianWebBasedClientsLogs"
```

To install Web-based Clients with local UAA and an external Configuration Hub, run the following command:

```
Install.exe /quiet PublicPort=443 UAAHttpPort=9480 UAADatabasePort=9432 HistorianHttpPort=8070
HistorianDatabasePort=8432 AdminClientId=admin AdminClientSecret=abc
UseExternalConfigHub=1 ExternalConfigHubMachineName=abc123 ConfigHubClientID=admin
ConfigHubClientSecret=xyz DataPath="C:\ProgramData\HistorianWebBasedClientsLogs"
```

To install Web-based Clients with external Proficy Authentication and a local Configuration Hub, run the following command:

```
Install.exe /quiet PublicPort=443 UAAHttpPort=9480 UAADatabasePort=9432 HistorianHttpPort=8070
HistorianDatabasePort=8432 AdminClientId=admin AdminClientSecret=abc UseExternalUaa=1
ActiveUaaBaseUrl=https://<external UAA machine hostname>:443
ConfigHubContainerPort=5000 ContainerPort=4890 ConfigHubInstallFolder="C:\Program Files
(x86)\GE\ConfigurationHub"
```

```
ConfigHubClientID=admin ConfigHubClientSecret=xyz
DataPath="C:\ProgramData\HistorianWebBasedClientsLogs"
```

To install Web-based Clients in a cluster environment with local Proficy Authentication and local Configuration Hub, run the following command:

```
Install.exe /quiet PublicPort=443 UAAHttpPort=9480 UAADatabasePort=9432
HistorianHttpPort=8070 HistorianDatabasePort=8432 AdminClientId=admin AdminClientSecret=abc
ConfigHubContainerPort=5000
ContainerPort=4890 ConfigHubInstallFolder="C:\Program Files (x86)\GE\ConfigurationHub"
ConfigHubClientId=admin ConfigHubClientSecret=xyz DataPath="C:\ProgramData\HistorianWebBasedClientsLogs"
DestinationHistorian=<Historian server host name> IsClusterNode=1
PostgresBaseDir="E:\pgsql" ClusterFQDN="cluster.domain.com"
HistorianClusterMembershipPort=45564 HistorianClusterReceiverPort=4000
UAAClusterMembershipPort=45565 UAAClusterReceiverPort=4005 MulticastAddress=228.0.0.4
```

Web-based Clients are installed in the following folder: *<installation drive>*:\Program Files \GE, and the following registry paths are created:

- HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital
- HKEY_LOCAL_MACHINE\SOFTWARE\GE

If you want to use Configuration Hub installed using other products such as iFIX, Plant Applications, and so on, [set up authentication](#) to point to the Proficy Authentication instance.

Upgrade Web-based Clients

- When you upgrade, Web-based Clients and associated data will be lost. Therefore, back up Web-based Clients and associated data using the `uaa_config_tool` utility provided in the `Utilities` folder of the ISO package. For information, refer to [Migrate User Authentication Data from Historian to Common Proficy Authentication Service \(on page 185\)](#).



Tip:

After installation, `uaa_config_tool` is available in the following folder as well:
<installation drive> \Program Files \GE Digital \Historian Config

- You cannot upgrade Web-based Clients from a version earlier than 8.0. This is because, starting 8.0, Web-based Clients are installed separately (not as part of the Historian server installation). Therefore, you must do either of the following:
 - Install Web-based Clients on a new machine.

- Uninstall the Historian server (remember to back up the Proficy Authentication using the UAA_config_tool utility), and then install Web-based Clients.
- If the machine name has changed, you must uninstall and reinstall Web-based Clients.
- If you want to use a different Proficy Authentication server from the previous one, you must manually migrate the Proficy Authentication data to new Proficy Authentication server using the uaa_config_tool utility.
- If you want to switch from using a local Proficy Authentication to using an external Proficy Authentication (or vice versa), you must manually change the Proficy Authentication details.

1. [Install Web-based Clients \(on page 104\)](#).

Web-based Clients will be upgraded to the latest version.

2. Clear the browser cache.

You can now access Web-based Clients.

Connect to a Remote Proficy Authentication Service

Provide the details of the external Proficy Authentication instance while [installing Web-based Clients \(on page 104\)](#).

To host a Proficy Authentication service, you can use the same machine on which Web-based Clients are installed or a different one. This topic describes how to connect to a Proficy Authentication service that is set up on a machine different from the one on which you have installed Web-based Clients.

1. Access the Web Admin console.
2. Select **Not Secure**, and then select **Certificate**.
3. Select the root CA certificate in the **Certificate Path** section.
The **Certificate Export Wizard** window appears.
4. Select the **Base-64 encoded X.509 (.CER)** format.
5. Install the certificate in Trusted Root Certification Authorities store.
6. Rename the certificate file from `.cer` to `.pem`.
7. Access Certificate Management Tool.
8. Access the **External Trust** section and import the renamed certificate.
9. Select **No** when prompted to restart GeOphubMasterStarter.
10. Restart the **GE Historian Tomcat** service.
11. Reopen the browser.

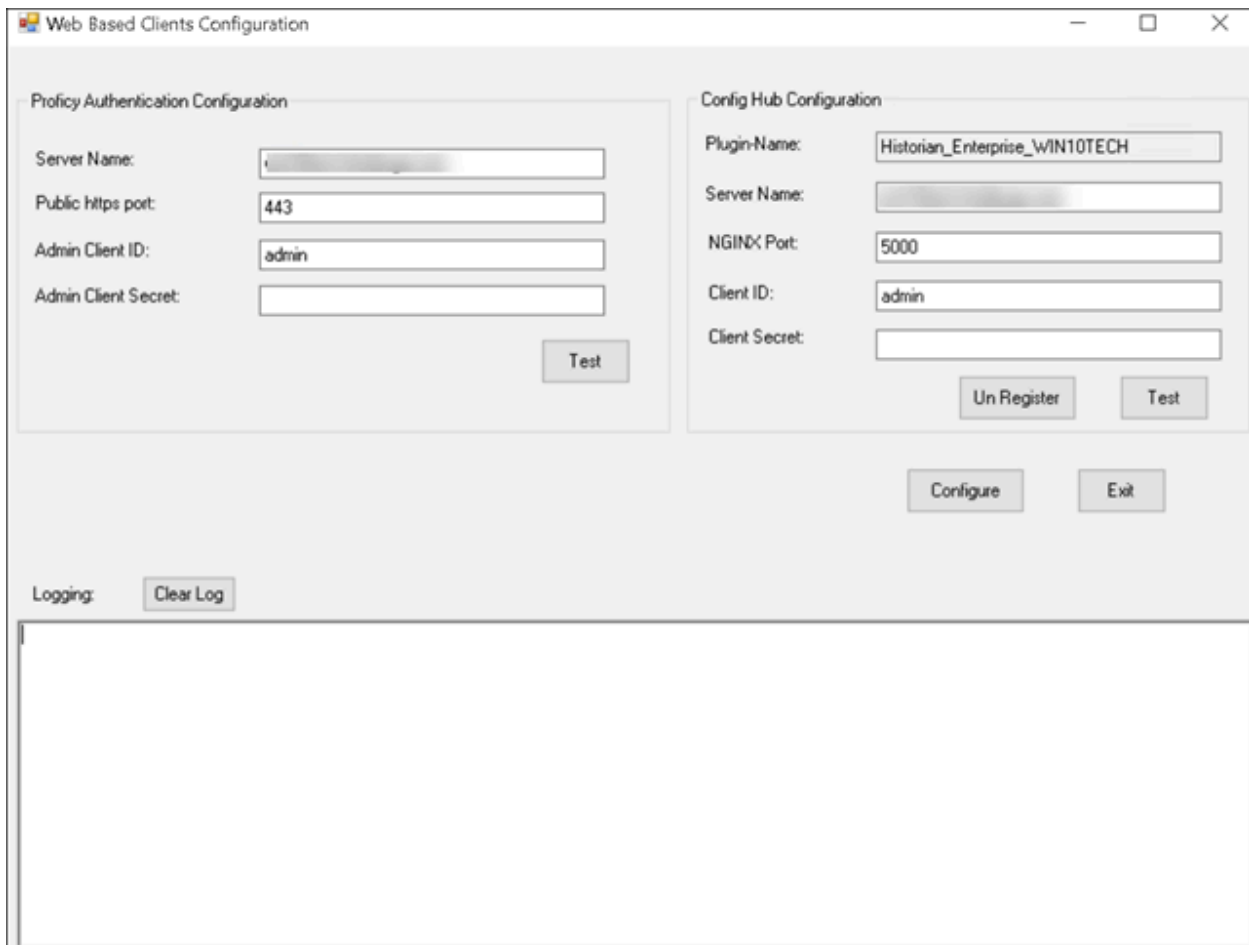
[Map the user groups of the remote Proficy Authentication service with the Historian Proficy Authentication group \(on page 159\)](#)

Configure Web-based Clients

You can configure the following settings for Web-based Clients:

- Reconfigure Proficy Authentication to point to a different Proficy Authentication server.
- Reconfigure the same Proficy Authentication instance to resolve any issues with login.
- Re-register Configuration Hub to resolve any issues.
- Unregister Configuration Hub, and register another one.

To perform these tasks, Historian provides a utility called Web Based Clients Configuration. It is installed during Web-based Clients installation.



The screenshot shows the 'Web Based Clients Configuration' utility window. It is divided into two main configuration sections:

- Proficy Authentication Configuration:** Includes fields for Server Name, Public https port (set to 443), Admin Client ID (set to admin), and Admin Client Secret. A 'Test' button is located below these fields.
- Config Hub Configuration:** Includes fields for Plugin-Name (set to Historian_Enterprise_WIN10TECH), Server Name, NGINX Port (set to 5000), Client ID (set to admin), and Client Secret. It features 'Un Register' and 'Test' buttons.

At the bottom of the window, there are 'Configure' and 'Exit' buttons. A 'Logging' section with a 'Clear Log' button is located at the bottom left, above a large empty text area for log output.

To run this utility, run the `Web_Clients_Configuration_Tool.exe` file. By default, it is located in the following folder: `C:\Program Files\GE Digital\Historian Config`

Remote Management Agents

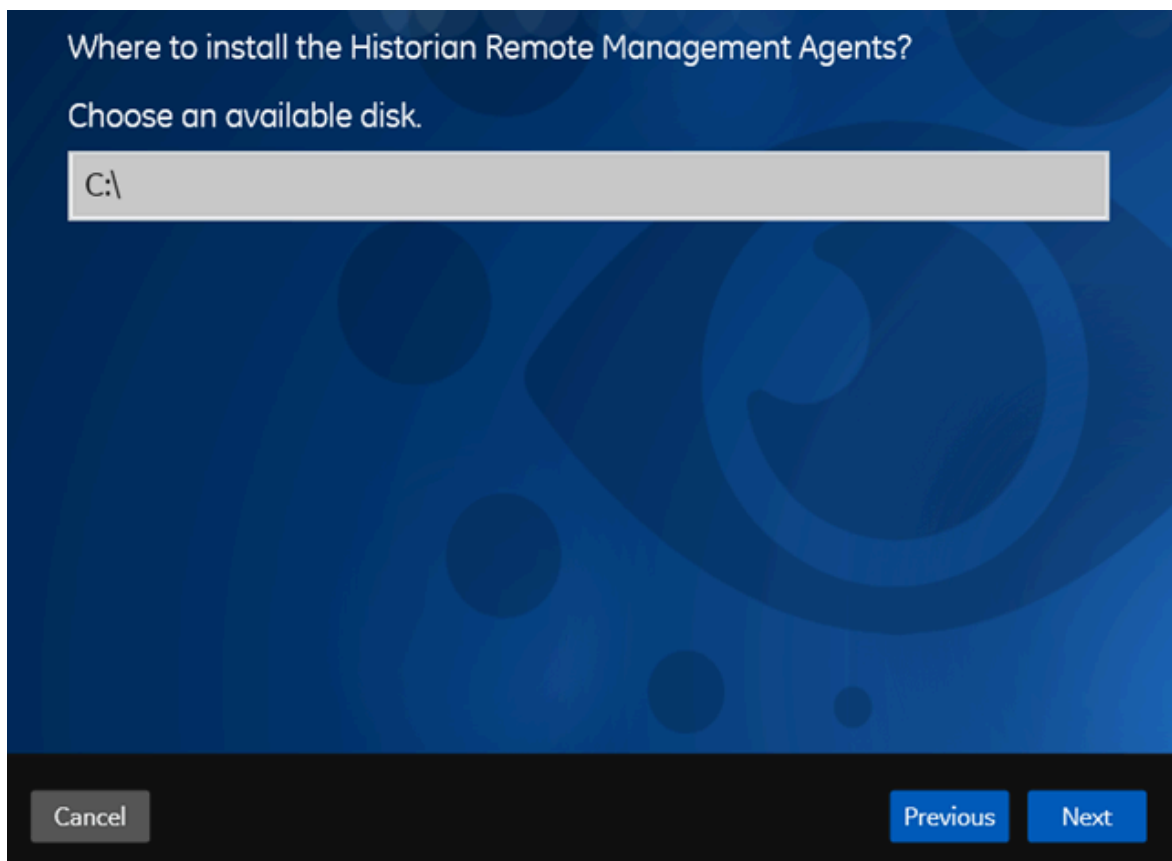
Install Remote Management Agent Using the Installer

Ensure that all the collectors that you want to manage remotely are in the running state.

If the collectors that you have installed are earlier than version 9.0, you must install Remote Management Agent on each machine on which the collectors that you want to manage are installed. For collectors version 9.0 or later, Remote Management Agent are automatically installed when you install collectors.

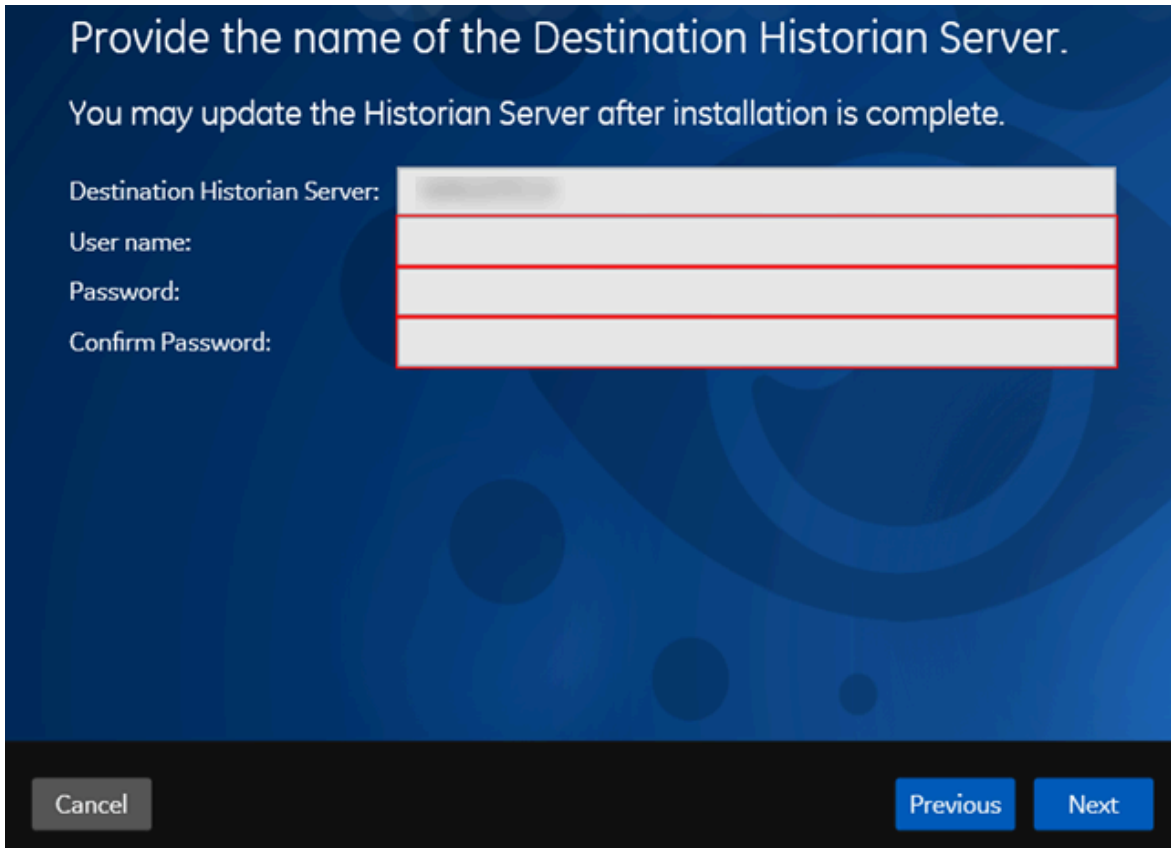
This topic describes how to install Remote Management Agent using the installer. You can also [install them at a command prompt \(on page 140\)](#).

1. Run the `InstallLauncher.exe` file.
2. Select **Install Remote Management Agents**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box, and then select **Next**.
The default installation drive appears.



5. If needed, modify the installation drive, and then select **Next**.

The destination Historian server page appears.

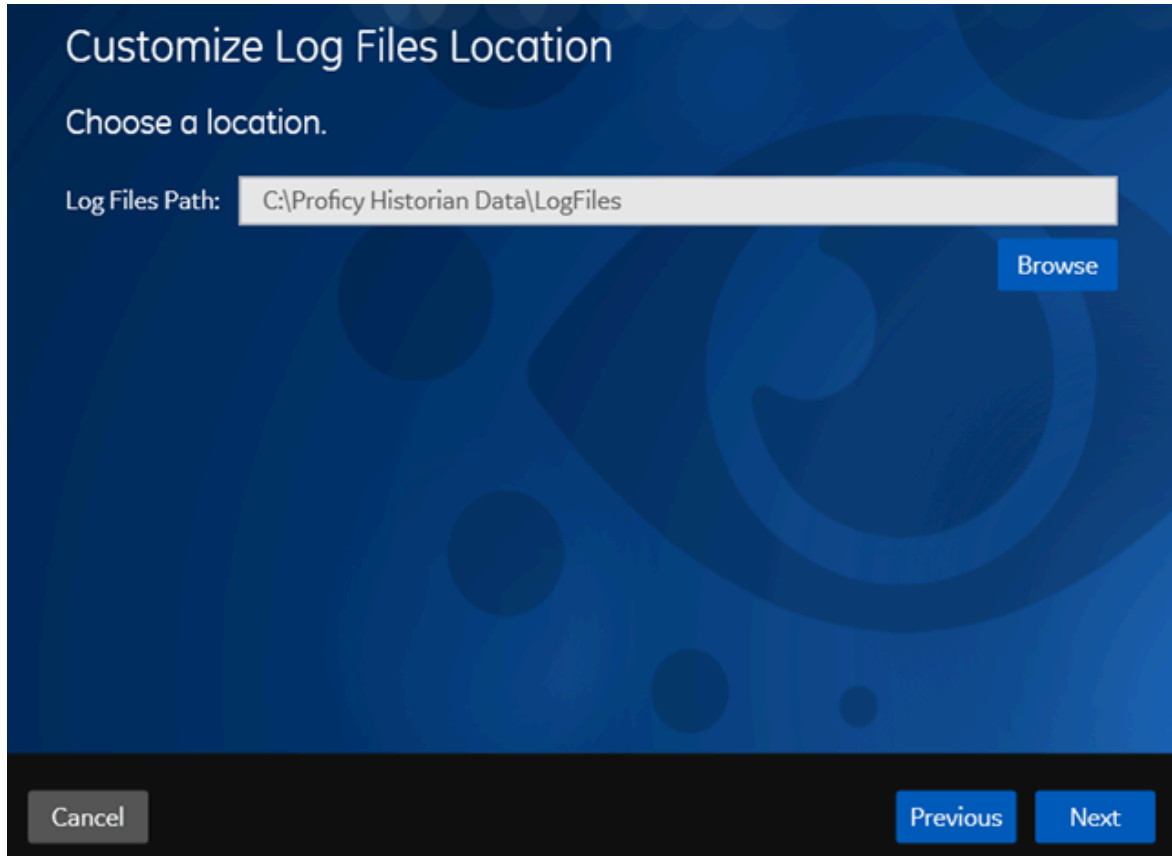


The screenshot shows a dark blue installation window with the following text and fields:

- Header: "Provide the name of the Destination Historian Server."
- Sub-header: "You may update the Historian Server after installation is complete."
- Form fields (all highlighted with a red border):
 - Destination Historian Server: [text input field]
 - User name: [text input field]
 - Password: [text input field]
 - Confirm Password: [text input field]
- Navigation buttons at the bottom:
 - Cancel (grey button)
 - Previous (blue button)
 - Next (blue button)

6. Enter the details of the default Historian server to which Remote Management Agent will connect, and then select **Next**.

The log files location appears.



7. As needed, modify the location of the log files, or leave the default value, and then select **Next**.

A message appears, stating that you are ready to install Remote Management Agent.

8. Select **Install**.

- Remote Collector Management is installed on your machine.
- A folder named `Historian Remote Management Agents` is created in the `GE Digital` folder in the installation location that you specified.
- Remote Collector Management is running, and a `.shw` file is created in the log folder. This file contains the details of the collectors that are running on the machine.
- For each collector that you manage using Remote Collector Management, a new entry named `ServiceName` is created in the collector registry. If the `ServiceName` key is not created or updated incorrectly, refer to [Troubleshooting Remote Collector Management Issues](#) (*on page* [141](#)).

Install Remote Management Agent at a Command Prompt

Ensure that all the collectors that you want to manage remotely are in the running state.

If the collectors that you have installed are earlier than version 9.0, you must install Remote Management Agent on each machine on which the collectors that you want to manage are installed. For collectors version 9.0 or later, Remote Management Agent are automatically installed when you install collectors.

This topic describes how to install Remote Management Agent at a command prompt. You can also [install them using the installer \(on page 138\)](#).

1. Access the command prompt, and navigate to the RMA folder in the install media.
2. Run the following command, replacing the values in angular brackets with the appropriate values:

```
HistorianRMA_Install.exe -s RootDrive=<installation drive> DestinationServerName=<Destination Historian server name>
UserNamel=<Windows username> Password=<Windows password> DataPath="C:\Proficy Historian Data\LogFiles"

