Proficy Historian 9.1

Getting Started Guide

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

Chapter 1. Getting Started Guide

Historian Overview

Historian Overview

Proficy Historian is a high-performance data archiving system designed to collect, store, and retrieve time-based information at an extremely high speed. 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.

Data Collectors

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

Note: To collect data from CIMPLICITY, you must use the Historian OPC collector with the CIMPLICITY OPC 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 File collector
- The Calculation collector
- The Server-to-Server distributor
- The OSI PI Distributor
- The OPC Classic Alarms and Events collector
- The iFIX Alarms and Events collector

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.

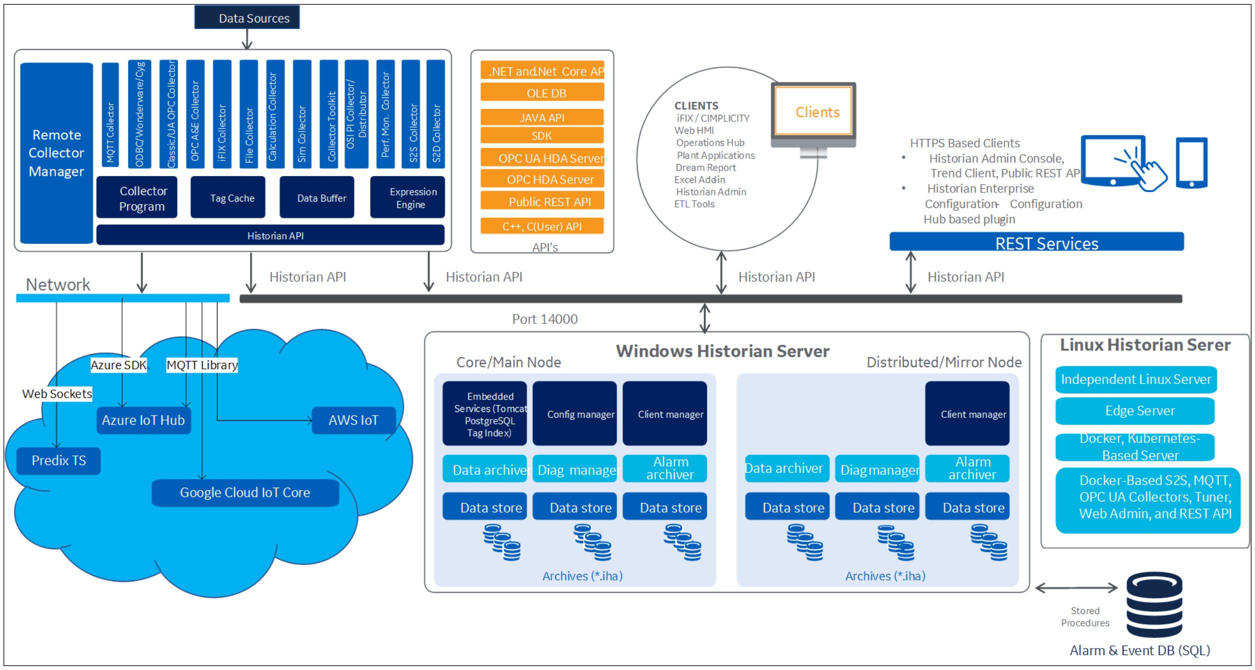
The Historian Data Archiver is a service that indexes all the data by tag name and timestamp and stores the result in an .iha file. The tag name is a unique identifier for a tag (which is a specific measurement attribute). For iFIX users, a Historian tag name normally represents a Node.Tag.Field (NTF). 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.

Historian System Architecture

Th following image shows the Historian system architecture:



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 clients communicate with the Server through the Historian API. This list describes the functions performed by each component:

Historian Alarms and Events

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

Refer to *Historian Alarms and Events* for more information.

Historian Data Collectors

Data Collectors gather data from a data source on a schedule or event basis, 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):

- Maintaining a local cache of tag information to sustain collection while the server connection is down.
- Automatically discovering available tags from a data source and presenting them to Historian Administrator.
- 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 both collector and device time stamping, where applicable.
- Scheduling data polling for polled collection.
- Performing a first level of data compression (collector compression).
- Responding to control requests, such as requests to pause or resume collection.
- Options to send data to Historian or Cloud service through a Web socket connection

For mission-critical data collection, redundant collectors are possible. Historian includes a mirroring option for high availability and load balancing, so the data is available for the organization all the time.