HistorianRMA_Install.exe -s RootDrive=C:\ UserNamel=Administrator Password=AdminPassword
DestinationServerName=VMHISTWEBAUTO DataPath="C:\Proficy Historian Data\LogFiles"
```

- Remote Collector Management is installed on your machine.
- A folder named `Historian Remote Management Agents` is created in the `GE Digital` folder in the installation location that you specified.
- Remote Collector Management is running, and a `.shw` file is created in the log folder. This file contains the details of the collectors that are running on the machine.
- For each collector that you manage using Remote Collector Management, a new entry named `ServiceName` is created in the collector registry. If the `ServiceName` key is not created or updated incorrectly, refer to [Troubleshooting Remote Collector Management Issues \(on page 138\)](#).

Install the OPC UA HDA Server

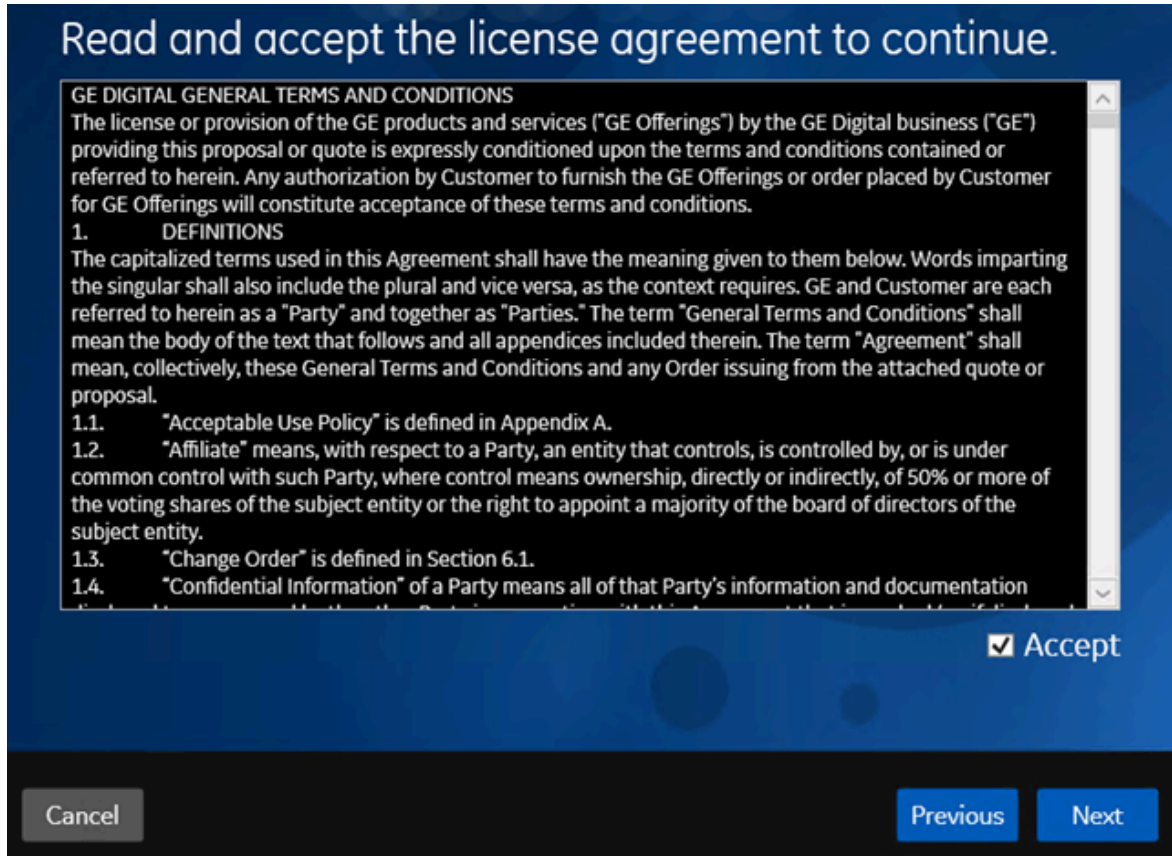
[Install Historian \(on page 44\)](#).



Note:

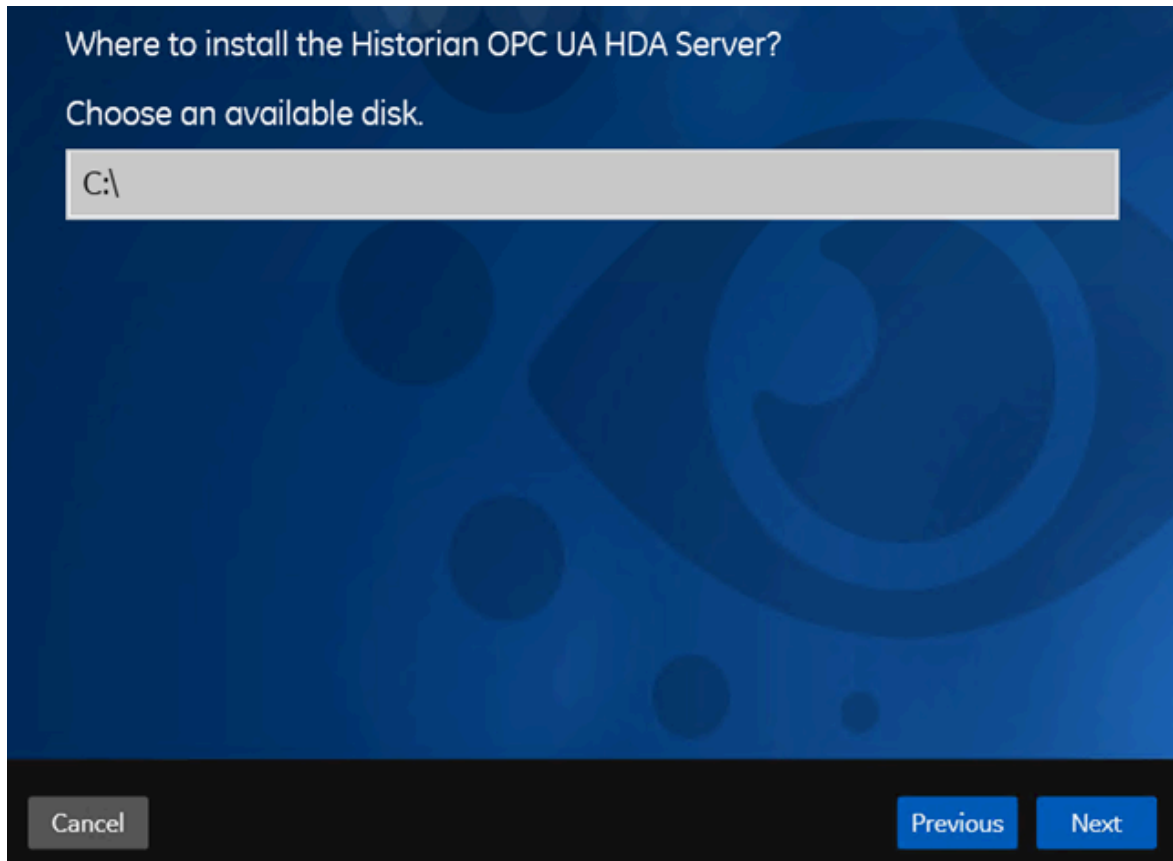
You can install Historian and the OPC UA HDA server on the same machine or on different machines.

1. Run the Historian installer.
2. Select **Install Historian OPC UA HDA Server**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.



4. Select the **Accept** check box, and then select **Next**.

The following page appears, asking you to select the installation drive.



5. Select the installation drive, and then select **Next**. You can retain the default one, or choose a different one.

The **OPC UA HDA Server Attributes** page appears.

OPC UA HDA Server Attributes

Historian OPCUA HDA Server :	
Port Number :	48010
URI	opc.tcp:// :48010

Cancel
Previous
Next

6. Provide values as described in the following table, and then select **Next**.

Field	Description
Historian OPCUA HDA Server	Enter the host name or the IP address of the machine on which you want to install the OPC UA HDA server. By default, the local host name appears.
Port Number	Enter the port number that you want the OPC UA HDA server to use.
URI	The URI to access the OPC UA HDA server. This field is disabled and populated with a value in the following format: <code>opc.tcp://<host name>:<port number></code> , where <code><host name></code> and <code><port number></code> are the values that you have entered in the preceding fields.

The **Historian Server Details** page appears.

Historian Server Details

Historian Server Name :

Historian Server User Name :

Historian Server Password :

7. Provide values as described in the following table, and then select **Next**.

Field	Description
Historian Server Name	Enter the name of the Historian server that you want to connect to the OPC UA HDA server.
Historian Server User Name	Enter the username of the Historian server.
Historian Server Password	Enter the password of the Historian server.

The **You are ready to install** page appears.

8. Select **Install**.

The Historian OPC UA HDA server is installed. Reboot the machine when prompted to do so.

- If you have installed the OPC UA HDA server on a remote machine, enable the firewall.
- Install an OPC UA client.
- Configure the OPC UA HDA server.

The Excel Add-In for Historian

Install the Historian Excel Add-in Using the Installer

Install one of the following 32-bit or 64-bit Microsoft® Excel® applications:

- Microsoft® Excel® 2019
- Microsoft® Excel® 2016
- Microsoft® Excel® 2013
- Microsoft® Excel® 2010

You can install Excel Add-In separately or during Client Tools installation. This topic describes how to install Excel Add-In separately using the installer. You can also [install it at a command prompt \(on page 146\)](#). However, do not install Excel Add-In on the machine on which you have installed Historian Administrator or data archiver.

1. Run the `InstallLauncher.exe` file.
2. Select **Historian Excel Add-in**.

The installer runs through the installation steps.



Note:

If using certain versions of Windows (like Windows 10 or Windows 2019), you may receive an error message, stating that some of the DLL files are not registered. You can ignore these messages.

3. When prompted to reboot your system, select **Yes**.

Excel Add-In is installed.

[Activate Excel Add-In \(on page 147\)](#).

Install the Historian Excel Add-in at a Command Prompt

1. Install one of the following 32-bit or 64-bit Microsoft® Excel® applications:
 - Microsoft® Excel® 2019
 - Microsoft® Excel® 2016
 - Microsoft® Excel® 2013
 - Microsoft® Excel® 2010

2. [Install Excel Add-in using the installer \(on page 146\)](#) on a machine. When you do so, a template file named `setup.iss` is created at `C:\Windows`. This file stores the installation options that you have provided during the installation. You can then use this template to install Excel Add-in at a command prompt on other machines.

You can install Excel Add-In separately or during Client Tools installation. However, do not install Excel Add-In on the machine on which you have installed Historian Administrator or data archiver.

1. Copy the `setup.iss` file to each machine on which you want to install Excel Add-in at a command prompt.
2. In the folder that contains the `setup.iss` file, run the following command: `setup.exe /s /sms`
The installer runs through the installation steps.

**Note:**

If using certain versions of Windows (like Windows 10 or Windows 2019), you may receive an error message, stating that some of the DLL files are not registered. You can ignore these messages.

3. When prompted to reboot your system, select **Yes**.

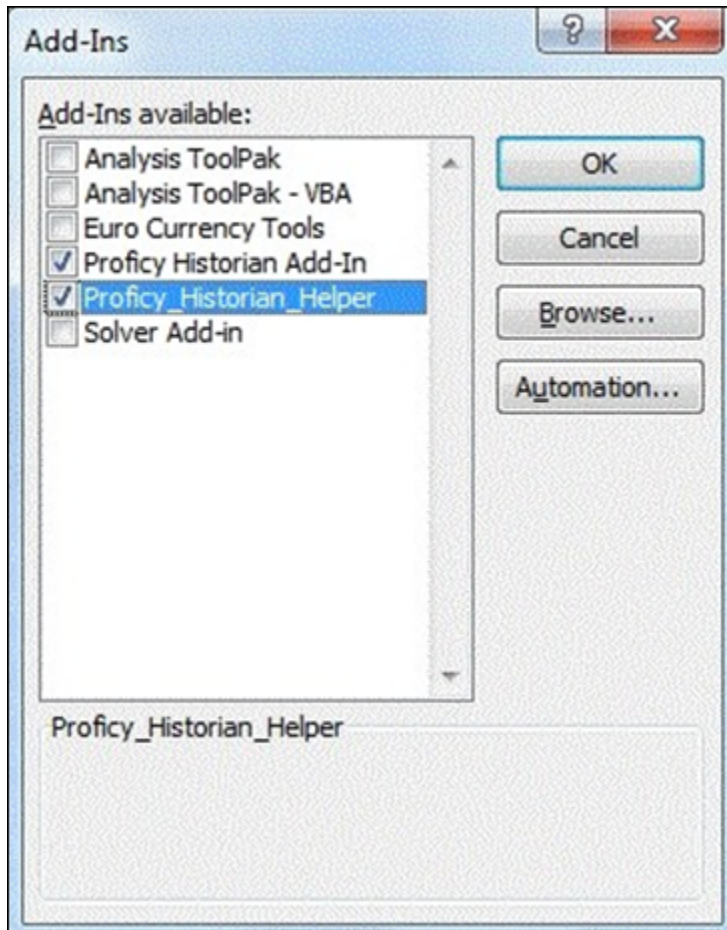
Excel Add-In is installed.

[Activate Excel Add-In \(on page 147\)](#).

Activate Excel Add-In

[Install Excel Add-In \(on page 146\)](#).

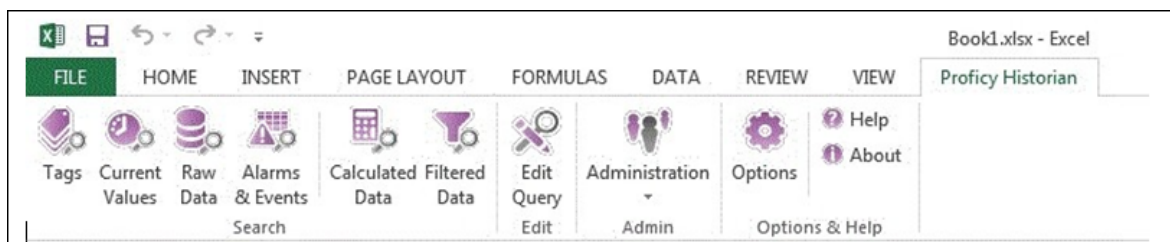
1. Open a new Microsoft Excel worksheet.
2. Select **File > Options**.
The **Excel Options** window appears.
3. Select **Add-Ins**.
4. In the **Manage** box, select **Excel Add-ins**, and then select **Go**.
The **Add-Ins** window appears.



5. Select the **Proficy Historian Add-In** and **Proficy_Historian_Helper** check boxes, and then select **OK**.

If the **Proficy Historian Add-In** and **Proficy_Historian_Helper** check boxes do not appear, select **Browse** to locate the `Historian.xla` file for the check boxes to appear. This file is created if you have installed Microsoft Excel after installing Excel Add-In. By default, the `Historian.xla` file is located in the `C:\Program Files\Proficy\Historian` or `C:\Program Files (x86)\Proficy\Historian` folder.

Excel Add-In is now ready to use and the **Proficy Historian** menu is now available in the Microsoft Excel toolbar.



Software Requirements

The following components are required to use Excel Add-in for Operations Hub:

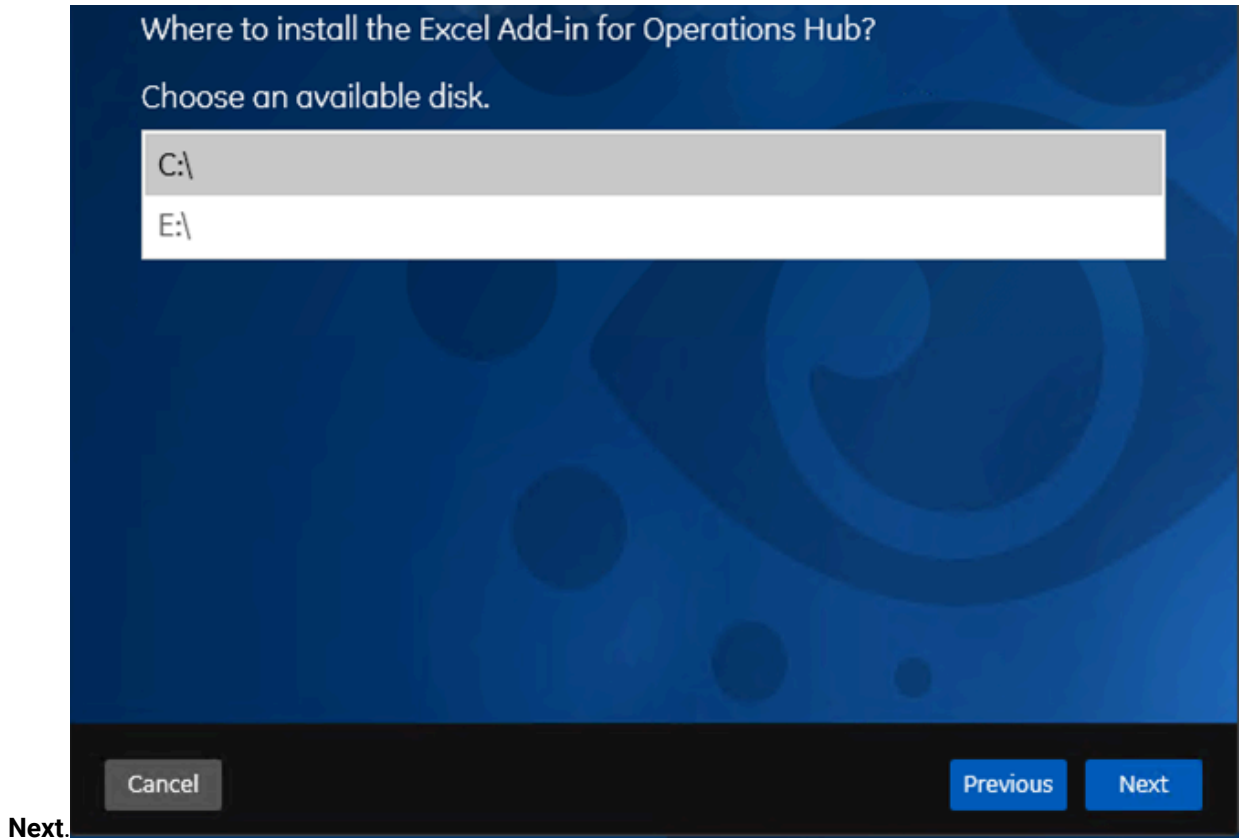
Component	Version	Description
Operations Hub	2.0, 2.1	<p>If you have purchased the standard or enterprise license of Historian, you receive a no-cost license for Operations Hub, which enables you to:</p> <ul style="list-style-type: none"> • Access to the Historian Analysis run-time application, which is an in-built HTML5 application in Operations Hub. • Perform advanced trend analysis, including inserting annotations. • Define an asset model including tag mapping.
Microsoft Excel	2016 and 2019 (32 bit or 64 bit)	
Historian REST APIs		<p>Historian REST APIs are required to integrate between Historian and Operations Hub. Historian REST APIs are installed automatically when you install Historian Web-based Clients (on page 109).</p>

Install Excel Add-In for Operations Hub

[Install the Historian server \(on page 44\)](#) and other [software requirements \(on page 149\)](#).

1. Run the `InstallLauncher.exe` file.
2. Select **Install Excel Add-in for Operations Hub**.
The welcome page appears.
3. Select **Next**.

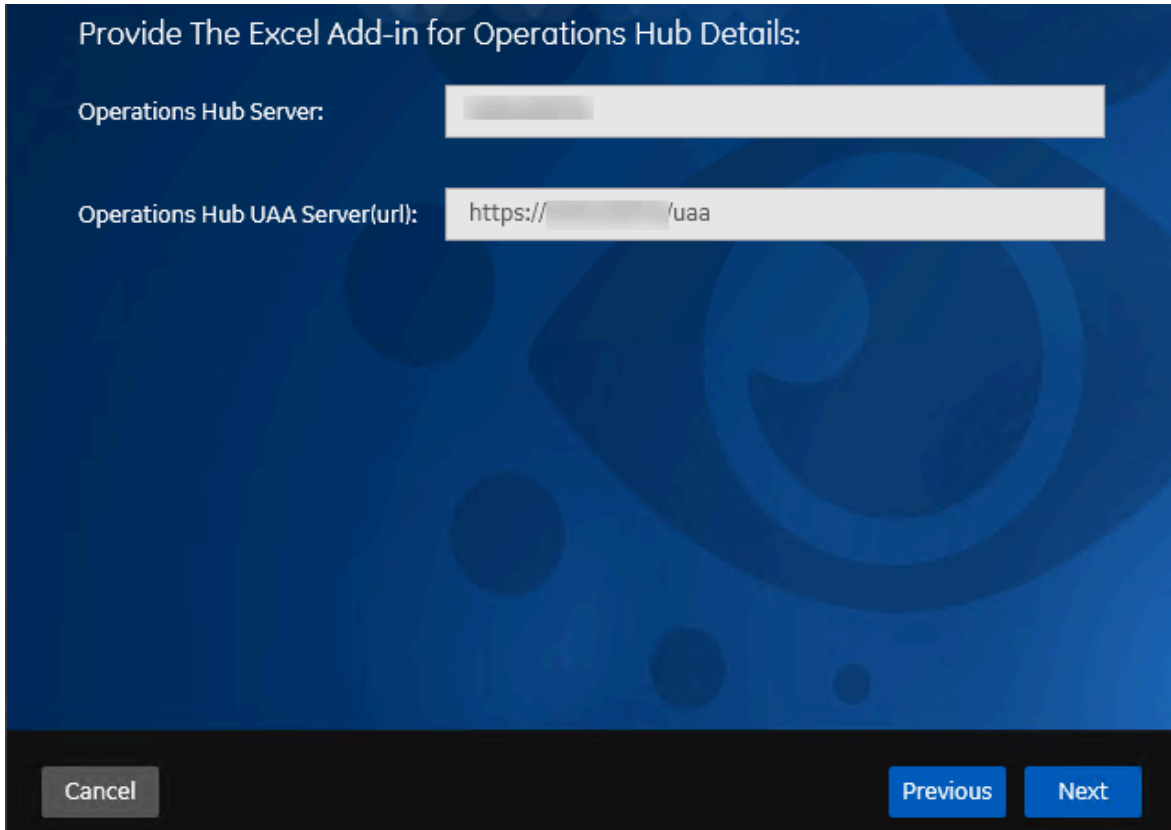
4. Read and accept the license agreement, and then select **Next**.
5. Select the available disk to install the Excel Add-in for Operations Hub, and then select



Note:

We recommend that you select the drive where Microsoft Excel is installed.

6. Provide the details of Operations Hub, and then select **Next**.



Provide The Excel Add-in for Operations Hub Details:

Operations Hub Server:

Operations Hub UAA Server(url):

Cancel Previous Next

The **You are ready to install** page appears.

7. Select **Install**.

Excel Add-In for Operations Hub is installed.

Copy/export the issuer certificate (on page 151), and then install/import it (on page 152).

Copy or Export the Issuer Certificate on Server

Install Excel Add-In for Operations Hub (on page 149).

1. Navigate to the machine where Operations Hub is installed.
2. Select **Site Information (Not secure)**.
3. Select **Certificate (invalid)**.
The **Certificate** window appears.
4. Select **Certificate Path**.
5. Select the Root CA certificate.
6. Select **Details**.
7. Select **Copy to file**.
The **Certificate Export Wizard** window appears.
8. Select **DER encoded binary X.509(.CER)** format and select **Next**.

9. Select **Browse** to save the certificate file at desired location.
10. Complete the certificate export.

[Install or import the certificate \(on page 152\).](#)

Install/Import the Issuer Certificate

[Copy or export the issuer certificate \(on page 151\)](#) on the machine on which Excel Add-In for Operations Hub is installed.

1. Right-click the certificate, and then select **Install Certificate**.
The **Certificate Import Wizard** page appears
2. Select **Local Machine**, and then, select **Next**.
3. Select **Place all certificates in the following store**.
4. Select **Trusted Root certification Authorities**, and then select **OK**.
5. Select **Next**, and then select **Finish**.
The certificate is imported.

[Configure the Operations Hub server \(on page 152\).](#)

Connect to Operations Hub

To query a model defined in Operations Hub, you must first connect to the Operations Hub server. You will then receive a token from the server, which will be used for authentication.

1. Select **Configuration** menu in Admin.
The **Operations Hub Configuration** window appears.
2. Provide values as described in the following table.

Field	Details
Operations Hub Server	The Operations Hub server name to which you want to connect and get the data.
Operations Hub Proficy Authentication Server (url)	The URL of the Proficy Authentication service of Operations Hub. Example: https://<ophubservername>/uaa



Note:

The **Token Status** field indicates the status of the connection with Operations Hub server.

3. Select **Connect**.

The login page appears.

4. Provide the **User Identifier** and **Password** to connect to Operations Hub.

5. Select **Open UaaAuthSchemeHandler**.

Operations Hub Server to which you are connected and the status of the token appears.

6. Select **Save** to save the Operations Hub server details. The configuration will be retained and used when you open excel add-in again.

Install the Historian ETL Tools

- If you want to use the Historian Extract, Transform, and Load (ETL) tools to transfer data from a PI Historian server, install the PI SDK package.
- If you want to use the ETL tools to transfer data from an eDNA server, copy the following eDNA binaries to the `<installation drive>\Program Files\GE Digital\Historian ETL eDNA Extract` folder:

- `EzDnaApi.dll`
- `EzDNAApiNet.dll`

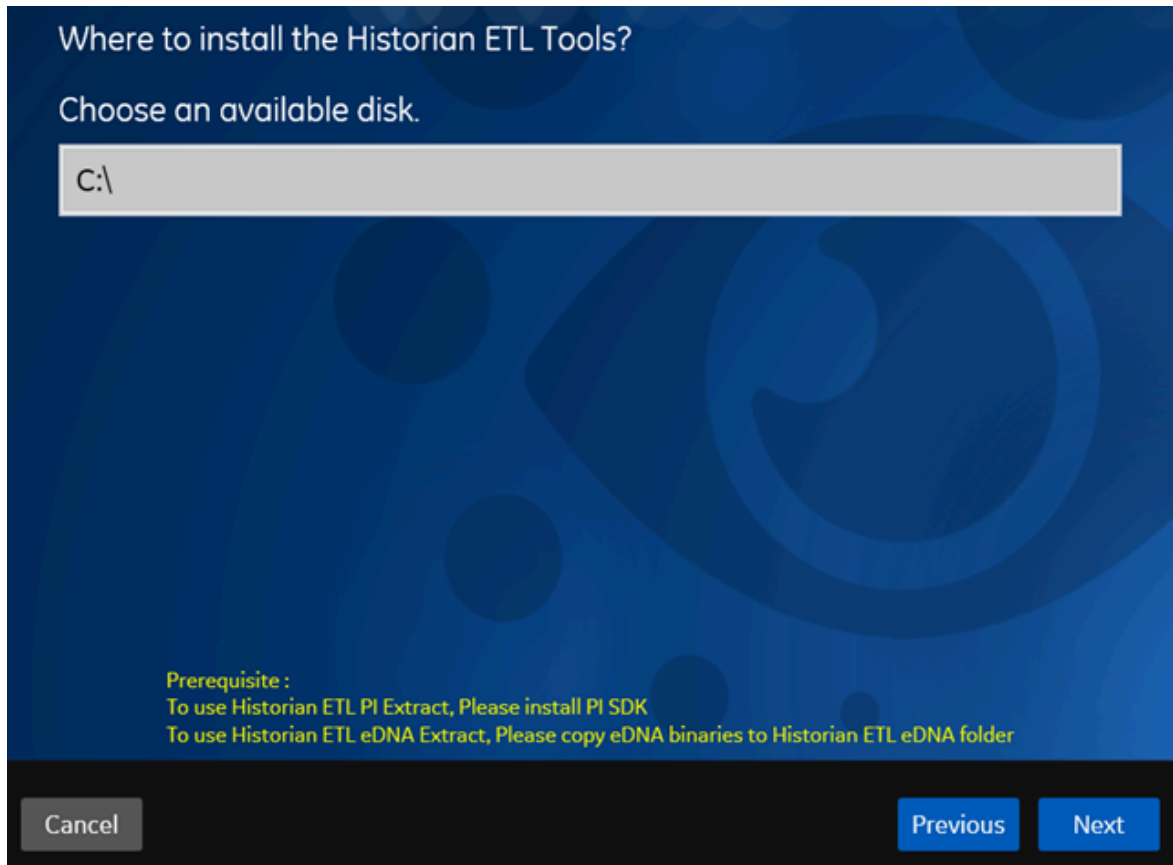
By default, these files are available in the following folder on the machine on which the eDNA server is installed: `C:\Program Files(x86)\eDNA`

Installing ETL installs the following tools:

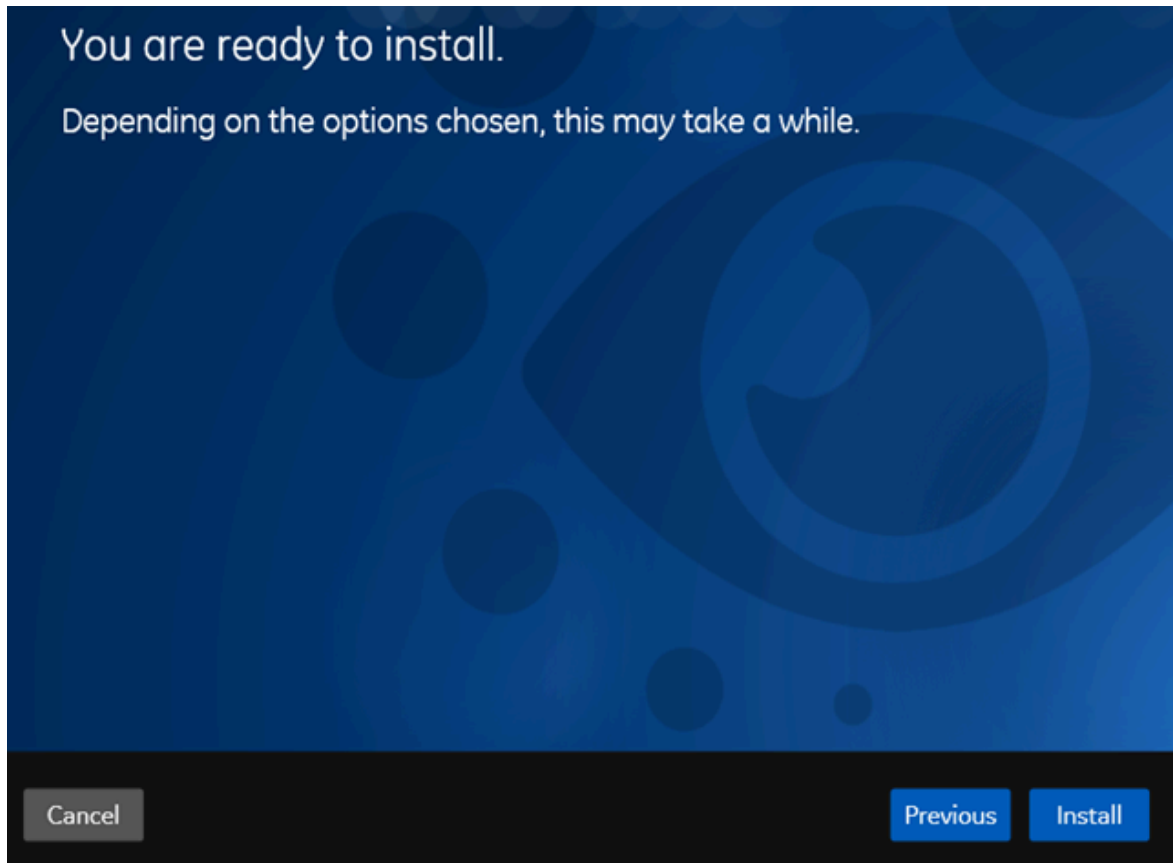
- The Extract tool
- The Transform tool
- The Load tool

This topic describes how to install ETL to extract, transform, and load data from an onsite Historian machine to the destination Historian server. You must install Historian ETL on both the onsite Historian machine and the destination Historian server (that is, the source and destination machines for data transfer).

1. Run the `InstallLauncher.exe` file.
2. Select **Install Historian ETL Tools**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box, and then select **Next**.
The default installation drive appears.



5. If required, modify the installation drive for Historian ETL, and then select **Next**.
A message appears, stating that you are ready to install ETL.



6. Select **Install**.

The Historian ETL tools are installed on your machine.

- The following folders are created in the *<installation drive>/Program Files/GE Digital* folder:
 - Historian ETL eDNA Extract
 - Historian ETL Extract
 - Historian ETL Load
 - Historian ETL ODBC Extract
 - Historian ETL PI Extract
 - Historian ETL Transform
- The following services are installed:
 - Historian ETL eDNA Extract
 - Historian ETL Extract
 - Historian ETL ODBC Extract_x64
 - Historian ETL ODBC Extract_x86

- Historian ETL Load
- Historian ETL PI Extract
- The following registry paths are created:
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\GE Digital\Historian ETL eDNA Extract
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\GE Digital\Historian ETL ODBC Extract
 - HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL Extract
 - HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL ODBC Extract
 - HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL PI Extract
 - HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL Load

1. If you want to extract data from an eDNA server, copy the `Customdna.ini` file in the eDNA server into the `C:\Windows` folder on the machine on which you have installed ETL.
2. Extract data from an eDNA server (*on page*), ODBC data source (*on page*), Proficy Historian (*on page*), or PI Historian (*on page*).

About Installing Help

Historian documentation is available both online and offline. This topic describes how to install the offline Help documentation. Online Help is available here: <https://www.ge.com/digital/documentation/historian/>

You can install Help using a GUI-based installer or at the command prompt.

Install Help Using the Installer

This topic describes how to install Help using the installer. You can also [install Help at a command prompt \(on page 157\)](#).

1. Run the `InstallLauncher.exe` file.
2. Select **Install Help**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box to accept the license agreement, and select **Next**.
5. If needed, change the installation drive, and then select **Next**.
6. If needed, change the port number for the NodeJS server to run. This step is required if the default port number is not available.
7. Select **Next**.

8. Select **Install**.

The Help is installed.

9. Select **Next**.

The stand-alone Help is installed in the following folder: `<installation drive>:\Program Files\Proficy\Proficy Historian\ProficyDoc`. You can access the Help from any of the Historian applications or by accessing the `index.html` file.

Install Help at a Command Prompt

This topic describes how to install Help at a command prompt. You can also [install Help using the installer \(on page 156\)](#).

1. Navigate to the `Help` folder.
2. If you want to use the default installation drive (C:/) and port number (7070), run the following command:

```
Help_Install.exe -s
```

Otherwise, run the following command:

```
Help_Install.exe -s RootDrive=<installation drive> PortNumber=<port number>
```

The Help is installed. You can access the Help from any of the Historian applications or by accessing the `index.html` file. By default, this file is available in the `C:\Program Files (x86)\GE Digital\Historian Help` folder.

Using External Proficy Authentication or LDAP Groups

About Proficy Authentication

In Historian, user authentication is handled using Proficy Authentication, which provides user account and authentication (UAA) service. Proficy Authentication provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including OAuth2.

When a user is created, modified, or deleted in Historian, the associated user account is being created, modified, or deleted in the Proficy Authentication instance, respectively.



Note:

This is done in the backend automatically. Therefore, most users will not require knowledge on UAA to perform basic user management, except when additional configuration is required.

To use Proficy Authentication, you can choose between the following options while installing Web-based Clients:

- **Use a local Proficy Authentication service:** Use this option if you want to create a local Proficy Authentication instance. This is the default option. You can create this while installing Web-based Clients.
- **Using a remote Proficy Authentication service:** Use this option if you are currently using a Proficy Authentication service on a remote machine. You can install this service using Historian Web-based Clients, or you can use any other UAA service (such as Proficy Authentication installed using Operations Hub). You can then manage these users in Web-based Clients. The users in the remote Proficy Authentication service can then use Web-based Clients.

This section describes how to use the Proficy Authentication IdP Configuration tool to map remote Proficy Authentication groups, LDAP groups, and LDAPS groups with the Proficy Authentication groups. For information on creating groups and users using the Proficy Authentication IdP Configuration tool, refer to:

- https://www.ge.com/digital/documentation/uaa/c_uaa_about_uaa_groups.html
- https://www.ge.com/digital/documentation/uaa/c_uaa_about_uaa_users.html



Note:

Mapping SAML groups is not supported.

About Proficy Authentication Groups

A Proficy Authentication group is created for a specific type of users who will likely perform the same type of activities.

If you have groups in a remote Proficy Authentication service, you can use them with Historian using the Proficy Authentication LDAP Integration tool. This section describes how to map the groups in the remote Proficy Authentication service with Historian counterparts. By default, Historian contains the following Proficy Authentication groups:

- **historian_visualization.admin:** Provides access to Trend Client and the Web Admin console.
- **historian_visualization.user:** Allows access to Trend Client.
- **historian_rest_api.read:** Provides read access to public REST API.
- **historian_rest_api.write:** Provides write access to public REST API.
- **historian_rest_api.admin:** Provides read/write access to public REST API.
- **historian_enterprise.admin:** Provides read/write access to Configuration Hub APIs.

**Note:**

Instead of mapping the groups, you can choose to map individual users with Historian users. For instructions, refer to [Managing Proficy Authentication Users Using the Configuration Tool \(on page 221\)](#).

Workflow

1. Provide the details of the remote Proficy Authentication service while [installing Web-based Clients \(on page 104\)](#).
2. [Connect to the remote Proficy Authentication service \(on page 136\)](#).
3. [Map the Proficy Authentication groups \(on page 159\)](#) with that of the Historian Proficy Authentication instance. You can map the groups in [LDAP \(on page 161\)](#) and [LDAPS \(on page 164\)](#) (LDAP via SSL) as well.

Using Server Certificates

To use server certificates with Historian, use the Certificate Management tool. This tool supports the following combination of files to import the certificate chain and the private key:


- A PEM file that contains the certificate chain and the private key.
- A PEM file that contains the certificate chain, and another PEM file for the private key.
- A PFX file that has the certificate chain and the private key.

For instructions on using the Certificate Management tool, refer to https://www.ge.com/digital/documentation/opshub/windows/windows/c_about_certificate_management.html.

Map Remote Proficy Authentication Groups With Historian Proficy Authentication

[Connect to the remote Proficy Authentication service \(on page 136\)](#).

If you want users from a remote Proficy Authentication service to use Historian, you must map the corresponding Proficy Authentication groups with a Historian Proficy Authentication group, which is created during Web-based Clients installation.

1. Double-click the Proficy Authentication IdP Configuration tool icon () , and log in the Proficy Authentication client ID and secret.

**Tip:**

By default, this icon appears on the desktop after you install Web-based Clients.

The **Identity Providers** page appears.

2. Select the **Map Existing Proficy Authentication Groups** check box.
3. In the **Proficy Authentication Connection** section, provide values as specified in the following table.

**Important:**

- The values that you provide in this step must match the values that you provided in the **User Account and Authentication Service** page while installing Web-based Clients. These values are required to connect to the Historian Proficy Authentication.
- Web-based Clients work only with a single instance of Proficy Authentication, which is specified during Web-based Clients installation. After installation, you cannot change the instance of Proficy Authentication that Web-based Clients will use.

Box	Description
URL	Enter the authorization server URL of the Proficy Authentication service that you specified in the Proficy Authentication Base URL box during installation (for example, https://localhost).
Client ID	Enter Admin as client ID.
Client Secret	Enter the client secret configured for the OAuth client that you specified in the Admin Client Secret box during installation.

4. Select **Test**.
If connection to the Proficy Authentication server is established, a message appears, confirming the same.
5. Select **Continue**.
In the **Proficy Authentication Mapping** section, the drop-down list box contains a list of groups in

Historian Proficy Authentication. In the **Filter** box, a list of groups in the existing Proficy Authentication instance appear.

6. In the drop-down list box, select the Historian Proficy Authentication group to which you want to map the existing Proficy Authentication groups.
7. In the **Filter** box, select the check boxes corresponding to the existing Proficy Authentication groups that you want to map.

**Note:**

If a group is already mapped to the Proficy Authentication group that you have selected, the check box is already selected.

8. Select **Map Members**.

A message appears, confirming that the Historian Proficy Authentication group is mapped to the existing Proficy Authentication groups that you have selected.

The existing Proficy Authentication groups are mapped with the Historian Proficy Authentication groups.

Map LDAP Groups with Historian Proficy Authentication


- Ensure that you have set up an LDAP server. For Historian, it is a Windows domain controller or an Active Directory server.
- On your domain (or Active Directory), create users and groups. For the Historian Proficy Authentication server to allow users to log in, you must identify an attribute in the LDAP schema that you can use as the username for Historian. This attribute is used to uniquely identify each user. In addition, since Historian usernames do not contain a space, values of this attribute must not contain a space either.

**Tip:**

Typically, the `sAMAccountName` and `userPrincipalName` attributes in LDAP meet these conditions, supported by Windows Active Directory. By default, the `sAMAccountName` attribute is used in the search filter, but you can change it while installing Historian.

If you want LDAP users to use Web-based Clients, you must map the corresponding Proficy Authentication groups with a Historian Proficy Authentication group, which is created using Web-based Clients installation. If you want to use LDAP via SSL, refer to [Map LDAPS \(LDAP via SSL\) Groups with Historian Proficy Authentication \(on page 164\)](#).

Even if you have mapped LDAP groups in an older version of Historian, you must map the groups again as described in this topic.

1. Double-click the Proficy Authentication IdP Configuration tool icon () , and log in the Proficy Authentication client ID and secret.



Tip:

By default, this icon appears on the desktop after you install Web-based Clients.

The **Identity Providers** page appears.

2. Select the **Map Existing LDAP Groups** check box.
3. In the **Proficy Authentication Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL that you have specified in the Proficy Authentication Base URL box during installation (for example: https://localhost/). For an external or a shared Proficy Authentication instance, enter: https://<Proficy Authentication server name> If using Historian 7.x UAA, enter a value in the following format: https://<Historian 7.x UAA server name>:8443. If you have changed the default port number, provide the correct one. If using Historian 8.x UAA, enter a value in the following format: https://<Historian 8.x UAA server name> (no port number required).
Client ID	Enter the Proficy Authentication server client ID. The default value is admin.
Client Secret	Enter the client secret value that you provided in the User Account and Authentication Service page while installing Web-based Clients. If you use an external Proficy Authentication, enter the client secret of the external Proficy Authentication.

4. Select **Test**.
5. After the connection is successful, select **Continue**.
6. In the **LDAP Connection** section, provide values as specified in the following table.

Box	Description
Base URL	Enter the base URL of the LDAP server (for example, ldap://localhost:389/). Use localhost

Box	Description
	if you have installed Web-based Clients in the domain controller machine. Otherwise, enter: <code>ldap://<domain server>:389</code>
Bind User DN	Enter the distinguished name of the bind user (for example, <code>cn=admin,ou=Users,dc=test,dc=com</code>).
Password	Enter the password of the cn user mentioned in the Bind User DN field. For example, if you have entered <code>cn=admin</code> , provide the administrative password.
User Search Base	Enter the starting point for the LDAP user search in the directory tree (for example, <code>dc=developers,dc=com</code>).
User Search Filter	Enter the subdirectories to include in the search filter (for example, <code>cn={0}</code>).
Group Search Base	Enter the subdirectories to include in the search filter (for example, <code>member={0}</code>).
Group Search Filter	Enter the starting point for the LDAP group search in the directory tree (for example, <code>ou=s-copes,dc=developers,dc=com</code>).

7. Select **Test**.
8. After the connection is successful, select **Continue**.

In the **Proficiency Authentication Mapping** section, the **Proficiency Authentication Group** field contains a list of groups in Historian Proficiency Authentication.



Tip:

You can search for an LDAP group by entering a value in the **LDAP Group Search Filter** box. The default value is `(objectclass=*)`. When you select **Search**, a list of groups based on the values in the **User Search Base** and **Group Search Base** fields appear. If you have a large number of groups, we recommend that you narrow down the search criteria. For example, if you have an LDAP group `cn=visadmins,cn=users,dc=test,dc=com`, you can use



(cn=visaadmins*) to retrieve a list of groups that begin with cn=visaadmins. Ensure that you enclose the value in parentheses.

9. In the **Proficy Authentication Group** field, select the Historian Visualization Proficy Authentication group to which you want to map LDAP groups.
10. In the **Filter** box, select the check boxes corresponding to the LDAP groups that you want to map.



Note:

If a group is already mapped with the Historian Proficy Authentication group that you have selected, the check box is already selected. If you have mapped LDAP groups in an older version of Historian, you must clear the check boxes and select them again.

11. Select **Map Members**.

A message appears, confirming that the Historian Proficy Authentication group is mapped with the LDAP groups that you have selected.

The LDAP groups are mapped with the Historian Proficy Authentication groups.

Map LDAPS (LDAP via SSL) Groups with Historian Proficy Authentication

- Ensure that you have set up an LDAP server. For Historian, it is a Windows domain controller or an Active Directory server.
- Ensure that the LDAP server receives LDAPS communication.
- On your domain (or Active Directory), create users and groups. For the Historian Proficy Authentication server to allow users to log in, you must identify an attribute in the LDAP schema that you can use as the username for Historian. This attribute is used to uniquely identify each user. In addition, since Historian usernames do not contain a space, values of this attribute must not contain a space either.



Tip:

Typically, the `sAMAccountName` and `userPrincipalName` attributes in LDAP meet these conditions, supported by Windows Active Directory. By default, the `sAMAccountName` attribute is used in the search filter, but you can change it while installing Historian.

If you want LDAP users to use Web-based Clients, you must map the corresponding Proficy Authentication groups with a Historian Proficy Authentication group, which is created using Web-based

Clients installation. If you want to use LDAP without SSL, refer to [Map LDAP Groups with Historian Proficy Authentication \(on page 161\)](#).

Even if you have mapped LDAP groups in an older version of Historian, you must map the groups again as described in this topic.

To log in to Trend Client or the Web Admin console, you must enter a username and password. Historian sends these credentials to the LDAP server, which verifies these credentials. If you want these credentials to be sent securely and to the intended LDAP server, you must use LDAPS (that is, LDAP via SSL).

Each LDAP server has a unique certificate containing its name and public key. When the Proficy Authentication server connects to an LDAP client, it receives a certificate to connect to the LDAP server via SSL.


This topic describes the following methods to achieve this:

- **Install the certificate:** Use this method if you have the certificate to access the LDAP server. This method is more secure than the next one.
- **Skip the certificate verification:** Use this method if you do not have the certificate to access the LDAP server. It still encrypts the messages, but you must ensure that you have connected to the intended LDAP server. If the connection is redirected, it can lead to security issues. To avoid this issue, you must compare the certificate that you have received with the expected certificate.



Tip:

If you do not have an SSL certificate, refer to the following article to generate it: <https://docs.microsoft.com/en-us/archive/blogs/microsoftservercertigerteam/step-by-step-guide-to-setup-ldaps-on-windows-server>

1. Double-click the Proficy Authentication IdP Configuration tool icon () , and log in the Proficy Authentication client ID and secret.



Tip:


By default, this icon appears on the desktop after you install Web-based Clients.

The **Identity Providers** page appears.

2. Select the **Map Existing LDAP Groups** check box.
3. In the **Proficy Authentication Connection** section, provide values as specified in the following table.

Box	Description
URL	<p>Enter the authorization server URL that you have specified in the Proficy Authentication Base URL box during installation (for example: https://localhost/). For an external or a shared Proficy Authentication instance, enter: https://<Proficy Authentication server name></p> <p>If using Historian 7.x UAA, enter a value in the following format: https://<Historian 7.x UAA server name>:8443. If you have changed the default port number, provide the correct one. If using Historian 8.x UAA, enter a value in the following format: https://<Historian 8.x UAA server name> (no port number required).</p>
Client ID	Enter the Proficy Authentication server client ID. The default value is admin.
Client Secret	Enter the client secret value that you provided in the User Account and Authentication Service page while installing Web-based Clients. If you use an external Proficy Authentication, enter the client secret of the external Proficy Authentication.

4. Select **Test**.
5. After the connection is successful, select **Continue**.
6. In the **LDAP Connection** section, provide values as specified in the following table.

Box	Description
Base URL	<p>Enter the base URL of the LDAP server (for example, ldaps://localhost:636/). Use localhost if you have installed Web-based Clients in the domain controller machine. Otherwise, enter: ldaps://<domain server>:636</p> <ul style="list-style-type: none"> ◦ If you have a valid certificate, select  (or https), and then upload the SSL certificate. ◦ If you do not have a valid certificate, select the Skip SSL Verification check box.
Bind User DN	Enter the distinguished name of the bind user (for example, cn=admin,ou=Users,dc=test,dc=com).

Box	Description
Password	Enter the password of the cn user mentioned in the Bind User DN field. For example, if you have entered cn=admin, provide the administrative password.
User Search Base	Enter the starting point for the LDAP user search in the directory tree (for example, dc=developers,dc=com).
User Search Filter	Enter the subdirectories to include in the search filter (for example, cn={0}).
Group Search Base	Enter the subdirectories to include in the search filter (for example, member={0}).
Group Search Filter	Enter the starting point for the LDAP group search in the directory tree (for example, ou=s-copes,dc=developers,dc=com).

7. Select **Test**.

8. After the connection is successful, select **Continue**.

In the **Proficy Authentication Mapping** section, the **Proficy Authentication Group** field contains a list of groups in Historian Proficy Authentication.



Tip:

You can search for an LDAP group by entering a value in the **LDAP Group Search Filter** box. The default value is (objectclass=*). When you select **Search**, a list of groups based on the values in the **User Search Base** and **Group Search Base** fields appear. If you have a large number of groups, we recommend that you narrow down the search criteria. For example, if you have an LDAP group cn=visadmins,cn=users,dc=test,dc=com, you can use (cn=visaadmins*) to retrieve a list of groups that begin with cn=visaadmins. Ensure that you enclose the value in parentheses.

9. In the drop-down list box, select the Historian Visualization Proficy Authentication group to which you want to map LDAP groups.

10. In the **Filter** box, select the check boxes corresponding to the LDAP groups that you want to map.

**Note:**

If a group is already mapped with the Historian Proficy Authentication group that you have selected, the check box is already selected. If you have mapped LDAP groups in an older version of Historian, you must clear the check boxes and select them again.

11. Select Map Members.


A message appears, confirming that the Historian Proficy Authentication group is mapped with the LDAP groups that you have selected.

The LDAP groups are mapped with the Historian Proficy Authentication groups.

Restart the GE Operations Hub Proficy Authentication Tomcat Web Server service.

Remove Mapping Between Historian Proficy Authentication Groups and LDAP Groups

If you want to stop users from an LDAP group from using Historian Web-based Clients, you can remove the mapping between the Proficy Authentication group of Historian and LDAP. If you want to stop integration between the Historian Proficy Authentication and LDAP altogether, you must remove the mapping for all the groups of the Proficy Authentication instance.

1. Double-click the Proficy Authentication IdP Configuration tool icon () , and log in the Proficy Authentication client ID and secret.

**Tip:**

By default, this icon appears on the desktop after you install Web-based Clients.

The **Identity Providers** page appears.

2. Select the **Map Existing Proficy Authentication Groups** check box.
3. In the **Proficy Authentication Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL of the LDAP server. For example: <code>https://localhost/</code>
Client ID	Enter the Proficy Authentication server client ID. The default value is admin.

Box	Description
Client Secret	Enter the client secret value that you provided in the User Account and Authentication Service page while installing Web-based Clients. If you use an external Proficy Authentication, enter the client secret of the external Proficy Authentication.

4. Select **Test**.

If connection to the Proficy Authentication server is established, a message appears, confirming the same.

5. In the **LDAP Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the base URL of the LDAP server (for example, ldap://localhost).
Bind User DN	Enter the distinguished name of the bind user (for example, cn=admin,ou=Users,dc=test,dc=com).
Password	Enter the password for the LDAP user ID that searches the LDAP tree for user information.
User Search Filter	Enter the starting point for the LDAP user search in the directory tree (for example, dc=developers,dc=com).
User Search Base	Enter the subdirectories to include in the search (for example, cn={0}).
Group Search Filter	Enter the starting point for the LDAP group search in the directory tree (for example, ou=scopes,dc=developers,dc=com).
Group Search Base	Enter the subdirectories to include in the search (for example, member={0}).

6. Select **Test**, and then select **Submit**.

If connection to the LDAP server is established, a message appears, confirming the same.

7. Select **Test** again, and then select **Continue**.

In the **LDAP Mapping** section, the drop-down list box contains a list of groups in Historian Proficy Authentication. In the **Filter** box, a list of LDAP groups appears.

8. In the drop-down list box, select the Historian Proficy Authentication group whose mapping you want to remove.


In the **Filter** box, check boxes for the Proficy Authentication groups that are mapped to the selected Historian Proficy Authentication group are selected.

9. In the **Filter** box, clear the check boxes corresponding to the LDAP groups for which you want to remove the mapping.
10. Select **Map Members**.
The mapping between the Proficy Authentication groups of Historian Proficy Authentication and LDAP is removed.
11. Repeat steps 8 through 10 for all the Historian Proficy Authentication groups for which you want to remove the mapping.

Mapping between the Proficy Authentication Groups of Historian and LDAP has been removed.

Remove Mapping Between Proficy Authentication Groups of Historian and an Existing Proficy Authentication Instance

If you want to stop users from a Proficy Authentication group of an existing Proficy Authentication instance from using Historian Web-based Clients, you can remove the mapping between the Proficy Authentication group of Historian and the existing Proficy Authentication instance. If you want to stop integration between the Historian Proficy Authentication and the existing Proficy Authentication instance altogether, you must remove the mapping for all the groups of the Proficy Authentication instance.

1. Double-click the Proficy Authentication IdP Configuration tool icon () , and log in the Proficy Authentication client ID and secret.



Tip:

By default, this icon appears on the desktop after you install Web-based Clients.

The **Identity Providers** page appears.

2. Select the **Map Existing Proficy Authentication Groups** check box.
3. In the **Proficy Authentication Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL that you specified in the Proficy Authentication Base URL box during installation (for example, https://localhost).
Client ID	Enter Admin as client ID.
Client Secret	Enter the client secret configured for the OAuth client that you specified in the Admin Client Secret box during installation.

4. Select **Test**.

If connection to the Proficy Authentication server is established, a message appears, confirming the same, and the **Continue** button is enabled.

5. Select **Continue**.

In the **Proficy Authentication Mapping** section, the drop-down list box contains a list of groups in Historian Proficy Authentication. In the **Filter** box, a list of groups in the existing Proficy Authentication instance appear.

6. In the drop-down list box, select the Proficy Authentication group for which you want to remove the mapping.

In the **Filter** box, check boxes for the Proficy Authentication groups that are mapped to the selected Historian Proficy Authentication group are selected.

7. In the **Filter** box, clear the check boxes corresponding to the Proficy Authentication groups for which you want to remove the mapping.

8. Select **Map Members**.

The mapping between the Proficy Authentication groups of Historian Proficy Authentication and the existing Proficy Authentication instance is removed.

9. Repeat steps 6 through 8 for all the Historian Proficy Authentication groups for which you want to remove the mapping.

Mapping between the Proficy Authentication groups of Historian and the existing Proficy Authentication instance has been removed.

Change the Log Levels of Proficy Authentication

1. Access the `log4j.properties` file in the following folder: `C:\Program Files\GE`

`\Operations Hub\uaa-tomcat\webapps\uaa\WEB-INF\classes`

2. For each module, select one of the following log levels depending on your requirement:

- TRACE
- DEBUG
- INFO
- WARN
- ERROR
- FATAL
- OFF

3. If you want to disable Tomcat logging:

a. Stop the GE Operations Hub Proficy Authentication Tomcat Web Server service.

b. In the `C:\Program Files\GE\Operations Hub\uaa-tomcat\bin` folder, rename the `tomcat8w.exe` file `UaaTomcat.exe`, and run this application as an administrator.

- c. Select **Logging**.
 - d. Remove the auto keyword from the Redirect Stdout and Redirect Stderr labels.
 - e. Start the GE Operations Hub Proficiency Authentication Tomcat Web Server service.
4. If you want to change the Tomcat log level:
- a. Stop the GE Operations Hub Proficiency Authentication Tomcat Web Server service.
 - b. Access the `context.xml` file located in the `C:\Program Files\GE\Operations Hub\uaa-tomcat\conf`.
 - c. In the Context tag, add: `swallowOutput="true"`
 - d. Access the `logging.properties` file in the same folder, and set the **2localhost.org.apache.juli.AsyncFileHandler.level** to one of the following values, which are in the order of less verbose to more verbose:
 - SEVERE
 - WARNING
 - INFO
 - CONFIG
 - FINE
 - FINER
 - FINEST
 - ALL
 - e. Start the GE Operations Hub Proficiency Authentication Tomcat Web Server service.

Migrating Historian Data

Migrating the Alarms and Events Data

If you have upgraded Historian, you must migrate the alarms and events data as well. Only then you can retrieve the data.

The steps to migrate depend on the Microsoft SQL version in which the alarms and events data is stored:

- If using Microsoft SQL 2008 or later, you can install Historian and its components, install a supported version of Microsoft SQL, and then migrate the data.
- If using a version earlier than Microsoft SQL 2008, you must first migrate the data to Microsoft SQL 2008, and then migrate it to a supported version of Microsoft SQL.

To migrate data, you can choose one of the following options:

- **Before upgrading to the latest version of Historian:** In this case, you can use Historian Administrator of the older version of Historian to migrate the data.
- **After upgrading to the latest version of Historian:** In this case, you can use the Proficy Alarm Database Migration tool, which is provided with Historian.

This section describes how to migrate data using the migration tool.

Workflow for Migrating Alarms and Events Data

If the alarms and events data is currently in Microsoft SQL 2008 or later:

1. Install the following components on the target machine in the given sequence:
 - a. [Historian \(on page 44\)](#)
 - b. [Alarms and Events \(on page 90\)](#)
 - c. [Collectors \(on page 92\)](#)
 - d. [Client Tools \(on page 100\)](#)
 - e. [Standalone Help \(on page 156\)](#)
2. [Back up the alarms and events data \(on page 174\)](#).
3. Install Microsoft SQL on the target machine. Refer to [Software Requirements \(on page 31\)](#) for a list of supported versions.
4. Restore the data that you have backed up to Microsoft SQL.
5. As needed, perform calculations on the migrated data. Ideally, you must create an archive already to store the calculated data. For unsolicited calculation tags, migration of data will cause the calculation to be triggered automatically for the time associated with the migrated data points. Archives will potentially grow beyond the configured default size. To avoid this issue, adjust the value for the `DataIsReadOnlyAfter` field on the **Security** section of the **Data Store Maintenance** page of Historian Administrator (or the `ActiveHours` property) so that the value is large enough to contain the calculated data. By default, this value is 1 month.

If the alarms and events data is currently in a version earlier than Microsoft SQL 2008:

1. Using Microsoft SQL Server Management Studio, back up the alarms and events data. If the database is large, consider taking a partial backup instead of a full backup.
2. Install Microsoft SQL Server 2008 on the target machine.
3. Restore the data that you have backed up in step 1.
4. In Microsoft SQL Server Management Studio, under **Databases**, right-click the database that you have restored, and then select **Properties > Options**.
5. In the **Compatibility level** field, select **SQL Server 2008**.
6. Install the following components on the target machine in the given sequence:

- a. [Historian \(on page 44\)](#)
 - b. [Alarms and Events \(on page 90\)](#)
 - c. [Collectors \(on page 92\)](#)
 - d. [Client Tools \(on page 100\)](#)
 - e. [Standalone Help \(on page 156\)](#)
7. [Back up the alarms and events data \(on page 174\)](#) that you have restored in step 3.
 8. Install a supported version of Microsoft SQL on the target machine. Refer to [Software Requirements \(on page 31\)](#) for a list of supported versions.
 9. Restore the data that you have backed up in step 7 to Microsoft SQL.
 10. As needed, perform calculations on the migrated data. Ideally, you must create an archive already to store the calculated data. For unsolicited calculation tags, migration of data will cause the calculation to be triggered automatically for the time associated with the migrated data points. Archives will potentially grow beyond the configured default size. To avoid this issue, adjust the value for the `DataIsReadOnlyAfter` field on the **Security** section of the **Data Store Maintenance** page of Historian Administrator (or the `ActiveHours` property) so that the value is large enough to contain the calculated data. By default, this value is 1 month.

Back Up the Alarms and Events Data

Install the following components in the given sequence:

1. [Historian \(on page 44\)](#)
2. [Alarms and Events \(on page 90\)](#)
3. [Collectors \(on page 92\)](#)
4. [Client Tools \(on page 100\)](#)
5. [Standalone Help \(on page 156\)](#)

If, however, the alarms and events data is currently in a version earlier than Microsoft SQL 2008, you must first migrate the data to Microsoft SQL 2008, and change the compatibility level to **SQL Server 2008**.

1. Go to the `<Historian installation folder>\Proficy DataBase` folder, and open the `Proficy.Historian.AandE.Migration.exe` file.
The **Backup Existing Alarms and Events** window appears.
2. In the **Time Range** section, in the **From** and **To** fields, select the start time and end time of the backup duration.
We recommend that you select small duration if you have many alarms. If you want to migrate the alarms in blocks of time, choose the oldest alarms first.
3. In the **Database Name** field, enter the name of the database that you want to back up. Typically, this will be the same as the Microsoft SQL server you are using.

4. Depending on whether you want to use Windows credentials or Microsoft SQL credentials, select either **Use Windows Authentication** or **Use SQL Authentication**, respectively.
5. In the **User Id** and **Password** fields, enter the login credentials. Provide the username of a user who has the permission to connect and back up alarms.
6. In **Backup Folder Path** field, provide the absolute path, including the file name, to store the backed up alarms (for example, c:\temp\March2010.bak). You can enter the path of a local file or a remote one, depending on whether the Microsoft SQL server is installed on the local machine or a remote machine.
7. Select **Test Connection** to check if the source database is active and the information is accurate. The **Begin Backup** button is activated.
8. Select **Begin Backup**.
The alarms and evens data is backed up. The count of the rows that are backed up appears.

Install a supported version of Microsoft SQL, and [restore the data \(on page 175\)](#) that you have backed up. Refer to [Software Requirements \(on page 31\)](#) for a list of supported versions.

Restore the Alarms and Events Data

Install Microsoft SQL. Refer to [Software Requirements \(on page 31\)](#) for a list of supported versions.

1. Go to the *<Historian installation folder>\Proficy DataBase* folder, and open the *Proficy.Historian.AandE.Migration.exe* file.
The **Backup Existing Alarms and Events** window appears.
2. Select **Migrate Alarms and Events Backup**.
3. In the **Backup Folder Path** field, provide the absolute path of the file (including the file name) in which you want to restore the data (for example, c:\temp\March2010.bak). You can enter the path of a local file or a remote one, depending on whether the Microsoft SQL server is installed on the local machine or a remote machine.
4. In the **Database Name** field, enter the name of the database that you want to back up. Typically, this value is the same as the Microsoft SQL server you are using.
5. Depending on whether you want to use Windows credentials or Microsoft SQL credentials, select either **Use Windows Authentication** or **Use SQL Authentication**, respectively.
6. In the **User Id** and **Password** fields, enter the login credentials. Provide the username of a user who has the permission to connect and back up alarms.
7. Select **Test Connection** to check if the source database is active and the information is accurate. The **Begin Migrator** button is activated.
8. Select **Begin Migrator**.
The alarms and evens data is restored. The count of the rows that are restored appears.

Using the Migration Tool

The IHA Migration Tool (`MigrateIHA.exe` for 32 bit or `MigrateIHA_x64.exe` for 64 bit) allows you to migrate data up to 30 years old if the data is already stored in `IHA` files from any version of Historian. Use the Migration Tool to move data from one archiver to another when you cannot simply restore the `IHA` in Historian Administrator.

The Migration Tool opens an `IHA` file as a binary data file and reads the raw samples from it. Those raw samples are then written to a destination archiver, in a similar way to how an OPC collector or File collector would write data. Any errors returned from the data archiver are reported in the main window and repeated in the log file.



Note:


- You can migrate UserDefined types, MultiField tags, and Array tags.
- When you are migrating the data stores, the source data store is created in the destination.
- Using this Migration Tool, you can upgrade from two previous versions of Historian to the latest version.
- The performance of this tool is impacted with the addition of Client Manager and Configuration Manager. For best performance, use this on a Single Server install only.

Migrating Historical Data

You need to run this tool as an administrator to migrate and create the log files in the `C:\` directory.

To migrate historical data stored in `IHA` files from any version of Historian:

1. In the `Historian` folder, double-click the Migration Tool executable (`MigrateIHA.exe` for 32-bit or `MigrateIHA_x64.exe` for 64-bit) to open the IHA Migration Utility.

The icon for the executable looks as follows: .

2. Select **Configure Options** from the **Options** menu.
3. Enter or modify any specific configuration information.
When choosing an `IHC` file, do not specify one currently in use by the Data Archiver. (For more information, see [Configuring Migration Options \(on page 177\)](#).)
4. Select **File > Migrate Historical Data** .
The **Select Historical Data File(s)** window appears.
5. Select a historical file and select **Open**.

Refer to the **IHA Migration Utility** main page for information on the progress of the migration and any encountered errors.



Note:

The IHA Migration Utility page only displays the most recent lines of the log file. For the full set of logged messages, refer to the log file, typically located in `C:\IHAMigration.Log`.

6. Optionally, perform these steps:

a. You can upgrade the older version's archive files to the latest version by selecting the bulk upgrade option.

Stop the Data Archiver service and select **File > Bulk Upgrade Historical Data**.

If you do a bulk upgrade of historical data immediately after you install the latest version on Historian, then save on upgrading while the system reboots.

b. To clear the log messages displayed in the page, select **File > Clear Display**.

c. To view the logs saved in the `IHAMigration.log` file, select **File > View Log File > ..**

Configuring Migration Options

1. In the Migration tool (`MigrateIHA.exe` for 32 bit or `MigrateIHA_x64.exe` for 64-bit), select **Options > Configure Options**.

The **Migration Options** window appears showing the default server information and the default migration options.

2. Enter options the following options.

Related reference

[Server Pane \(on page 178\)](#)

[Options Pane \(on page 179\)](#)

[Tags to Migrate Pane \(on page 179\)](#)

[Time to Migrate Pane \(on page 179\)](#)

Server Pane

Field	Description
Server	The default server (set during installation). If you do not want to write data to the default server, enter the desired server in this field.
Username and Password	If you have created and established Security Groups in your Historian Security Environment, you may need to enter the user name and password here. By default, if you do not supply any information, the current logged in user will be used in security checking.

Options Pane

It is always advisable to take a copy of the configuration file and work on the copy rather than working on the original file.

Tags to Migrate Pane

Option	Description
Migrate All Tags	Select this option to migrate all the tags from the selected archiver.
Migrate only tags that exist in destination	Select this option to migrate all the tags that exists in the source destination.
Migrate using tag mask	Select this option to migrate tags with the mask specified. You can specify an exact tag name to migrate that tag only.
Migrate only tags that exist in source config file	To migrate the tags that are present only with the source config file.

Time to Migrate Pane

Option	Description
Use IHA TimeFrame	Select this option to migrate all the tags which has the IHA time frame.
Use Below TimeFrame	Select this option to migrate all the tags in the specified time frame. You need to specify the Start Date/Time and End Date/Time if you select this option.

Data Migration Scenarios

You can migrate tags and their data on the same Historian Server or between servers. When migrating your data, consider the following guidelines:

- Get new collection working first

When the data is collected from the collectors or the API programs, then you should consider adding the tag definitions into the destination server and directing data to be written there before you start migration, because migration may take several hours or days.

- Migrate data from oldest to newest

It is advisable to migrate the oldest data first and then the newest, to make the optimal use of archive space.

- Pay attention to TagID

Every tag in Historian 4.5 and above has a property called TagID, that uniquely identifies it and allows data retrieval to locate the data. Even if you have a tag of with the same name in another archiver, that tag has a different TagID and is considered as a different tag. You can see the TagID of a tag in the Excel Tag Export. Preserve that number when moving a tag from one system to another.

The following are commonly used scenarios while migrating data on the same Historian server or between servers.

- Migrating a Tag and its data from one data store into another data store.
- Merging a Historian Server into an existing data store on another machine. .

Migrating a Tag and its Data

If you want to separate a single large user data store of tag into multiple smaller data stores on the same machine, and if your software license allows it, then you should assign the tag to the new data store and then migrate the data.

Consider when data is collected for the year 2009 in `Tag1`. The collected data is archived in the default User data store. If you want to move `Tag1` residing in the `User` data store to another data store, (for example, the `Motor` data store), then you must create the `Motor` data store if it does not already exist and if your license allows it.

The next step is to change the data store of the tag. You can change the data store of the tag either using Historian Administrator or using Excel Tag Import. The new incoming data gets collected in the Motor data store. If you do a raw data query, you will get only the latest data and the previous data will not be available. To get the old data, you must migrate the data residing in the `User` data store to the `Motor` data store.

To migrate a tag and its data from one data store to another data store on the same server:

1. Use `iharchivebackup -c` to make a backup of the `.ihc` file.
The backup of the Config file is automatically created in the `Archives` folder.
2. In Historian Administrator, back up each archive from oldest to newest.

3. Launch the Migration Tool (`MigrateIHA.exe` for 32-bit or `MigrateIHA_x64.exe` for 64-bit) using Administrator privileges.
4. Select **Options > Configure Options**.
5. In the **Server** pane, enter the **Server name**.
6. In the **Options** pane, enter the **IHC File** path in the **Config File** path field, using the browse button. This is the path to the IHC backup that you made in step 1.
7. In the **Tags to Migrate** pane, select the **Migrate Using Tag Mask** option and enter the **Tag Name** you moved to the new data store.
8. In the **Time to Migrate** pane, ensure the **Use IHA TimeFrame** option is selected.
9. Select **File > Migrate Historical Data**.
10. Select the archive file that you backed up in Step 2 and monitor the progress of the migration. When the migration is complete, query the data to see the migrated data can be queried. Repeat with the remaining archives from oldest to newest.

As needed, perform calculations on the migrated data. Ideally, you must create an archive already to store the calculated data. For unsolicited calculation tags, migration of data will cause the calculation to be triggered automatically for the time associated with the migrated data points. Archives will potentially grow beyond the configured default size. To avoid this issue, adjust the value for the `DataIsReadOnlyAfter` field on the **Security** section of the **Data Store Maintenance** page of Historian Administrator (or the `ActiveHours` property) so that the value is large enough to contain the calculated data. By default, this value is 1 month.

Merging a Historian Server

A typical scenario is to merge a Historian Server into an existing data store on another machine.

If your system architecture has evolved from multiple smaller servers into fewer large archives, you can eliminate the smaller machines while preserving all your tag configuration and collected data.

Consider the following example. You have two machines, Machine A and Machine B. Machine A is running current or any earlier version of Historian and has 100 tags and 10 archive files. The data of these tags are collected from the collector and is being queried by users. Machine B is running the current version of Historian.

**Note:**

- This example does not include Alarm migration. If Machine A was being used to store alarms, then you need to migrate those before eliminating Machine A.
- You cannot migrate tags with Enumerated Data Sets. If you want to migrate data for Enumerated Data Sets, then you must create the Enumerated Data Sets in Historian Administrator or Microsoft Excel and then migrate the tags.
- To migrate tags which are condition based triggers, then you must create the condition-based triggers for that tag in Historian Administrator or Microsoft Excel and then migrate the tags.

You can migrate data only if the file format of the archive files format is `.IHA`. If the back-up archive is in `.zip` format, extract the `zip` files and copy all the `.IHA` files separately in a folder.

1. Before migrating, copy the `.IHC` and all the `.IHA` files from Machine A to Machine B.
2. Launch the Migration Tool (`MigrateIHA.exe` for 32-bit or `MigrateIHA_x64.exe` for 64-bit) with Administrator privileges.
3. Select **Options > Configure Options**.
4. In the **Server** pane, enter the **Server name**.
5. In the **Tags to Migrate** pane, ensure that the **Migrate All Tags** option is selected
6. In the **Options** pane, enter the **IHC File** path in the **Config File** path field, using the browse button. The path you enter is the path to the `.IHC` file brought over from Machine A.
7. In the **Time to Migrate** pane, ensure the **Use IHA TimeFrame** option is selected.
8. Ensure **Throttle Output** is selected.
9. To migrate the data, select **File > Migrate Historical Data** and select the archive file that has the oldest data.
The tags and data are migrated to the default data store in time slices. The **MigrateIHA** window displays the progress and any Tag Add or Data Add errors are displayed in the log file. You can estimate the remaining time by watching the progress.
10. Repeat the previous steps for each of the remaining archives, from oldest to newest data.
11. Add the collector to the Historian Server on Machine B.
See the *Adding a Data Collector to an Historian Server* topic in *Data Collectors - General*.

Migration Tool Command-Line Syntax

Command Syntax

- For 32-bit:

```
MigrateIHA.exe "<IHA file name with full path>" "<IHC filename with full path>"
```

- For 64-bit:

```
MigrateIHA_x64.exe "<IHA file name with full path>" "<IHC filename with full path>"
```

Command-line Options

Option	Description
<code>/NOTHROTTL</code>	This does not throttle any part of the migration process, but may impact resources on the server. Optionally, you can remove this switch as required. By default, throttling is rated at 5000 events per second.
<code>/NOMESSAGES</code>	This does not migrate messages into the newly created archive. Using this switch may or may not reduce the size of your archives, depending on the number of messages stored in the archive. By default, messages are migrated if this switch is not used.
<code>/EXISTINGTAGS</code>	This will migrate data for only those tags that exist in the destination archiver.
<code>/b</code>	This option of the <code>start.exe</code> file allows the IHA Migration tool to start without opening a new window for each instance. If you are migrating a pre 4.5 IHA file you will need to have the IHC file for that IHA and specify the IHC file in the Options window or on the command line. Otherwise, you will get a warning message.
<code>/wait</code>	This option of the <code>start.exe</code> file allows each instance of the IHA Migration tool to complete the migration before starting the next migration in the sequence.
<code>/NOIHC</code>	This option skips verifying for IHC file and proceed with the migration. IHC file is not required, if batch command have <code>/NOIHC</code> option.

Notes

- If you are migrating from a command line, provide IHC file, else, use /NOIHC option to omit the IHC file.
- If you do not have the IHC or you are not sure you have the correct IHC then you should use the pre-4.5 version of MigrateIHA to migrate the IHA. Otherwise, the data will not migrate correctly.
- You should keep a copy of the original IHA file.
- The IHC must contain all the tags that are in the IHA file, so use the most current IHC you have.
- You must use double quotes when you enter the IHA and IHC file even if you do not have spaces in your file path or file name.
- Migrating an IHA will upgrade it to 4.5 format.
- If you are migrating a 4.5 IHA you should provide the IHC file in the Options window but if you do not have the IHC you can safely continue past the warning message.

Creating a Batch File to Migrate Multiple IHA Files

The IHA Migration utility migrates only one archive at a time by design. However, if you need to add more than one archive at a time, you can create a batch file to automate multiple archive merges.

When creating a batch file you need to provide the batch file with a logical name and save the batch (.bat) file in a location that can be easily accessed using the command prompt.



Note:

When migrating any archive, you should start with the archive with the oldest data first, followed by newer data, in sequence, to minimize the amount of disk space used in the Data Archiver.

For example:

```
cd c:\Program Files\Historian
start /b /wait migrateiha /NOTHROTTLE /NOMESSAGES
"c:\Historian Data\Backups\server_Archive001.iha"
"c:\Historian Data\Backups\server_Config.ihc".
```

Interoperability of Historian Versions

Interoperability guidelines for Historian versions include:

- Historian Collectors below v6.0 can write to Historian v7.0 Archivers; however, since the earlier collector versions cannot automatically connect to a mirror, users need to point those collectors to the mirror system.
- Historian Clients below v6.0 can retrieve data from Historian v7.0 Archivers.
- Historian v7.0 or later Clients can retrieve data from a single Historian Data Archiver below v6.0.
- Historian v7.0 or later Collectors can write to a single Historian Data Archiver below v6.0.
- An SDK program built on an Historian v7.0 or later node does not run on an Historian below v6.0.
- An SDK program that you created in Historian below v7.0 must be rebuilt on a computer with Historian v7.0 or later if you want to run it on that version.
- It is recommended that you use consistent versions of client and server applications. If you do use different client and server versions of the Historian, regularly back up all archives and tag configurations.

**Note:**

To determine the version of the server, client, and SDK, select the **About** link in Historian Administrator. The version of the Historian installer can be seen in the **Control Panel / Uninstall programs**; this version is different from the Historian core version seen in Historian Administrator **About** link.

Migrate User Authentication Data from Historian to Common Proficy Authentication Service

Starting Historian 8.0 version, you can use the common Proficy Authentication service.

**Note:**

You can either choose the common Proficy Authentication deployed by any other products such as, Operations Hub, Plant Apps; or the common Proficy Authentication deployed by Historian.

To use the common Proficy Authentication service, you must migrate the Proficy Authentication data should from Historian to the new local or external Proficy Authentication.

To enable this migration of data the `uaa_config_tool` is introduced.

**Note:**

- While migrating Proficy Authentication details, we are setting default password as user123 for all the users. You should change it using Proficy Authentication config tool once migration is done.
- While setting up new password, it may ask you to enter the port number. By default, the port number is 443. If you have provided a different value in the Public https port field in the TCP port assignments page while installing Web-based Clients, you must provide that value.
- Using this tool, you can back up the Proficy Authentication data only for Historian 7.2 or earlier. And, you can migrate the data to Historian 8.0 or later.

**Important:**

Back up the data before upgrading to the latest version of Web-based Clients.

It includes the following tasks:

1. Back up Historian Proficy Authentication data.
 2. Migrate the data to an existing common Proficy Authentication service.
1. Open Command Prompt.
 2. Mount the ISO and navigate to the Utilities folder where the `uaa_config_tool.exe` file is located. After installation, `uaa_config_tool` is available in the following folder as well: `<installation drive of Historian>\Program Files\GE Digital\Historian Config`

**Important:**

You should back up the data before upgrading to 8.0 (Web-based Clients)

3. Enter the following command to take a back up of the data:

```
C:\ uaa_config_tool.exe backup_data -d "<destination folder>"
```

`<destination folder>` is the location where you want to save the back up files. Note that you must enter the value in quotes.

**Note:**

You may be prompted to enter the password twice for Historian Database and Proficy Authentication. Enter the password as GEIP123User

Back up is generated and the data is saved in the destination folder.

4. Copy the backup files to the machine where Web-based Clients are installed.
5. Enter the following command to migrate the data:

```
uaa_config_tool.exe migrate_data -h <host-addr> -m <portnum> -u <username> -s <secret> -l
"<location path of backup files>"
```

Example: `uaa_config_tool.exe migrate_data -h vmhistwin2016 -m 443 -u admin -s gowt43df -l "c:\myuaabackupfiles"`

**Note:**

While migrating Proficy Authentication details, it may ask for port number at migrating historian database. The default value is 8432. If, however, you have provided a different value in the **Historian database port** field in the **TCP port assignments** page while installing Web-based Clients, provide that value.

Value	Description
<host-addr>	Address of the host or destination where you want to migrate the data.
<portnum>	Port number of the destination.
<username>	Username
<secret>	Client Secret
<location path of backup files>	Source location where the data is backed up.

- The data is migrated to the destination that is, common Proficy Authentication service.
- The `umtlog` file is generated containing the details about backup and migration for users and groups.
- The `User_migration_report` is generated which contains the migration status of the user data.

**Note:**

Creation and migration of users and groups can fail if the user or group already exists in the destination.

If user migration fails, you can change the username in the backup file and repeat Step 5.

Implementing Historian Security

Implementing Historian Security

Historian is a high performance data archiving system designed to collect, store, and retrieve time-based information efficiently. By default, access to these Historian archives, tags, and data files is available to any valid operating system user account. In this default environment, all users are allowed to read, write, change, and delete archives, tags, or data files in Historian Administrator, SDK, migration tools, and Excel Add-In. However, you may want to make these features and data available only to authorized personnel. You can do this by creating and defining Historian security groups in your Windows Security.

Historian includes an Electronic Signature and Electronic Records security feature. This option provides installations related to 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. For more information on the Electronic Signature and Electronic Records feature, refer to [Historian in a Regulated Environment \(on page 221\)](#).

To ensure a secure environment when using Historian security, do not create any local user accounts unless Historian is set up on a standalone machine.

Whether or not you use Historian security, make sure that you disable Guest accounts on your computer to limit access to valid Windows user accounts.

To run Proficy Authentication commands, refer to [Managing Proficy Authentication Users Using the Configuration Tool \(on page 221\)](#).

About Protecting Your Process

If you want to restrict access to Historian archives, files, and tags, or protect your data files from unauthorized changes, you can enable Historian security. Using security is optional and is disabled by default. By enabling security, you can restrict access to:

- Modifying data using Excel Add-In
- Updating security for individual tags or groups of tags

- Creating, modifying, and removing tags
- Tag protection (adding, modifying, removing, and so on) can be applied at a global level to all tags or at the individual tag level.

Refer to [Implementing Tag Level Security](#) for more information.

- Reading data in the iFIX Chart object, Excel Add-In, and Migration Utilities
- Writing data
- Starting and stopping collectors
- Creating and deleting collectors
- Creating, modifying, and deleting archives

Historian uses the operating system security groups to create a security structure. You can enable security for a particular set of functions by adding specific Historian Security Groups to your groups. You can also add security groups to your domain controller.

By defining one or all of the groups, you begin to set up a security structure. Refer to the *Historian Security Groups* section for more information on the Historian Security Groups available.

Strict Authentication

With Historian's strict user account authentication features, `Enforce Strict Client Authentication` and `Enforce Strict Collector Authentication`, you can control access to the Historian server and safeguard user account credentials.

With strict authentication enabled, only known user accounts configured on the Data Archiver server computer will be able to access a Historian server. Similarly, enabling strict collector authentication enforces the same requirement for incoming collector connections.

For an account to be known at the Data Archiver, it has to exist on that archiver as a local account or exist on a Domain Controller available to the data archiver. Historian will access the local accounts or Domain Controller via Microsoft's Security Support Provider Interface (SSPI) and this involves having a Kerberos server setup optionally to assist in account validation.