Refer to `Historian Data Collectors` for more information.

Historian File collector

File collectors import .CSV or .XML files into Historian. The files can contain data, alarms, tagnames, or other configuration information, and messages that you can import with a File collector.

Refer to the *Historian Data Collectors* manual for more information.

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. For information, refer to Configuration Hub section in the online Help.

Historian Administrator

A 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.
- A Calculation collector with the ability to create a new tag based on calculations, and stores the result as time series data – available with Historian Administrator only.
- Setting up your OPC Classic HDA server – available with Historian Administrator only.

Refer to the *Using Historian Administrator* manual for more information.

Historian Web Admin console

The Historian Web Admin now operates in a web-based environment. The Historian Web Admin console provides an enhanced Dashboard that displays the health of the system in one convenient location. The Dashboard is available in the Web Admin console only. 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 (available in the Web Admin console only), tags, collectors, data stores and archives. The functionality of the Calculation collector and the ability to configure your OPC HDA Web server are not included in the Web Admin console.

The Web Admin console uses a client-access license (CAL).

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 Admin Console Dashboard.

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

Historian Client Manager

The Historian 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.

Historian Configuration Manager

The Historian 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.

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 Historian Web Administrator and Trend tool. It supports SSL and the use of certificates for enhanced security.

UAA Tomcat Container

An instance of Tomcat is used exclusively by Historian as an open source Java-based Web server to support the External UAA.

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.

UAA PostgreSQL Database

An instance of PostgreSQL is used exclusively by Historian to store UAA details.

Reverse Proxy Service

Provides secure connection by supporting https protocol.

Historian Extract, Transform, and Load (ETL) Tools

Transferring data from one Historian server to another is typically performed by Proficy Historian collectors. These collectors 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.

Historian Indexing Service

This is an indexing service that periodically runs against the Historian tag database, creates a tag index, and stores information in the PostgreSQL database instance, a preferred method to allow for quick search results.

Excel Add-In

The 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.

For more information, refer to *Using the Historian Excel Add-In*.

Excel Add-in for Operations Hub

The Historian Excel Add-in enables you to query historical data of objects and object types defined in Operations Hub. You should install Operations Hub to use this Excel Add-in.

Customers purchasing Historian Standard or Enterprise licenses now receive a no-cost license for the Operations Hub Server and Historian Analysis run-time application. This 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.

Excel Add-in for Operations Hub is tested with Excel 2016, 2019 versions (32 and 64 bit).

Historian OPC Classic HDA server

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

Refer to the *Historian OPC Classic HDA server* manual for more information.

Historian 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.

Historian 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.

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 OLEDB 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.

Refer to the *ihUserApi Help* system for more information.

Historian Web REST API

Historian includes a REST API to connect your Java Web-based Clients with Historian data. Refer to the *Historian REST API Reference Manual* in the `/Additional Documentation` folder of your installation directory for more information.

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.

JAVA APIs

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

Refer to the Historian JAVA API Reference Offline Manual in the /Additional Documentation folder of your installation directory for more information.

Collector Toolkit

The Collector Toolkit allows you to write programs that integrate tightly with Historian and leverage the same configuration tools, redundancy schemes, and health monitoring as collectors that ship with Historian. A custom collector is a collector developed using the Collector Toolkit. 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 CAL.

Historian Migration Tools

Historian provides migration tools to allow you to migrate your existing Classic Historian configurations and data and your iFIX Alarms and Events collector data into the Historian environment. Tags, collection rates, and deadbands for tags configured in Classic Historian can be transferred into Historian by the migration tools.

For more information, refer to *Migrating Advanced and Classic Historian Data*.

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 onto cloud). This topic provides a list of these components.

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.
- 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 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.

Historian File collector

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

Historian Extract, Transform, and Load (ETL) 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.

Historian Migration Tools

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

Collector Toolkit

The Collector Toolkit is used to develop a customized collector. To do so, you can use the Collector Toolkit to write programs that integrate with Historian and leverage the same configuration tools, redundancy schemes, and health monitoring as the Historian data 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 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.

Refer to *Historian Alarms and Events* for more information.

Historian Administrator

A 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.
- A Calculation collector with the ability to create a new tag based on calculations, and stores the result as time series data – available with Historian Administrator only.
- Setting up your OPC Classic HDA server – available with Historian Administrator only.

Refer to the *Using Historian Administrator* manual for more information.

Historian Web Admin console

The Historian Web Admin consoles provides a dashboard, which displays the health of the system in one convenient location. The dashboard is available in the Web Admin console only. 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 (available in the Web Admin console only), tags, collectors, data stores, and archives. However, the functionality of the Calculation collector and the ability to configure your OPC HDA web server are not included in the Web Administrator.

The Historian admin console uses a client-access license (CAL).

Historian Server

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 Admin Console Dashboard.

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

Fault Type	Fault Description	Fault Level
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

Historian Client Manager

The Historian 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.

Historian Configuration Manager

The Historian 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.

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 Historian Web Administrator and Trend tool. It supports SSL and the use of certificates for enhanced security.

UAA Tomcat Container

An instance of Tomcat is used exclusively by Historian as an open source Java-based Web server to support the External UAA.

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.

UAA PostgreSQL Database

An instance of PostgreSQL is used exclusively by Historian to store UAA details.

Reverse Proxy Service

Provides secure connection by supporting https protocol.

Historian Indexing Service

This is an indexing service that periodically runs against the Historian tag database, creates a tag index, and stores information in the PostgreSQL database instance, a preferred method to allow for quick search results.

Excel Add-In

The 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.

For more information, refer to *Using the Historian Excel Add-In*.

Excel Add-in for Operations Hub

The Historian Excel Add-in enables you to query historical data of objects and object types defined in Operations Hub. You should install Operations Hub to use this Excel Add-in.

Customers purchasing Historian Standard or Enterprise licenses now receive a no-cost license for the Operations Hub Server and Historian Analysis run-time application. This 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.

Excel Add-in for Operations Hub is tested with Excel 2016, 2019 versions (32 and 64 bit).

Historian 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.

Refer to the *The Historian OPC Classic HDA server* manual for more information.

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.

Data Retrieval Components

Data retrieval components are used to retrieve data that is stored in the Historian server. This topic provides a list of these components.

Historian Alarms and Events

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

Refer to *Historian Alarms and Events* for more information.

Historian Client Manager

The Historian 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.

Historian Configuration Manager

The Historian 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.

UAA Tomcat Container

An instance of Tomcat is used exclusively by Historian as an open source Java-based Web server to support the External UAA.

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.

Historian 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.

Refer to the *Historian OPC Classic HDA server* manual for more information.

Historian 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.

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 OLEDB 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.

Refer to the *ihUserApi Help* system for more information.

Historian Web REST API

Historian includes a REST API to connect your Java Web-based Clients with Historian data. Refer to the *Historian REST API Reference Manual* in the `/Additional Documentation` folder of your installation directory for more information.

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 programing language. To enable easier integration with Historian, JAVA APIs are provided. The JAVA APIs support 64-bit Windows Operating Systems.

Refer to the Historian JAVA API Reference Offline Manual in the /Additional Documentation folder of your installation directory for more information.

Standard and High-Availability Configuration

Standard and High-Availability Configuration Options

You have wide flexibility in configuring the Historian system. Since Historian can support a fully distributed architecture, you can spread the data collection, server, administration, and client data retrieval functions across many different nodes in a network, or you can install all the components on a single computer.

Since the Historian API is the basic building block for connectivity, all Historian functions, including data collection, administration, and data retrieval, use the Historian API.

You can connect the Historian API to a local Historian server in the same manner as to a remote Historian server by simply providing the name of the server. This name must be the computer name or the IP address of the target Historian server, and the server must have a TCP/IP connectivity. If you use the computer name of the server rather than the IP address, the IP address must be available to the client through DNS, a WINS server, or through the local host table.