By default, strict client and collector authentication is enabled on new installations to maximize security. When upgrading from a previous version of Historian, strict client and collector authentication is disabled to allow compatibility with older clients or collectors that cannot be upgraded concurrently.

It is recommended that all clients and collectors receive timely upgrade to the latest version, which permits enabling both strict client and collector authentication on the server for the highest security configuration.

By treating clients and collectors separately, it is possible to accommodate new and legacy authentication during the upgrade process. However, upgrading all clients and collectors to the latest version immediately will achieve a high level of security. The two options, Enforce Strict Client Authentication and Enforce Strict Collector Authentication, permit flexibility during the upgrade process by selectively accommodating legacy clients and collectors.

Local and Domain Security Groups:

You can choose local or domain security groups to access Historian. To do so, in **Historian Administrator > Data Stores > Security**, select **Use Local** or **Use Domain**. The following table provides recommended group to use based on the machine configuration and the security group of the logged-in user.

Machine Configuration	Security Group of the Logged-In User	Recommended Security Group
Workgroup	Local	Local
Domain	Local	Domain For domain machines, we recommend that you log in with a domain-level user and create security groups in the domain controller machine.
Domain	Domain	Domain

Strict Authentication Options:

This 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 OLE DB program, user written programs, or any other Proficy software.

Strict Client Authentication	Strict Collector Authentication	Comment
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.

Trusted Connections in Distributed Historian Service Environment:

This trusted connection works only in the Domain environment and it is enabled by default.



Note:

If you are adding a mirror copy to an existing node, make sure that both the nodes are in the same domain.

If you want to work in the workgroup setup, contact Online technical support & GlobalCare:www.digitalsupport.ge.com.

Disabling Strict Client and Collector Authentication

To permit older versions of clients and collectors to access a Historian 7.0 (or later) server, disable strict client and collector authentication.

1. Open the page and select **DataStore Maintenance Security**.
2. In the **Global Security** section:
 - Select the **Disabled** option button for **Enforce Strict Client Authentication**.
 - Select the **Disabled** option button for **Enforce Strict Collector Authentication**.

Security Strategy Guidelines

When you begin to implement security, you should first define a clear strategy. Consider the following when beginning to set up your security strategy:

- If you disabled the Guest account, a user must provide a valid username and password even if no groups are created.
- Protection is only provided for the functional areas for which you have built the associated Historian Security Groups.

- If you only choose to define some of the security groups, all users still have all access to any uncreated groups. All users are still assumed to be a member of a group unless that group has been created, with the exception of iH Audited Writers group. You must add the iH Audited Writers group to the Windows security groups so that a user can become a member of this group.

For example, if you elect to define the iH Security Admins group and iH Archive Admins group, both the members associated with those defined groups and all other valid users still have access to such functions as creating and modifying tags until you create the iH Tag Admins security group.

- If you implement any Historian Security groups, you must first add and define the iH Security Admins group.



Note:

If you do not create and define the iH Security Admins group, all valid users are assumed to be members of this group. This membership overrides any other security group that you set.

See also [Historian Security Groups \(on page 193\)](#).

Setting Historian Login Security

Use Historian Login Security settings if you want to validate users at the Data Archiver, instead of at the client. By applying these settings, users and applications are forced to provide a user name and password at connect time so that the archiver can validate them. For example, users in the security group such as `iH Security Admins` will be checked by the Archiver.

For Historian Login Security settings, you can view and set the property from the HistorianSDKsample server properties. The current setting is shown in the data archiver `SHW` file.

Historian Login Security property is available only in Historian SDK.

To set login security using the Historian SDK:

1. Run the SDK sample.
2. Connect to a server.
3. Select the server in the list box.
The **Server Properties** window appears.
4. On the right side of the window, locate the **AllowClientValidation** setting. By default, this value is set to `TRUE`. Select to set to `FALSE`, and select **OK**.

Historian Security Groups

Historian provides the following security groups:

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 Tag Admins are not responsible for setting Tag Level Security. This task can only be performed by an iH Security Admins. For more information on setting Tag Level Security, refer to the *Implementing Tag Level Security* section.

iH Archive Admins

Allowed to create, modify, remove, backup, and restore archives.

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.

Tag, archive, and collector changes log messages regardless of whether the user is a member of the iH Audited Writers Group.

iH Readers

Allowed to read data and system statistics. Also allowed access to Historian Administrator.

Use this table to identify the types of user groups you need to create and define in your security system.

Function	iH Security Admins	iH Un-Audited Writers	iH Un-Audited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
Create Tags: <ul style="list-style-type: none"> • Excel Add-In • SDK • Historian Admins • File collector 	X						X	
Remove Tags: <ul style="list-style-type: none"> • Historian Admins • SDK 	X						X	
Modify Tags:	X						X	

Function	iH Security Admins	iH Un-Audited Writers	iH Un-Audited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
<ul style="list-style-type: none"> • Excel Add-In • SDK • Historian Admins • File collector 								
Modify Archive Security: <ul style="list-style-type: none"> • SDK • Historian Admins 	X							
Backup Archive: <ul style="list-style-type: none"> • SDK • Historian 	X					X		

Function	iH Security Admins	iH Un-Audited Writers	iH Un-Audited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
an Admins								
Restore Backup: <ul style="list-style-type: none"> • SDK • Historian Admins 	X					X		
Create Archive: <ul style="list-style-type: none"> • SDK • Historian Admins 	X					X		
Start/Stop Collector: <ul style="list-style-type: none"> • SDK • Historian 	X							X

Function	iH Security Admins	iH Un-Audited Writers	iH Un-Audited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
Admins • Mission Control (iFIX)								
Browse Collector: • Historian Admins	X							X
Read Data: • Chart Object • Excel Add-In • SDK	X				X			
Write Data (UnAudited):	X	X	X					

Function	iH Security Admins	iH Un-Audited Writers	iH Un-Audited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
<ul style="list-style-type: none"> • Excel Add-In • SDK 								
Write Data (Audited): <ul style="list-style-type: none"> • Excel Add-In • SDK 	X			X				
Modify Data: <ul style="list-style-type: none"> • Excel Add-In • SDK 	X	X	X	X				
Update Security for Tag: <ul style="list-style-type: none"> • Excel Add-In • SDK • History 	X							

Function	iH Security Admins	iH Un-Audited Writers	iH Un-Audited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
ri-an Admins								
Migrate: • Migration Tools	X							
Login Connection Messages	X	X		X	X	X	X	X
Recalculate Data	X		X	X				X

Configure Internet Protocol Security (IPSEC)

Historian supports encryption based on Internet Protocol Security to secure traffic between various Historian components and collectors without the need to use VPN or other security protocols.

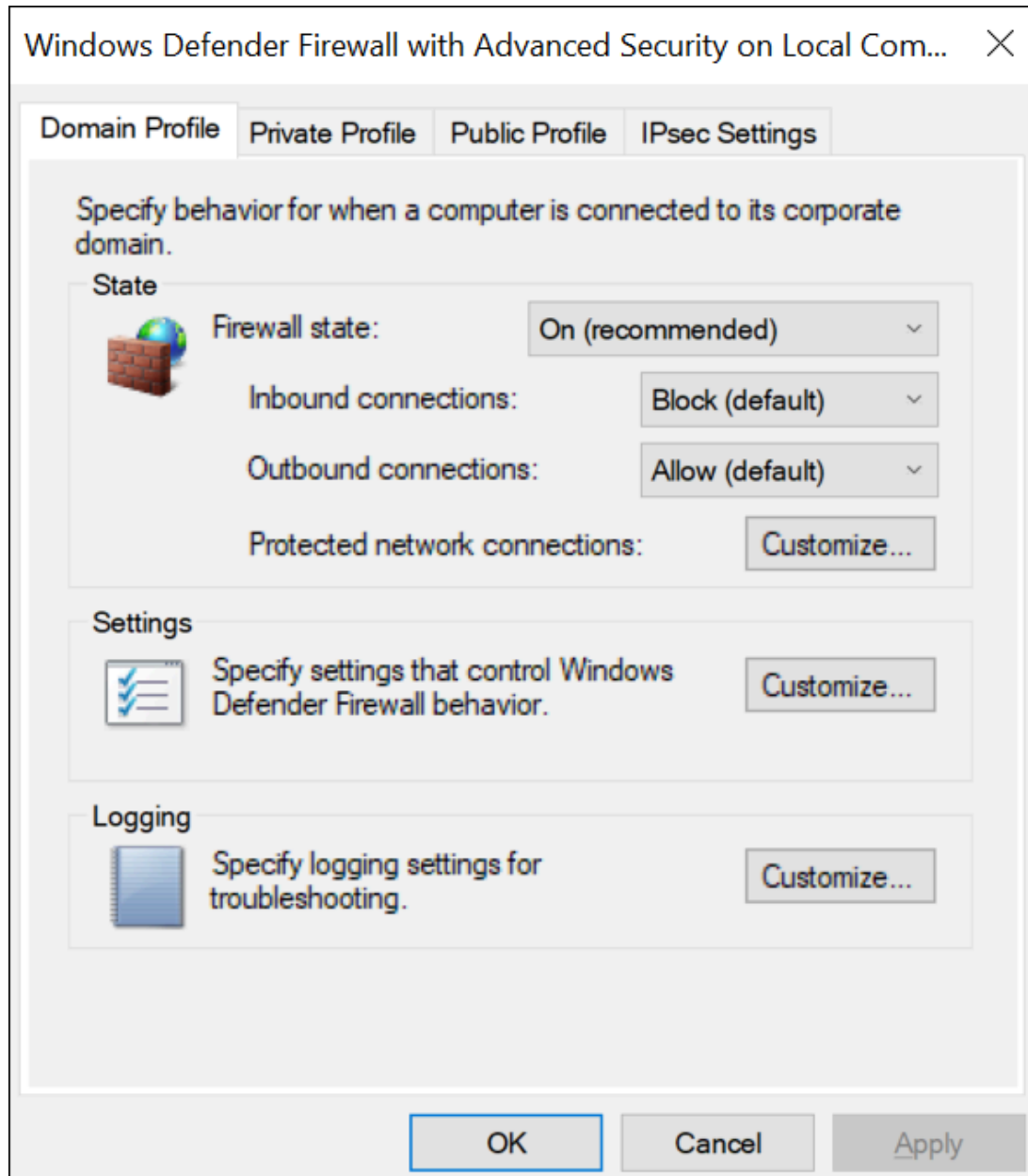
1. Run `wf.msc`.

The **Windows Defender Firewall with Advanced Security** window appears.

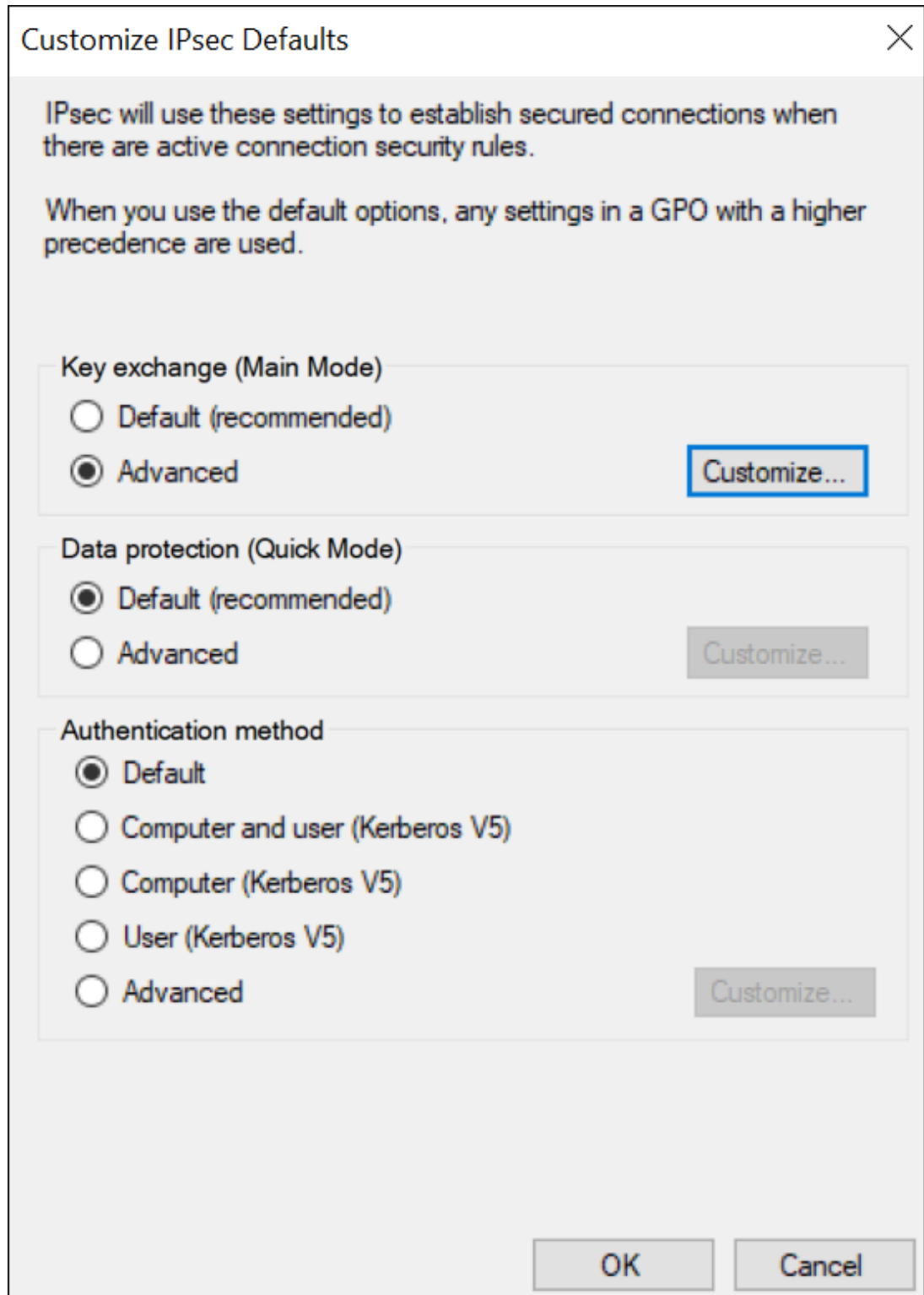
2. Create a security method:

- a. Select **Actions > Properties**.

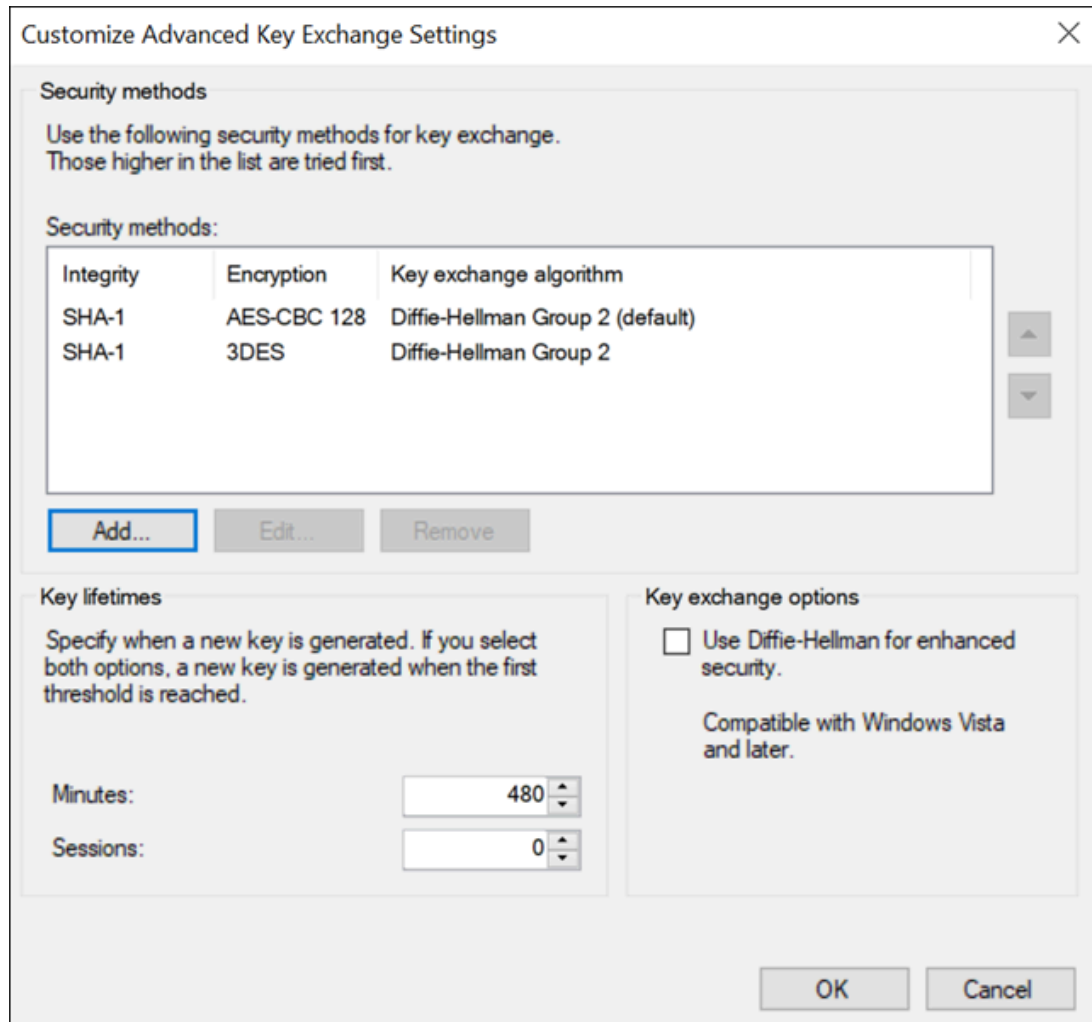
The **Windows Defender Firewall with Advanced Security on Local Computer** window appears.



- b. Select **IPsec Settings > Customize**.
The **IPsec Defaults** window appears.



- c. Under **Key exchange (Main Mode)**, select **Advanced > Customize**.
The **Customize Advanced Key Exchange Settings** window appears.



d. Select **Add**.

The **Add Security Method** window appears.

e. Select the algorithms that you want to use for each purpose. The following image shows an example.

Add Security Method [X]

Integrity algorithm:
SHA-384 [v]
[i] Compatible with Windows Vista SP1 and later.

Encryption algorithm:
AES-CBC 256 [v]
[i] Stronger than AES-192, higher resources usage.
Compatible only with Windows Vista and later.

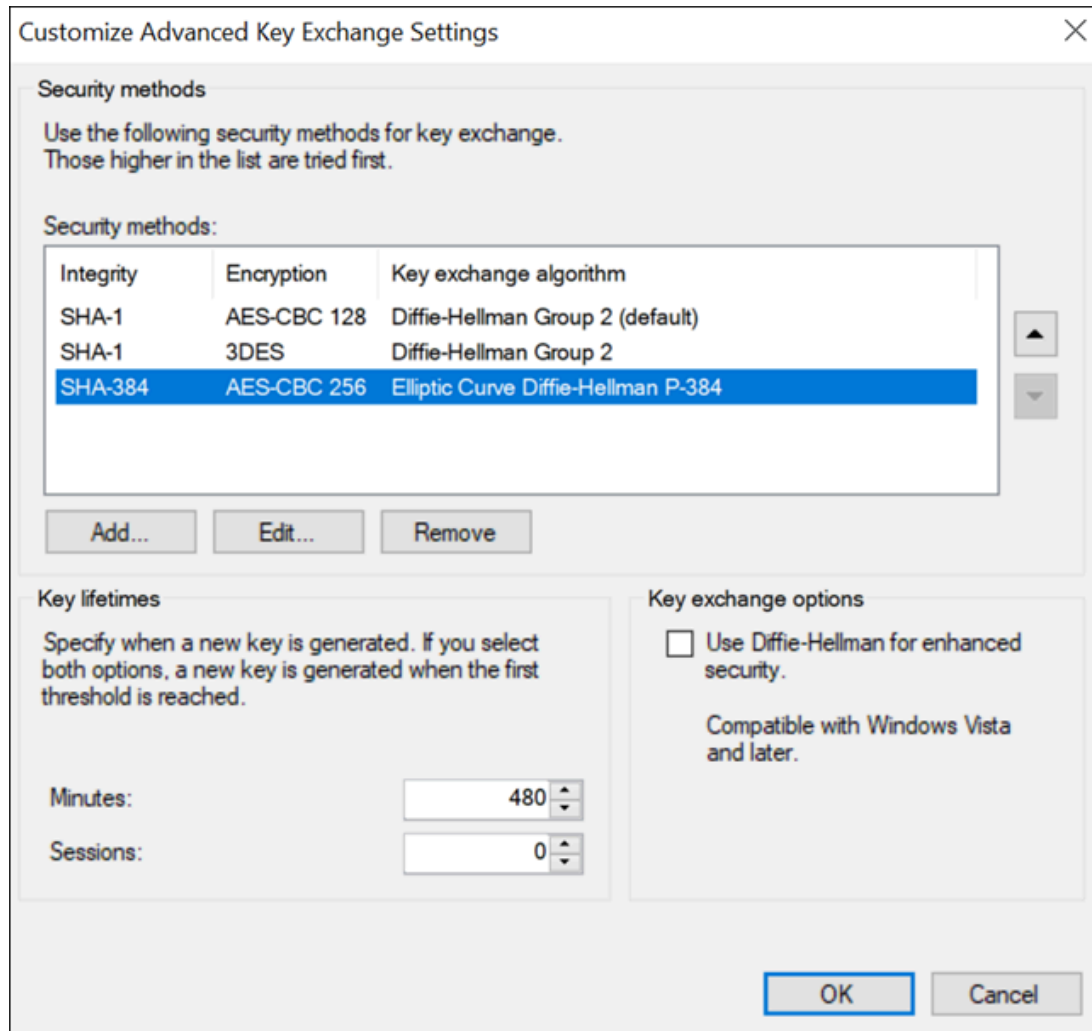
Key exchange algorithm:
Elliptic Curve Diffie-Hellman P-384 [v]
[i] Strongest security, highest resources usage.
Compatible only with Windows Vista and later.

OK Cancel

**Important:**

You must provide the same values for all the machines for which you want to configure IP security.

The security method that you have added appears in the list.



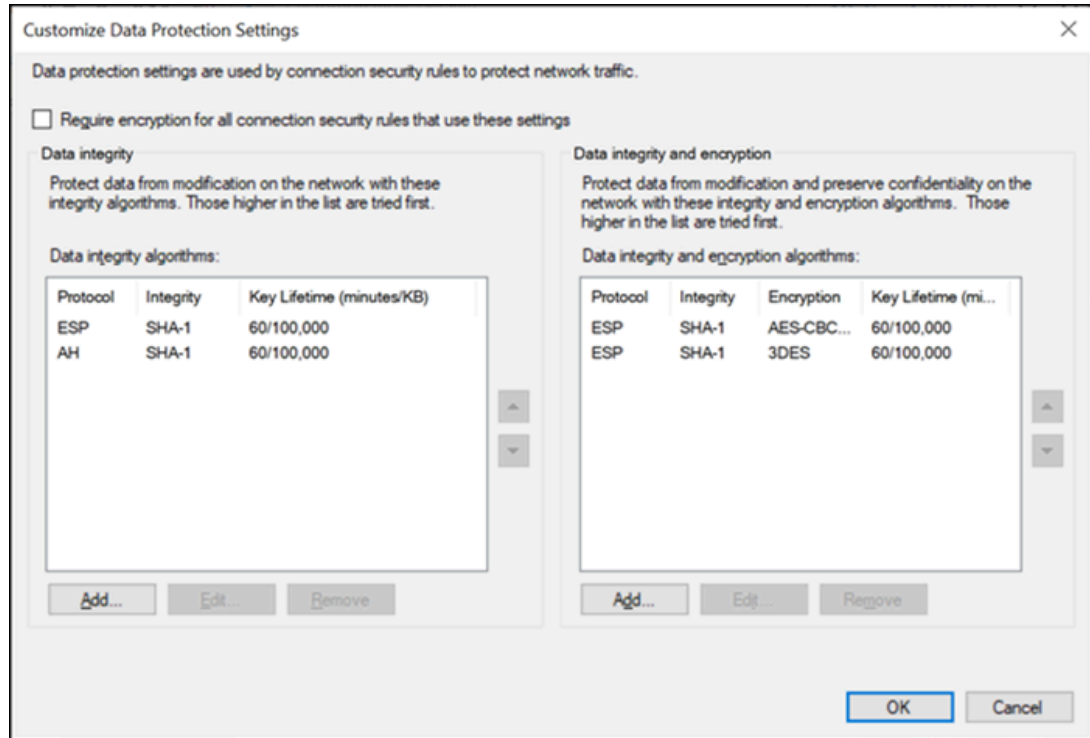
f. Move the security method that you have added to the top of the list. We recommend that you remove the other methods.

g. Select **OK**.

3. Add integrity and encryption algorithms:

a. In the **Customize IPsec Defaults** window, under **Data protection (Quick Mode)**, select **Advanced > Customize**.

The **Customize Data Protection Settings** window appears.



- b. Select the **Require encryption for all connection and security rules that use these settings** check box.
- c. Under **Data integrity and encryption**, select **Add**.
The **Add Integrity and Encryption Algorithms** window appears.

Add Integrity and Encryption Algorithms

Protocol

ESP (recommended)
ESP protocol provides privacy and integrity for the packet payload. ESP is compatible with Network Address Translation (NAT).

ESP and AH
Adding the AH protocol provides additional integrity for the IP header. This option is not compatible with NAT.

Algorithms

Encryption algorithm: AES-CBC 128

i Faster and stronger than 3DES. Compatible only with Windows Vista and later.

Integrity algorithm: SHA-1

i Stronger than MD5, uses slightly more resources.

Key lifetimes

Minutes: 60

KB: 1,000,000

OK **Cancel**

d. Under **Protocol**, ensure that **ESP** is selected.

e. Select the algorithms that you want to use for each purpose, and then select **OK**.

The algorithms that you have selected appear in the list.

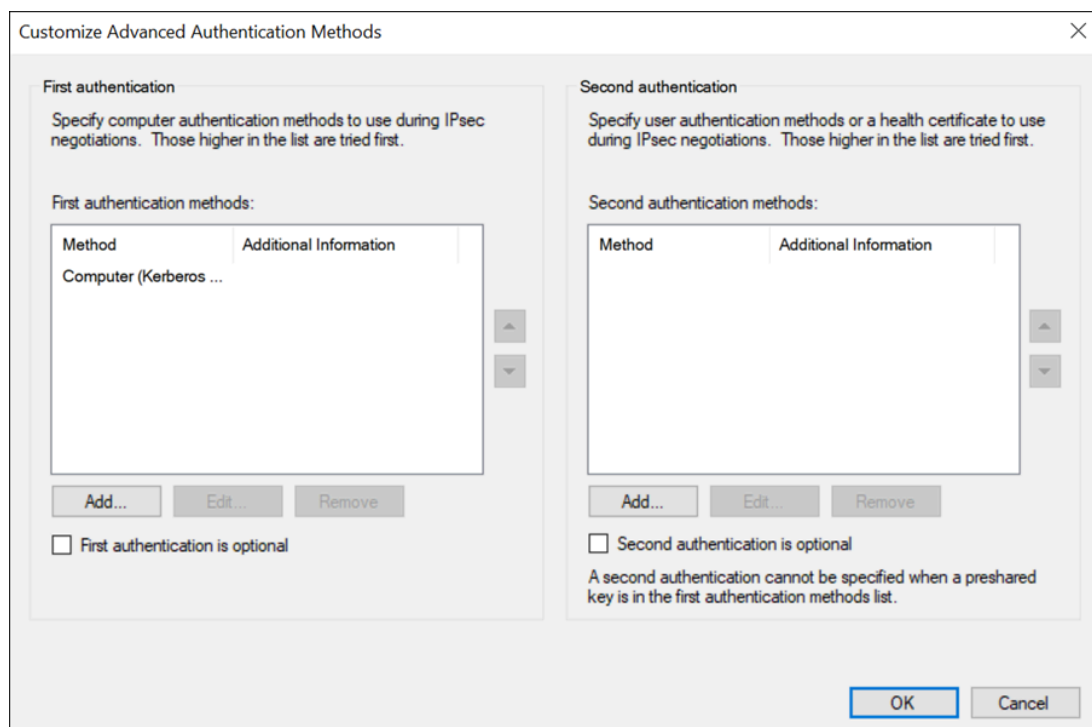
f. Move the algorithms to the top of the list. We recommend that you remove the remaining items in the list.

g. Select **OK**.

4. Create a first authentication method:

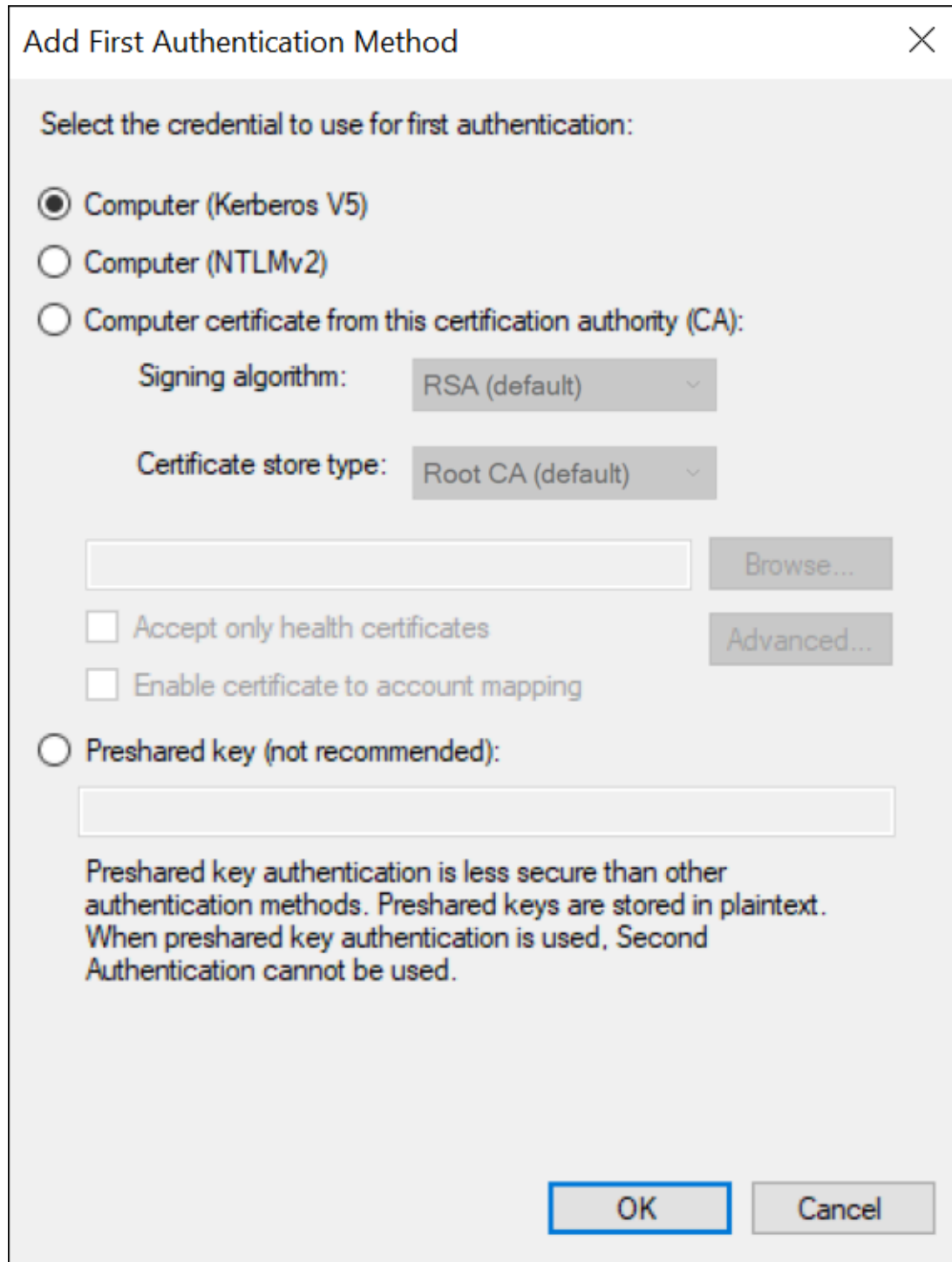
a. In the **Customize IPsec Defaults** window, under **Authentication Method**, select **Advanced > Customize**.

The **Customize Advanced Authentication Methods** window appears.



b. Under **First authentication methods**, select **Add**.

The **Add First Authentication Method** window appears.



- c. Provide the CA certificate that you want to use, and then select **OK**.
The certificate that you have provided appears in the list.

d. Move the certificate to the top of the list. We recommend that you remove the remaining items in the list.

e. Select **OK**.

5. Create a connection security rule:

For Windows x86, run the following set of commands to create a rule:

```
netsh advfirewall
consec
add rule name=""<rule name>" endpoint1=any endpoint2=any protocol=tcp port1=any port2=2010
action=requestinrequestout
```

For other versions, perform the following steps:

a. In the **Windows Defender Firewall with Advanced Security** window, select **Connection Security Rules**.

b. Select **Actions > New Rule**.

The **New Connection Security Rule Wizard** window appears.

New Connection Security Rule Wizard

Rule Type
Select the type of connection security rule to create.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

- Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.
- Authentication exemption**
Do not authenticate connections from the specified computers.
- Server-to-server**
Authenticate connection between the specified computers.
- Tunnel**
Authenticate connections between two computers.
- Custom**
Custom rule.

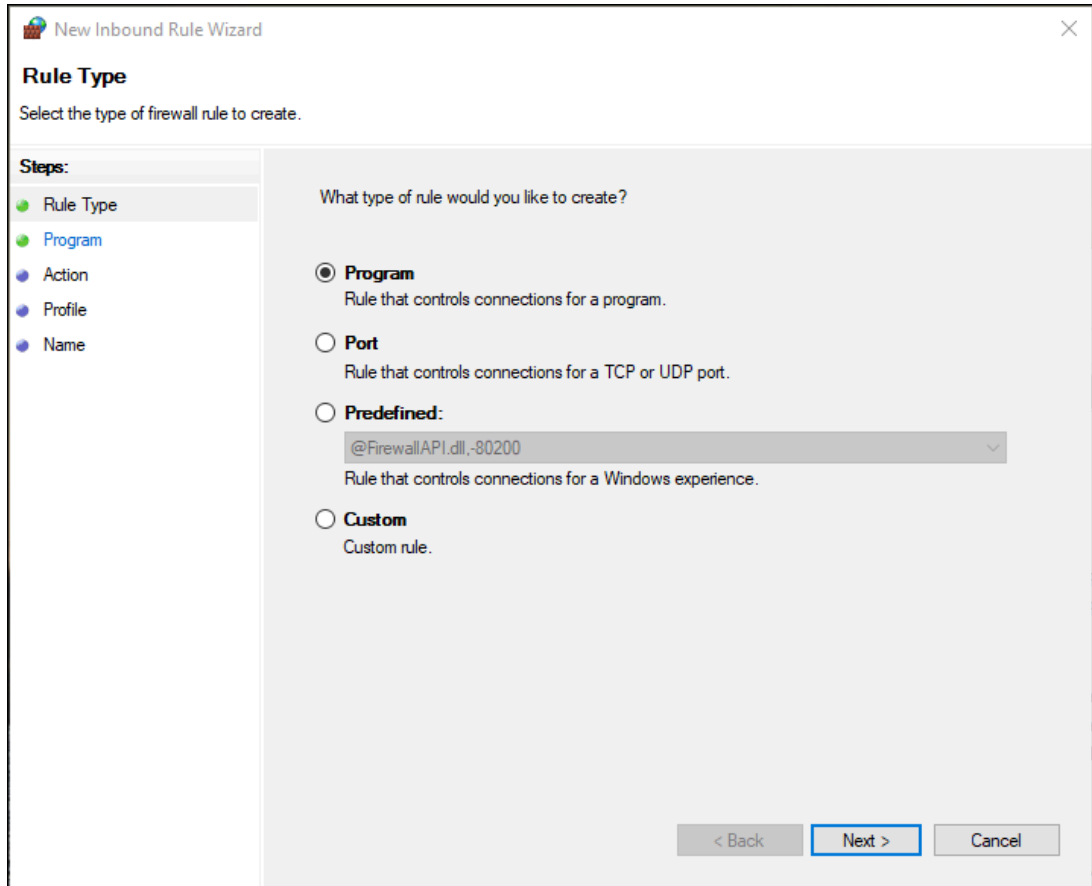
Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

< Back Next > Cancel

- c. Select **Custom**, and then select **Next**.
- d. Both for Endpoint 1 and Endpoint 2, select **Any IP Address**, and then select **Next**.
- e. Select **Require authentication for inbound and outbound connections**, and then select **Next**.
- f. Select **Default**, and then select **Next**.
- g. Enter values as described in the following table, and then select **Next**.

Field	Description
Protocol type	Select TCP .
Endpoint 1 port	Select All Ports .
Endpoint 2 port	Select Specific Ports , and then enter 2010.

- h. Select when to apply the rule, and then select **Next**.
 - i. Enter a name and description for the rule, and then select **Finish**.
The rule appears in the **Connection Security Rules** window.
 - j. Ensure that the rule is enabled.
6. If using Microsoft Windows Server 2019, 2016, 2012 R2 and/or Windows 8, 8.1, open up port number 5000:
- a. In the **Windows Defender Firewall with Advanced Security** window, select **Inbound Rules**.
 - b. Select **Actions > New Rule**.
The **New Inbound Rule Wizard** window appears.



- c. Select **Custom**, and then select **Next**.
- d. Select **All programs**, and then select **Next**.
- e. Enter values as described in the following table, and then select **Next**.

Field	Description
Protocol type	Select UDP .
Protocol number	Leave the default value as is.
Local port	Select Specific Ports , and then enter 5000.
Remote port	Leave the default value as is.

- f. Both for the local and remote IP addresses, set the scope to **Any IP address**, and then select **Next**.
- g. Select **Allow the connection**, and then select **Next**.

- h. Select when to apply the rule, and then select **Next**.
- i. Enter a name and description for the rule, and then select **Finish**.
The rule appears in the **Inbound Rules** window.
- j. Ensure that the rule is enabled.

IPSEC is now configured on the machine.

7. Repeat all the steps above on all the machines that host the Historian server and/or its components/clients.
8. To verify that the IPSEC cryptography is used:
 - a. Ensure that the Historian server is running.
 - b. Ensure that the collectors are connected to the Historian server, and that the collectors are running.
 - c. Specify the tags for data collection. You can do so using Configuration Hub (*on page*) or Historian Administrator (*on page*).
 - d. Verify that the collector is collected data.
 - e. On each machine on which you configured IPSEC, run `wf.msc`.
The **Windows Defender Firewall with Advanced Security** window appears.
 - f. Select **Monitoring > Security Associations > Main Mode**.
The **Main Mode** section displays the connection that you have created.

Security Setup Example

The following example takes you through the process of establishing your security needs and defining and setting up the levels of security.

For this example, assume the following user needs in a plant of 14 users:

User	Needs	Added to Security Group
USER1	Power user. Needs total access to security.	iH Security Admins
USER2	<ul style="list-style-type: none"> • Read/Write Data (no messages). • Create, modify, and delete tags. 	<ul style="list-style-type: none"> • iH UnAudited Writers • iH Tag Admins
USER3		

User	Needs	Added to Security Group
USER5 USER6 USER8	<ul style="list-style-type: none"> • Backup, restore, and create archives. • Connect to Data Archiver without creating login successful audit messages 	<ul style="list-style-type: none"> • iH Archive Admins • iH UnAudited Logins
USER4 USER7	<ul style="list-style-type: none"> • iRead/Write Data (no messages). • iCreate, modify, and delete tags. • iStart/Stop Collectors. • iBackup, restore, and create archives. 	<ul style="list-style-type: none"> • iH UnAudited Writers • iH Tag Admins • iH Collector Admins • iH Archive Admins
USER9-14	Read Data.	iH Readers

1. Establish the needs of your users. For this example, assume the user needs in a plant of 14 users, as described in the previous table.
2. Add and define the iH Security Admins Group.
Once you determine that you want to establish a security structure, you must create and define the iH Security Admins group. This group of users is typically the "power users" of the Historian. Security Administrator rights allow them to manage configuration and give them free rein to the entire system. For this example, only USER1 would be added to the iH Security Admins group.
3. Establish and create any other Historian Security Groups as needed.

**Note:**

Any user with Windows administrative permissions can add or remove Windows groups and users. As such, an administrator on a Windows computer, can add himself to any Historian security group.

Set up the functional security groups as needed. For this example, Write, Tag, Archive, and Collector security is required, so the groups associated with those functions should be added and defined. There is no need for Audited Writers and all valid users can read data, so neither the iH Audited Writers Group nor the iH Readers Group need to be added.

4. Define any individual Tag Level security.

In addition to defining iH Tag Admins that have the power to create, modify, and remove tags, you can also define individual tag level security to restrict access to sensitive tags. You can grant read, write, or administrative privileges per tag. For more information on setting Tag Level security, refer to the *Implementing Tag Level Security* section.

Setting Up Historian Security Groups

This section describes how to add the Historian Security Groups to your local and domain Windows security systems.

You can choose whether Historian uses LOCAL or DOMAIN security by selecting an option on the **Security** section of the **Data Store Maintenance** page in Historian Administrator. If you select the local security option, the groups are defined as local groups on the Historian server. If you select the Domain security option, the groups are defined as global groups in the primary domain controller of the Historian server. With domain security, Historian locates the Primary Domain Controller (PDC), if available, or a Backup Domain Controller (BDC) in order to establish groups. If the PDC and all BDCs are unavailable, the system locks all users out until rights can be established with a valid PDC or BDC.

**Note:**

If you change this setting, you must stop and re-start the Historian server for this change to take effect.

Creating a Local Group on Windows

1. Open the **Control Panel**.
2. Double-click the **Administrative Tools**.
3. Double-click the **Computer Management** icon.

The **Computer Management** console opens.

4. Select **Groups** from the **Local Users and Groups** folder in the system tree.
5. From the **Action** menu, select **New Group**.

The **New Group** window appears.

6. Enter the Historian Security Group name in the **Group Name** field.

For a list of available Historian Security Groups and their functions, see [Historian Security Groups \(on page 193\)](#).

**Note:**

You must enter the Historian Security Group name exactly as it appears. The security groups are case sensitive.

7. Optionally, enter a description of the Historian Security Group in the **Description** field.
8. Select **Create**.
9. Select **Close**.

Adding Users to Windows Security Group

Add your users to the Windows system.

1. Open the **Control Panel**.
2. Double-click the **Administrative Tools**.
3. Double-click the **Computer Management** icon.
The **Computer Management** console opens.
4. Select **Groups** from the **Local Users and Groups** folder in the system tree.
5. Select the group to which you want to add users.
6. From the **Action** menu, select **Properties**.
The **Users Properties** window appears.
7. Select **Add**.
8. Select the users or groups to add from the listed users or enter the names of the users or groups you want to add in the bottom field.
9. Select **Add**.

**Note:**

To validate the user or group names that you are adding, select **Check Names**.

10. When you have added all users to the group, select **OK**.

Adding a Local or a Domain User

1. Verify object type is **Users** or **Groups**.
2. If you want to add a local user, verify the **From This Location** setting is your local machine. (Select **Locations** to specify the local machine, if required.). If you want to add a domain user:
 - a. Select **Locations** to specify the domain, if required.
 - b. Select **Entire Directory** or the specific domain underneath **Entire Directory**.
 - c. Select **OK**.
3. Select **Advanced**.
The **Advanced** window appears.
4. Select **Find Now**.
5. From the list of users, select the users or groups to add or enter the names of the users or groups you want to add in the bottom field.
6. In the **Advanced** window, select **OK**.
7. In the **Select Users** window, select **OK**.
8. In the **Group Properties** window, select **OK**.

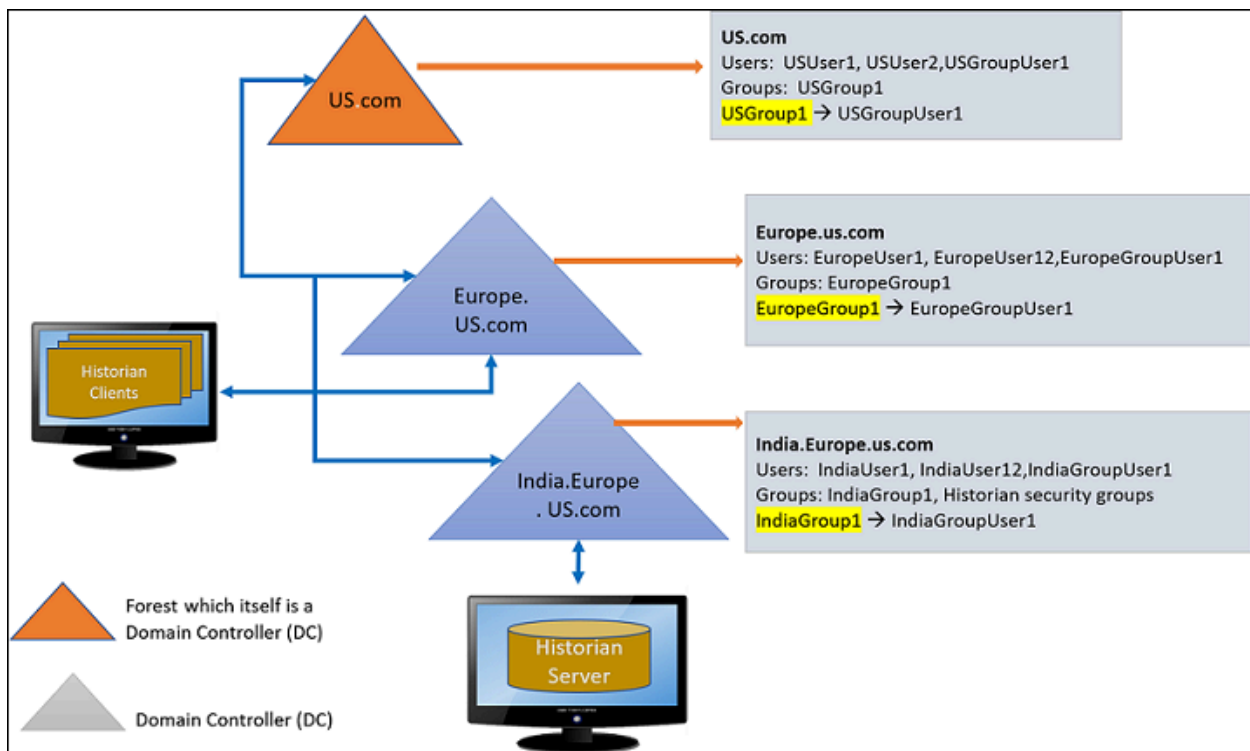
Active Directory Setup - an Overview

Historian Active Directory setup supports integration with complex models that include the following complexities:

- Users and administrators may belong to different domains within a forest.
- Domains may have sub-domains (multi-level) that need to inherit or refine on inherited permissions
- Group names may be longer than average to cater for group differentiation

The Active Directory setup supports authentication and authorization of users as members of groups from trusted or sub-domains (including assigning appropriate Historian access rights in line with Historian security roles/groups access).

The following figure provides an overview of the Active Directory setup with examples:



Configuring the Domain Users for active directory setup

To configure the domain (single\multi) environment in Historian Administrator:

Historian Security Groups should be created on the machine where the Domain controller of the Historian Server is installed. In the example illustrated above, the India.Europe.US.com domain controllers must contain the following Historian groups

- IH Security Admins
- IH Collector Admins
- IH Tag Admins
- IH Archive Admins
- IH UnAudited Writers
- IH UnAudited Logins
- IH Readers
- IH Audited Writers

**Note:**

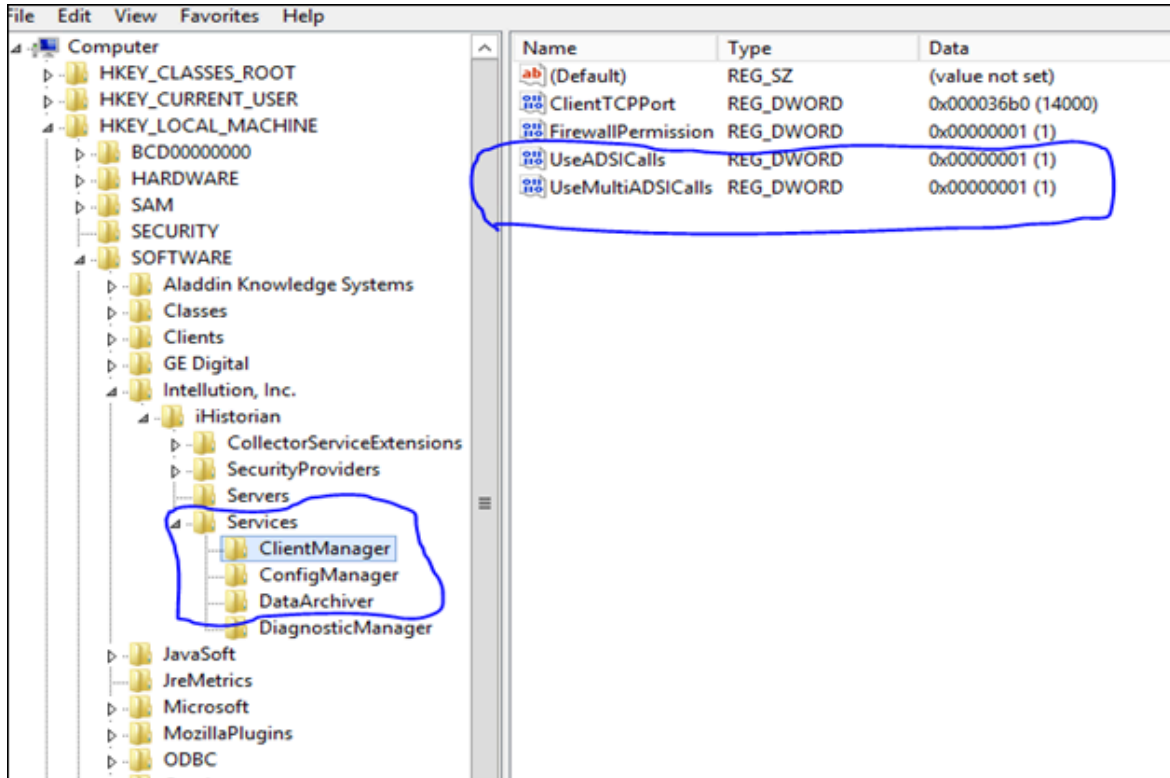
Historian Security Groups should be of type **Domain-Local** only.

1. On the **Data Stores** section, under **Security > Global Security**, select the **Use domain** option.

The screenshot shows the Proficy Historian web interface. The 'Data Stores' section is selected, and the 'Security Options' tab is active. Under 'Global Security', the 'Security Groups' option is set to 'Use Domain', which is highlighted with a red box. The 'Archives' table on the left lists several archives with their names and start times.

Name	Start Time
User_ConfigServer6_Archiv...	9/20/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/19/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/18/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/17/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/16/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/15/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/14/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/13/2018 5:00:00 ...
User_ConfigServer6_Archiv...	9/12/2018 5:00:00 ...
Empty	

2. Stop the Historian Services.
3. Add the Registry Entries for ClientManager, ConfigManager and DataArchiver as shown below.
Registry path: `HKKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\Historian\Services\`

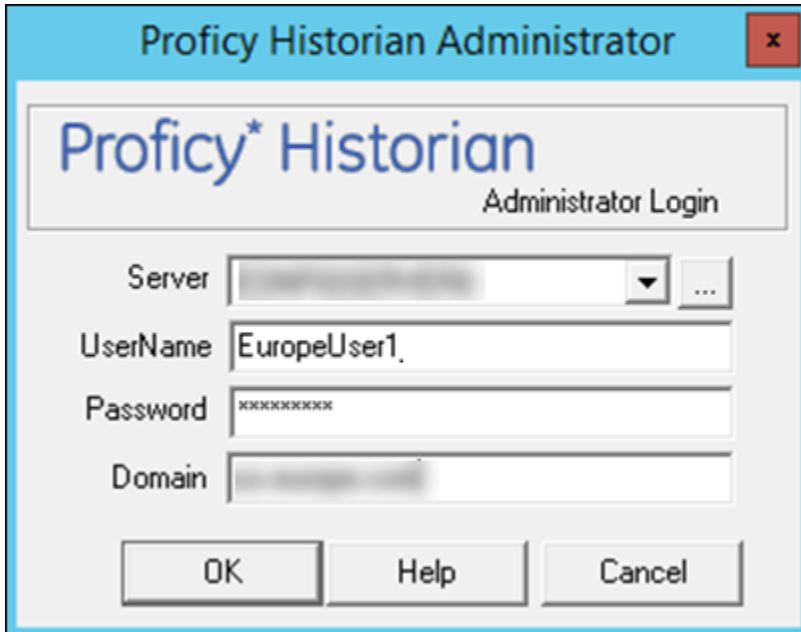


4. Start the Historian Services. The new registry entries will now be read by the corresponding Historian service.

Accessing Historian Server using Domain Users - Examples

Example 1: European domain user trying to connect to Historian Server installed in India.Europe.US.com Domain Controller (DC).

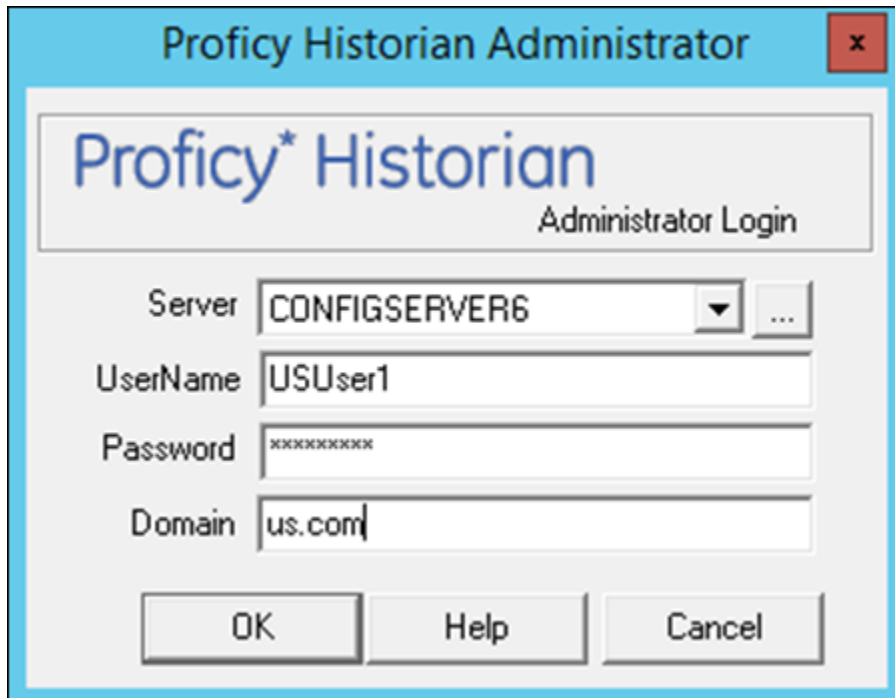
1. Create a user **EuropeUser1** in Europe.US.com DC.
2. Add the user (i.e. EuropeUser1) from Europe.US.com to "IH Security Admin" group in India.Europe.US.com DC
3. Log in to Historian Client using EuropeUser1 as shown below.



4. EuropeUser1 is added to IH Security Admin. The user will get full access to Historian Server.

Example 2: US domain user trying to connect to Historian Server (which is installed in India.Europe.US.com Domain Controller (DC)).

- a. Create a user **USUser1** in US.com DC.
- b. Add the user (i.e. USUser1) from US.com to "IH Readers" group in India.Europe.US.com DC
- c. Login to Historian Client using USUser1 as shown below.



5. USUser1 is added to IH Readers. The user will get only data read access to Historian Server.

Adding Nested Domain Groups to Historian Security Groups

The following procedure describes, a European domain group user trying to connect to Historian server, installed in India.Europe.US.com Domain Controller.

1. Create a user **EuropeGroupUser1** in Europe.US.com DC.
2. Create a group **EuropeGroup1**.
3. Add the EuropeGroupUser1 to EuropeGroup1.
4. Add the group (i.e. EuropeGroup1) from Europe.US.com to "IH Security Admin" group in India.Europe.US.com DC
5. Login to Historian Client using EuropeGroupUser1.
6. If a new user gets added to EuropeGroup1 then it gets automatically synced with Historian Security Groups.



Note:

As EuropeGroupUser1 added as a IH Security Admin, user will get full access to Historian Server.

US domain group user trying to connect to Historian Server installed in India.Europe.US.com Domain Controller.

- a. Create a user **USGroupUser1** in US.com DC (if not exist).
- b. Create a group USGroup1.
- c. Add the USGroupUser1 to USGroup1.
- d. Add the group (i.e. USGroup1) from US.com to "IH Security Admin" group in India.Europe.US.com DC
- e. Login to Historian Client using USGroupUser1.
- f. If a new user gets added to USGroup1 then it gets automatically synced with Historian Security Groups.

**Note:**

As USGroupUser1 added a IH Readers, user will get data read access to Historian Server

Managing Proficy Authentication Users Using the Configuration Tool

Use the Proficy Authentication Config tool to perform the following tasks:

- Add a local Proficy Authentication user.

**Note:**

Here a local Proficy Authentication user means a user defined by Proficy Authentication, not by an external identity provider such as LDAP.

- Remove a local Proficy Authentication user.
- Reset the password for a local Proficy Authentication user.
- Add a local Proficy Authentication user to an existing group.

Since OAuth2 scopes are implemented as Proficy Authentication groups, this means the same as adding a scope to a user.

- Remove a local Proficy Authentication user from an existing group.

A user who performs these functions is acts as the admin client and needs to know the secret of the admin client. The tool does provide a way for the user to cache the secret safely to be used later.

By default, this tool is available in the following folder: `C:\Program Files\GE Digital\Historian Config`. Run the tool from a Windows command prompt window.

Syntax

The tool's syntax follows this format:

```
uaa_config_tool verb [options]
```

where verb is one of the following:

- `add_user`
- `remove_user`
- `set_user_password`
- `add_user_to_group`
- `remove_user_from_group`
- `clear_secret`

Run the tool without a verb or any other options to view the help page.

The `uaa_config_tool` utility prompts for a port number. This is the port number that you have specified in the Public HTTPS Port field in the **TCP PORT ASSIGNMENTS** page. By default, it is set to 443. If you have changed the public HTTPS port number, enter the number. Otherwise, enter 443.

Options can be specified in the form of single dash followed by a short name, or double dash followed by a long name, followed by the value of the option, if any. For example, you can specify the user name `Alice` by either

```
-u Alice
```

or

```
--UserName Alice
```

Table 5. Options

Short name	Long name	Remark
<code>-t</code>	<code>--Target</code>	URL of the Proficy Authentication instance that the command should be performed on. Typically, the URL is <code>https://localhost:8443/uaa</code> , which is the default value. This option is optional and is only needed when the user wants to run the command against a remote Proficy Authentication instance (which is not recommended due to security concerns).
<code>-n</code>	<code>--ClientId</code>	ID of the client that the user is acting as. By default, it is <code>admin</code> . This option is optional and is only needed when the admin has set up the Proficy Authentication to delegate certain operations to others.

Table 5. Options (continued)

-s	<code>--ClientSecret</code>	<p>This is the secret used to authenticate the user for acting as the admin client (or an alternative client given in a <code>--ClientId</code> option). If the user has elected to cache the secret previously, then this option can be omitted. Otherwise, it has to be provided.</p> <p>The password must satisfy the following conditions:</p> <ul style="list-style-type: none"> • Must not contain only numbers. • Must not begin or end with a special character. • Must not contain curly braces.
-c	<code>--CacheSecret</code>	<p>This option is not followed by a value and is optional. If specified, the tool will cache the client secret so when the next time this tool is invoked the secret does not have to be specified. Note that the secret is encrypted and only the current Windows logon user can access and decrypt.</p>
-u	<code>--UserName</code>	<p>Name of the user that the tool is being invoked for. For example, the user that is being added or removed.</p>
-p	<code>--UserPassword</code>	<p>The password for the user being added or whose password is being reset. The option is only needed for the <code>add_user</code> and <code>set_user_password</code> commands.</p>
-g	<code>--Group</code>	<p>Name of the Proficy Authentication group (scope) that the user is being added to or removed from. The option is only needed for the <code>add_user_to_group</code> and <code>remove_user_from_group</code> commands.</p>

Examples

- To add a user named alice with the password Pa55word and the admin client secret myclientsecret (this is the admin client secret that you entered while installing Web-based Clients):

```
uaa_config_tool add_user -u alice -p Pa55word -s myclientsecret -c
```

If the Proficy Authentication server is on a remote machine named webhost.lab:

```
uaa_config_tool add_user -u alice -p Pa55word -s myclientsecret -t https://webhost.lab:443/uaa -c
```


- To provide user privileges to access the Web Admin console and Trend Client:

```
uaa_config_tool add_user_to_group -u alice -g historian_visualization.user -t https://webhost.lab:443/uaa
```

- To provide admin privileges to access the Web Admin console and Trend Client:

```
uaa_config_tool add_user_to_group -u alice -g historian_visualization.admin -t https://webhost.lab:443/uaa
```

- To provide Configuration Hub privileges, add alice to the group `historian_enterprise.admin`, using the previously cached admin secret:

```
uaa_config_tool add_user_to_group -u Alice -g historian_enterprise.admin -t https://webhost.lab:443/uaa
```

- To remove alice from a remote instance of Proficy Authentication as an alternative client (that is, other than `admin`) `useradmin`:

```
uaa_config_tool remove_user -u alice -t https://webhost.lab:8443/uaa -n useradmin -s MyOtherNonSecret
```

- To clear any cached client secret:

```
uaa_config_tool clear_secret
```



Note:

If the Windows logon account is not shared, it is not necessary to clear cached secret, since the cache is encrypted and only the same Windows user account can decrypt.

When there are Historian security groups on the local historian machine or on the domain server:

1. Create a new user account on the local Historian machine or on the domain server with same login name and password as the local Proficy Authentication user.
2. Add the new user to the appropriate Historian Security group on the local historian machine or on the domain server.

Create a Proficy Authentication Reader Client

To fetch Historian data, previously, you had to manually add each user to iH security groups. Only then the users could fetch the data. Now, this process has been simplified. All you must do is create a Proficy Authentication client. The Proficy Authentication client will be automatically added to the iH Readers security group on the server side. Therefore, you can use the client to fetch Historian data using REST APIs.

1. Access the Proficy Authentication Config tool, which is located in the following folder by default:

```
C:\Program files\GE Digital\Historian Config\uaa_config_tool
```

2. Access Command Prompt as an administrator, and then run the following command:

```

uaa_config_tool add_historian_reader_client -u <client name> -p <client password>
-n <username> -s <password> -t https://<Proficy Authentication URI>:443/uaa

```

To create a client named client1:

```

uaa_config_tool add_historian_reader_client -u client1 -p password123
-n user1 -s userpassword123 -t https://Proficy Authentication URI2010:443/uaa

```

The Proficy Authentication reader client is created. However, if it already exists, a message appears, stating the same.

About Accessing Cross-Domain Historian

You can now access Historian across various domains regardless of the domain to which your user account belongs. To do so:

- Ensure that all the domain controllers across various domains trust one another.
- Create iH security groups on each leaf node that contains the Historian server that you want to access.
- Ensure that you are part of at least one iH security group. You can be part of an iH security group directly, or you can be part of a universal domain group, which must be part of the iH security group.

About Domain Security Groups

When you configure Historian to use domain security groups, the data archiver attempts to locate the groups on the primary domain controller (PDC) or one of the backup domain controllers (BDC). When using a PDC, if a primary or backup domain controller cannot be located when the Historian Data Archiver service starts, access to Historian is denied to all users.

For troubleshooting, .shw file of the data archiver lists all PDCs and BDCs available at the time of archiver startup. Use this list to verify that the Historian server has visibility into the appropriate domain.

When using a PDC, after the list of Domain Controllers has been established, the Historian Server will use that list to query for Security Group Membership on an as needed basis. If at any time a request for Group Membership information is made and the Primary Domain Controller is not available, Historian selects the first Backup Domain Controller and attempts the same request. If a Backup Domain Controller successfully responds to the request, the process of querying for Group Membership can stop. Otherwise, Historian will attempt to query Group Membership information from the next available Backup Domain Controller. If no Backup Domain Controller successfully responds, access to the system is denied.

Changing security group configuration from Local to Domain or vice versa requires that the Historian Data Archiver service be restarted for the change to take effect.

Establishing Your Security Rights

Your security identity is established upon connecting to the server. This occurs through the following steps:

1. Specifying a user name and password of an account.

Upon connection, the system checks to see if you have a valid Windows 2003 account. If you have supplied a username and password (through the Excel Add-In for example), security checks that user. If username and password are not supplied and you are on a Windows 2003 or Windows 2008 machine or higher, security checks the currently logged in user.



Note:

If you do not pass a domain name the account will be checked locally in the same way a mapped drive attempt happens. You have to specify a username and password that exists on the server.

2. Determining group membership of that account.

Once the account is validated, the server determines group membership. For more information on the process and hierarchy of the groups, refer to the Security Checking Process diagram below.

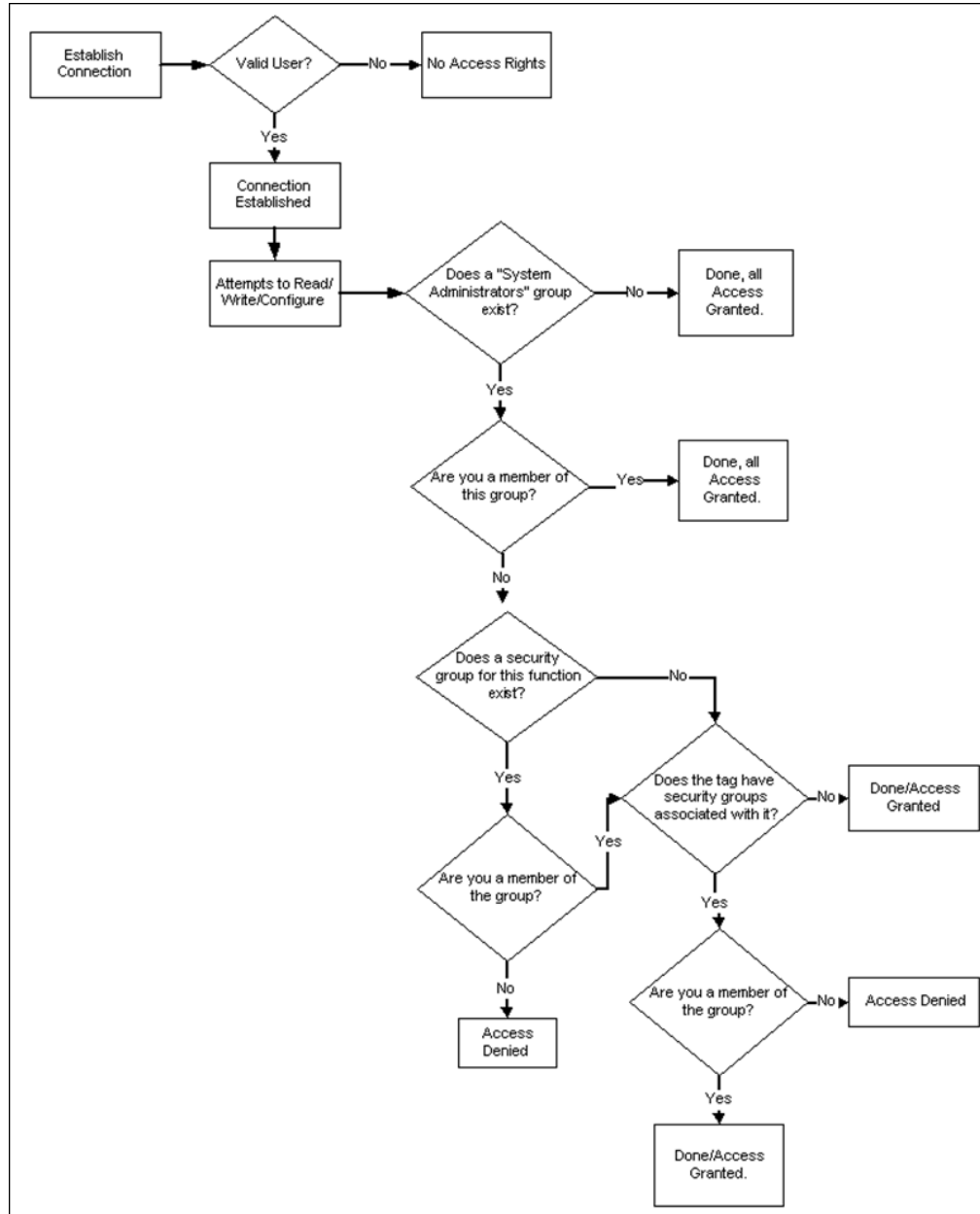
3. Caching membership profile.

Once the group and tag membership are determined, it is cached for the connection and not looked up again. If users are added to or deleted from a group, the cache is not updated.

**Note:**

The cache information is per connection, and not per IP address. In other words, it is cached per application and not per system.

Figure 1. Security Checking Process



Implementing Tag-Level Security

In addition to defining the iH Tag Admins who have the power to create, modify, and remove tags, you can also define individual tag level security to protect sensitive tags.

Set tag level security in Historian Administrator. You need the Historian Security Groups to implement tag-level security. You can use a Windows pre-defined group (power users, for example) or create your own separate group specifically for this function. For more information on creating and adding groups, refer to [Setting Up Historian Security Groups \(on page 214\)](#).

Users must have iH Security Admins rights to set individual tag level security, browse, or query tags in Historian Administrator.



Note:

Tag security is not enforced in the Trend Client when it comes to browsing the full list of tags. Security, however, is enforced when it comes to trending data for tags for which you have permission. For example, if you are logged into the Trend Client as a user that is a member of the User Group assigned to a tag's security Read Group, you will still be able to browse all Historian tags. However, you are only allowed to trend the tags for which the user is a member of the User Group assigned to the tag's security Read Group,

1. Access Configuration Hub (on page [214](#)).
2. In the **NAVIGATION** section, under the Configuration Hub plugin for Historian, select **Tags**.
A list of all the tags appears.
3. Select the row containing the tag whose security you want to define.
The tag details appear in the **DETAILS** section.
4. Enter values as described in the following table.

Field	Description
Read Group	<p>The Windows security group that can retrieve the tag data and plot it in a trend chart.</p> <p>For example, if you select a group with power users, in addition to members of the iH Security Admins group, only a member of the power users group will be able to read data for that tag. Even a member of the iH Readers group will not be able to access data for that tag, unless they are also defined as a member of the power users group.</p>

Field	Description
Write Group	The Windows security group that can write tag data (for example, using the Excel Add-in for Historian).
Administer Group	The Windows security group that can create, modify, and delete the tag.

**Note:**

If you are using domain groups (instead of local groups), the **Read Group**, **Write Group**, and **Administer Group** fields contain only the groups whose names begin with iH<space> (case-sensitive). Therefore, ensure that the group that you want to use begins with iH<space>.

Uninstalling Historian

Uninstalling Historian

Uninstalling Historian removes all saved Favorites from your Trend Client and all Users and Scopes you created. To keep these and other configurations on an upgrade, do not uninstall Historian unless you are changing server roles as previously described. If you must uninstall Historian on an upgrade, you can Export your favorites and save your data and tag configuration files for future use.

For information on uninstalling OPC Data Collectors, refer to the *Modifying and Uninstalling OPC Collectors* section of the *Historian Data Collectors* manual.

- When you want to uninstall Web-based Clients:
 - If you select the **Purge database during uninstall** check box, the entire database will be purged, and you must recreate the Proficy Authentication details, favourites, and so on. Therefore, if you want to retain Proficy Authentication details, do not select that check box.
 - If you have installed Operations Hub on the same machine, and if there is a shared Proficy Authentication package between Operations Hub and Web-based Clients, in some cases, a message appears, asking you to first uninstall Operations Hub before uninstalling Web-

based Clients. You can, however, uninstall Web-based Clients first; the shared Proficity Authentication package will not be deleted in that case.

- Configuration Hub will not be uninstalled because it is a common component. If needed, you can uninstall it separately.
- If you uninstall Historian after installing the Excel Add-In as described, ensure that you clear the **Historian** check box in the Microsoft Excel **Add-Ins** window. If you do not clear this option, you will receive an error each time you open Microsoft Excel.

1. To uninstall Historian from your computer:

- a. Double-click the **Programs / Uninstall a Program** link in the Control Panel.
- b. Select **Historian** and select **Uninstall**.



Note:

Historian archives are not removed by default. If you need to remove them, delete the folder manually.

A progress bar appears, showing that the software is being uninstalled. This may take some time.

To abort the uninstall, select **Cancel**.

2. To remove all related software from your computer:

- a. Double-click the **Programs / Uninstall a Program** link in the Control Panel.
- b. Select **Proficity Common Licensing**, and select **Uninstall**.

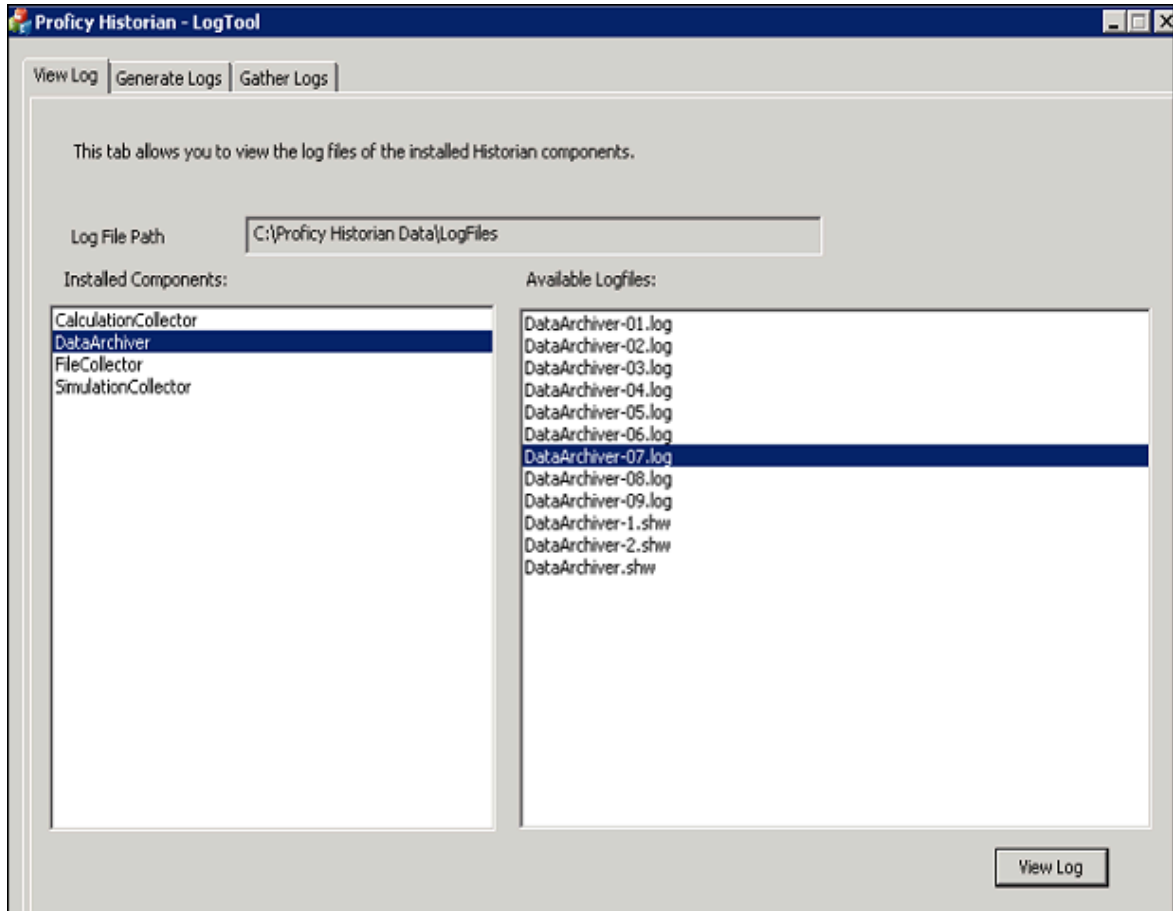
Troubleshooting

Managing Historian Log Files

Use the Historian LogTool to view, generate, or compress log files to use for troubleshooting.

Logtool.exe is located in the historian installation directory, for example: `C:\Program Files\Proficity\Proficity Historian\X64.`

1. Go to your installation directory and execute the Logtool.exe file.
The **LogTool** opens, displaying the **View Log** section.



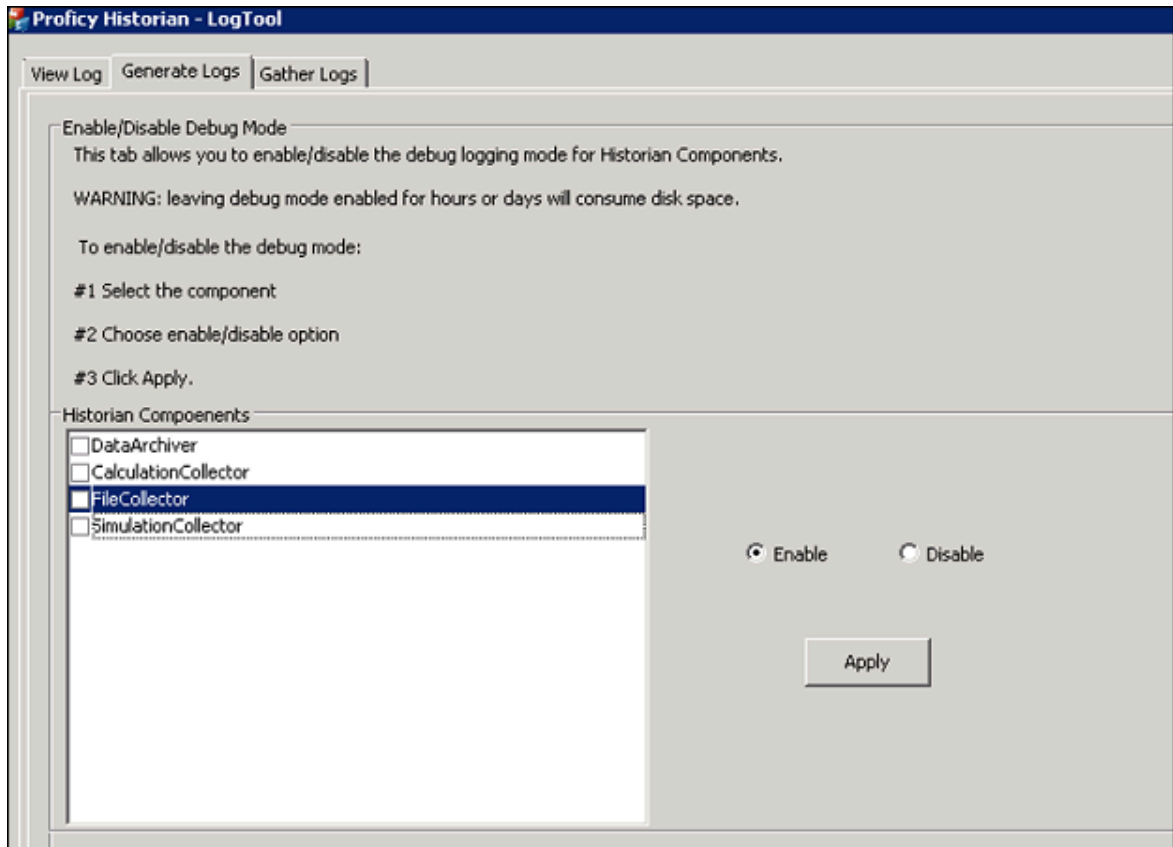
2. Select a component from the left panel to see the available log files, and select **View Log**.
3. Select **Generate Logs** to enable or disable the debug logging mode for Historian components:

This tool will enable/Disable the debug mode for Historian components. However, leaving the debug mode enabled for longer time consume the disk space

1. Select the component

2. Choose enable/disable option

3. Select apply



a. Select a Historian Component and select **Enable** or **Disable**.

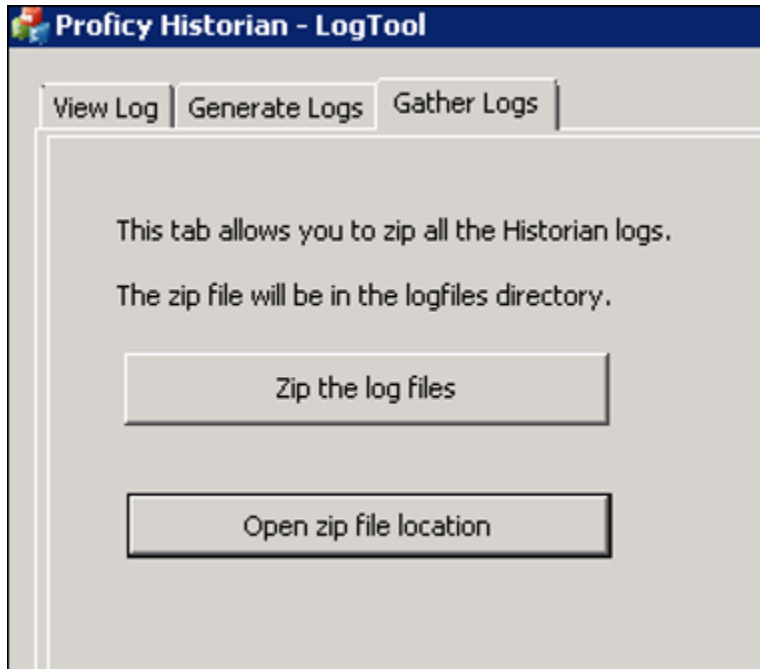


Note:

Leaving debug mode enabled for a component consumes disk space.

b. Select **Apply**.

4. Select **Gather Logs** and select **Zip the log files** to compress the log files and select **Open zip file location** to view the zip files.



Troubleshooting the Historian Server

iFIX-Related Files in C Drive Even if iFIX is not Installed

Description

If you install only Historian without installing iFIX, you may find some iFIX-related files in the C drive.

Workaround

You can ignore/delete them. If, however, you plan to install iFIX later, you must reinstall Historian Client Tools after installing iFIX.

Error Message when Upgrading the Historian Server on a Passive Node in a Cluster

Description

If you are upgrading the Historian server on a passive node, an error message may appear behind the installer screen, stating that the Archives directory is not created.

Error Message

Unable to create Archives directory.

Workaround

You can ignore this message, or you can make the node active before upgrading the Historian server.

Historian Server Rejects Collector or Client User Credentials

Description

If a client or collector is attempting to connect to the Historian server with strict authentication enabled on a Kerberos configuration, the server rejects valid credentials and does not allow the connection.

Workaround

Ensure that the server time and the domain controller time match with each other.

Historian Resource in a Cluster Environment is not Online

Workaround

Ensure that the cluster feature is included in your license.

Historian Resource Runs for a Long Duration and Fails Over

Workaround

Debug the log messages of the Data Archiver and the Clusters before taking appropriate actions.

While Label Error

Description

If the PFX file that you want to use with Historian does not contain a full-chained certificate, a while label error message appears.

Workaround

1. Create a PEM file from the PFX file by copying the content from all the certificates (such as root, intermittent, and leaf certificates) to the PEM file. It results in a full-chained certificate.
2. Get a KEY file from the vendor. Or, use a KEY file extracted from the PFX file using the Certificate Management tool. To do so, import the PFX file. The certificate and the KEY file will then be available in the <Operations Hub installation

location>\httpd\conf\cert folder. You can then use the `server.key` file in the folder.

3. Using the Certificate Management tool, import the PEM and KEY files to the machines on which the Historian server, the Operations Hub server, and clients are installed.

Troubleshooting Web-based Clients

Unable to Access Configuration Hub After Upgrading Web-based Clients

Description

After you upgrade Web-based Clients, you cannot access Configuration Hub.

Workaround

Clear your browser cache.

Error Occurs When You Try to Access Web-based Clients

Description

If you have logged in to Operations Hub, and then if you try to access Web-based Clients, and vice versa, an error occurs. This is because the user credentials of the first application to which you have logged in are used to log in to the other one as well.

Workaround

Try one of the following steps:

- Add the scopes of each application user to the other application.
- If you log in to Web-based Clients first, on the login page of Operations Hub, re-log in with the Operations Hub user. If you log in to Operations Hub first, log out of Operations Hub, log in to Web-based Clients, and then log in to Operations Hub, using the credentials of the respective users for each application.

Unable to Access Web-based Clients

Description

When you upgrade Historian, after installing Web-based Clients, a message asking you to restart the machine does not appear. Because of this, sometimes, you cannot access Web-based Components such as Configuration Hub, Trend Client, the Web Admin console, and REST APIs.

Workaround

Restart the machine, or start the following services:

- GE Historian PostgreSQL Database
- GE Historian Tomcat Server
- GE Operations Hub Httpd Reverse Proxy
- GE Operations Hub Proficy Authentication PostgreSQL Database
- GE Operations Hub Proficy Authentication Tomcat Web Server
- GE Proficy Authentication External IdP Configuration Service
- GE Security App Service

Certificate Issues When Trying to Log in

Workaround

[Connect to a Remote Proficy Authentication Service \(on page 136\)](#)

Web-based Clients are not connected to the Historian server

Workaround

- Ensure that the **Enforce Strict Client Authentication** and **Enforce Strict Collector Authentication** options are disabled in the **Data Stores Security** section in Historian Administrator.
- Ensure that the Proficy Authentication URL used by Web-based Clients matches the one you provided while installing the Historian server. If not, [change the Proficy Authentication server \(on page 89\)](#) so that the Historian server points to the same Proficy Authentication server as Web-based Clients.

Clients or Users Not Created

Description

Clients or users are not created because the required services were not running during the installation of Web-based Clients.

- An error message appears when you access Web-based Clients or Trend Client.
- The visualization client is not found. The following error message appears: No client with requested id: historian_visualization
- When you attempt to log in to Proficy Authentication, a message appears, stating that the credentials are incorrect.

Workaround

[Configure Web-based Clients \(on page 137\)](#) to point to a different Configuration Hub and Proficy Authentication instance.

The Reverse Proxy Service Stops Working

Description

If you install iFIX on a machine that has Historian Web-based Clients, the reverse proxy service stops working.

Workaround

Restart the reverse proxy service - GE Operations Hub Httpd Reverse Proxy.