It is recommended that you install the Historian server on a central dedicated server. Next, install data collectors on each data source, and point them back to the central Historian server by specifying the appropriate server computer name. Install a separate data collector for each type of collection interface used in your system.

You can also 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 install various types of collectors on a single computer, subject to constraints described in Install Collectors Using the Installer *(page 105)*.

Standard Historian Architecture

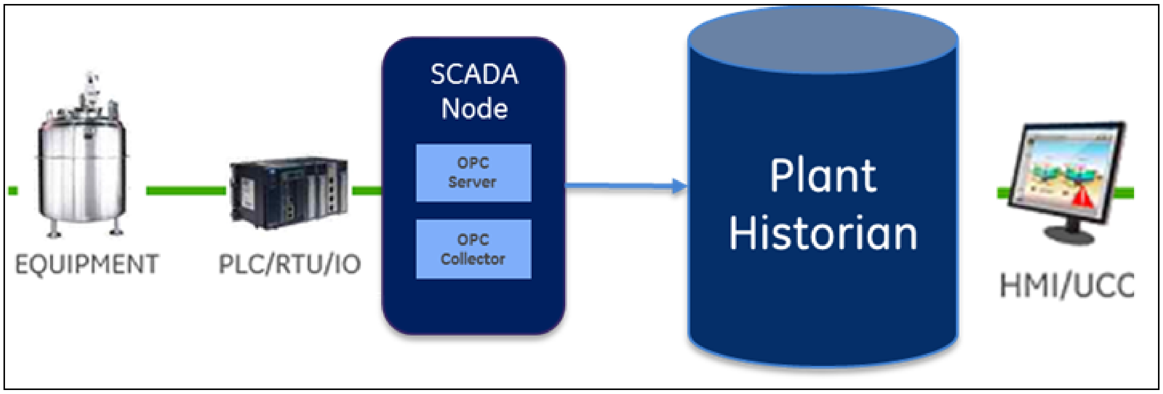
Standard Historian offers unique capabilities and benefits for a sustainable competitive advantage:

- Built-in data collection
- Good read/write performance speed
- Enhanced data security
- Robust redundancy and high availability

Single Node Data Only System

In a typical single node system, an OPC server or HMI is responsible for data collection. This data is used for trending and analyzing as illustrated in the following diagram:

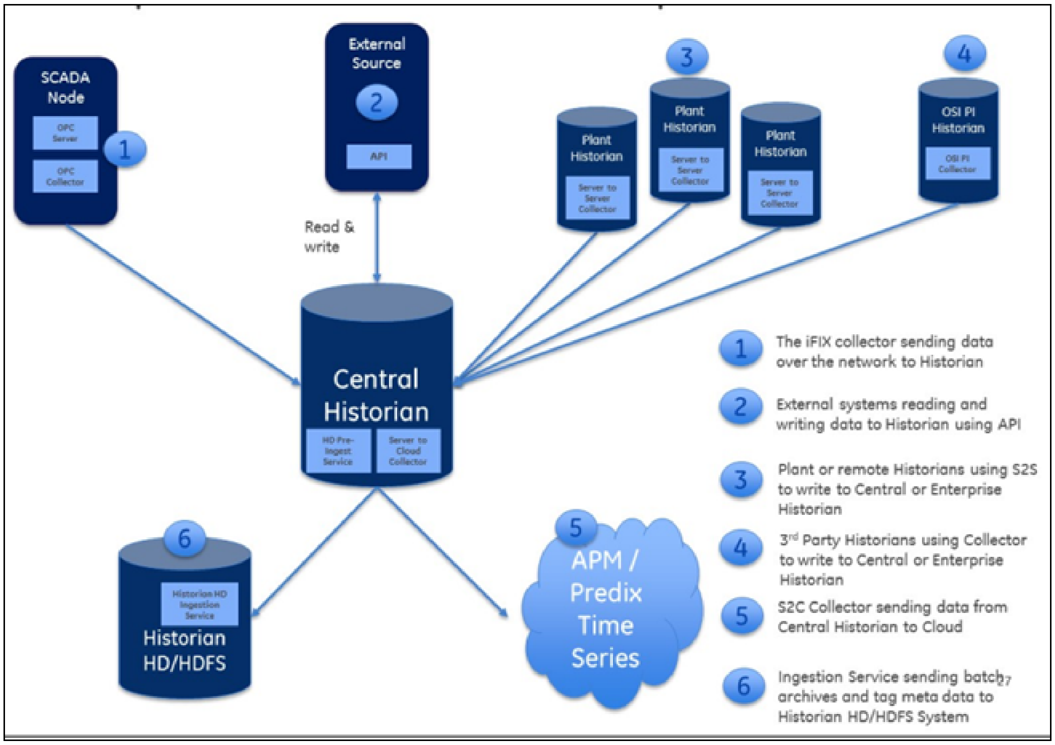
Figure: Single Node Data Only System



Data Collection from SCADA Systems and other Programs

The following diagram represents how data is collected from SCADA systems and other custom programs. The collected data is used for calculations and analysis.

Figure: Enterprise Data Collection Examples



1 The iFIX collector sending data over the network to Historian

2 External systems reading and writing data to Historian using API

3 Plant or remote Historians using S2S to write to Central or Enterprise Historian

4 3rd Party Historians using Collector to write to Central or Enterprise Historian

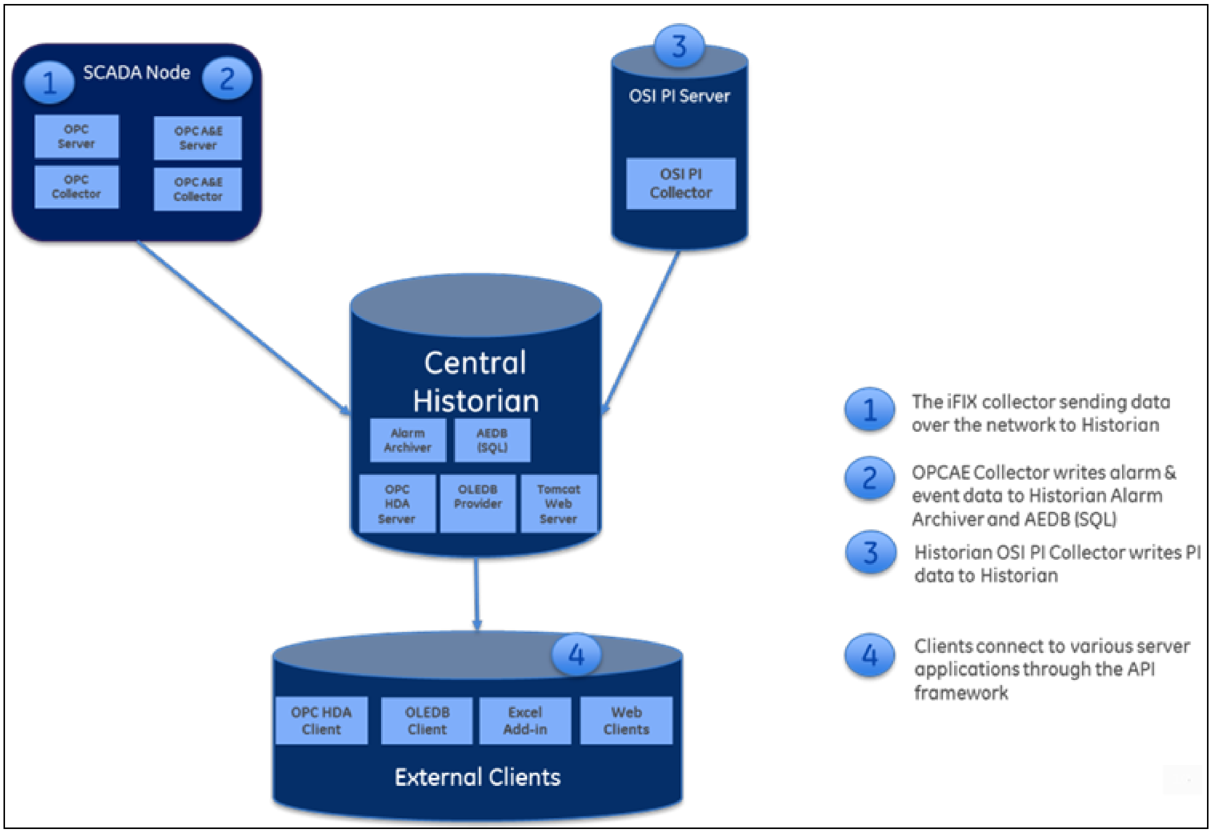
5 S2C Collector sending data from Central Historian to Cloud

6 Ingestion Service sending batch archives and tag meta data to Historian HD/HDFS System

Integration with Client Programs

The following diagram represents the integration with external client programs.

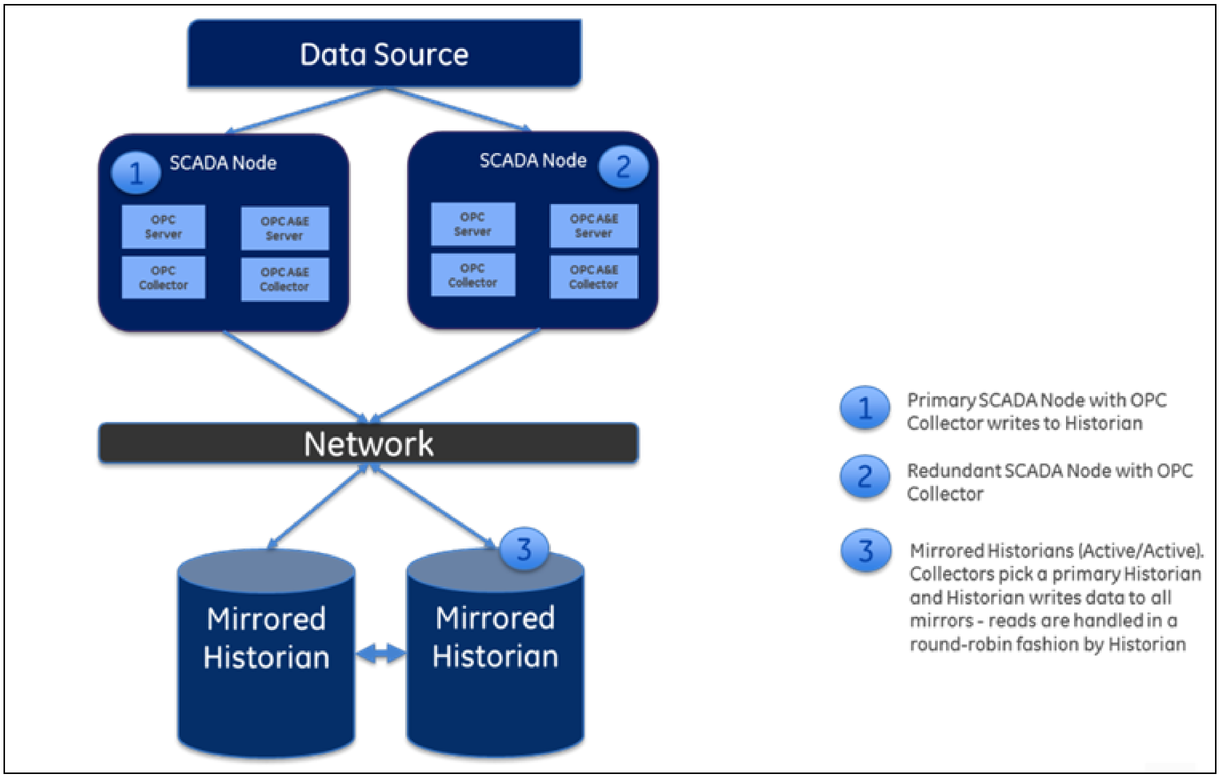
Figure: Data Collection and Client Connection Examples


SCADA Node
1
2
OPC Server
OPC A&E Server
OPC Collector
OPC A&E Collector
3
OSI PI Server
OSI PI Collector
Central Historian
Alarm Archiver
AEDB (SQL)
OPC HDA Server
OLEDB Provider
Tomcat Web Server
4
OPC HDA Client
OLEDB Client
Excel Add-In
Web Clients
External Clients
1 The iFIX collector sending data over the network to Historian
2 OPCAE Collector writes alarm & event data to Historian Alarm Archiver and AEDB (SQL)
3 Historian OSI PI Collector writes PI data to Historian
4 Clients connect to various server applications through the API framework

High-Availability Architecture

The following diagram shows a high-availability system with collector redundancy and mirrored Historians:

Figure: High Availability Example


Data Source
1 SCADA Node
OPC Server
OPC A&E Server
OPC Collector
OPC A&E Collector
SCADA Node 2
OPC Server
OPC A&E Server
OPC Collector
OPC A&E Collector
Network
Mirrored Historian
3
Mirrored Historian
1 Primary SCADA Node with OPC Collector writes to Historian
2 Redundant SCADA Node with OPC Collector
3 Mirrored Historians (Active/Active). Collectors pick a primary Historian and Historian writes data to all mirrors - reads are handled in a round-robin fashion by Historian

You can mirror stored data on multiple nodes to provide high levels of data reliability. Data mirroring involves the simultaneous action of every insert, update, and delete operation that occurs on any node. Historian allows you to maintain up to three mirrors, a primary and two additional mirrors.

Historian Data Mirroring

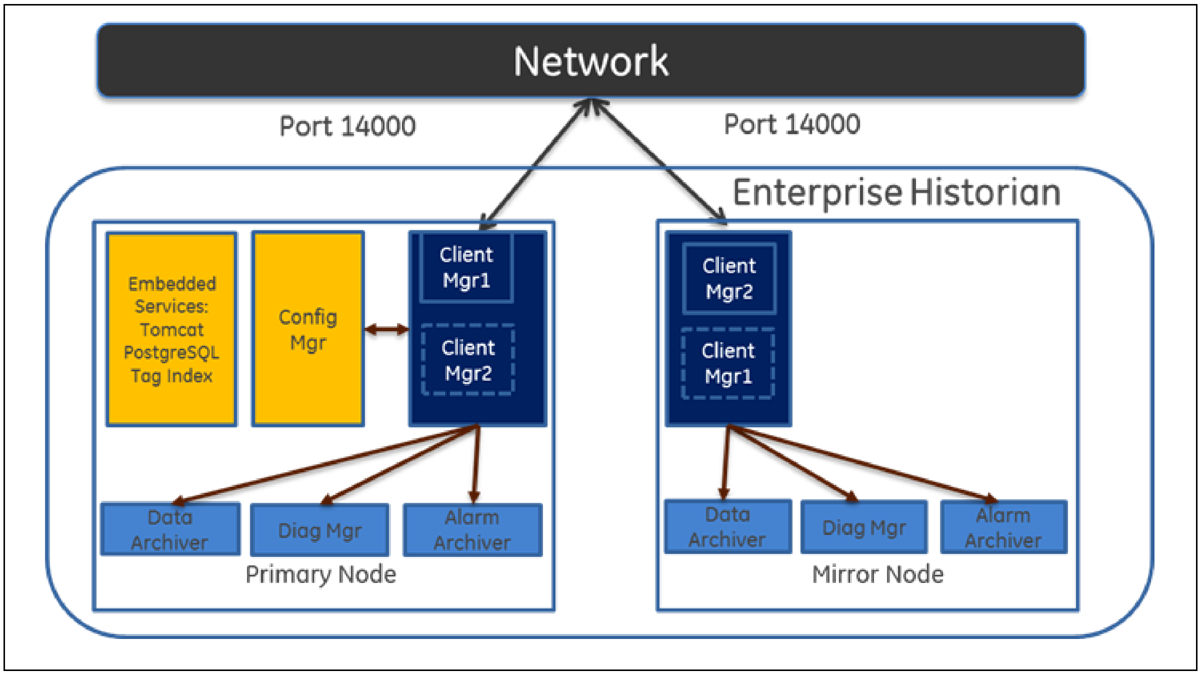
If you have purchased an Enterprise license for Historian and your license entitlement includes mirror nodes, you have the option of setting up to three mirrors (primary server + two mirrors).

Data mirroring provides continuous data read and write functionality. 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.

Mirrors must be set up in a single domain.

Figure: Mirroring Example



Client Connections in Mirrored Environments

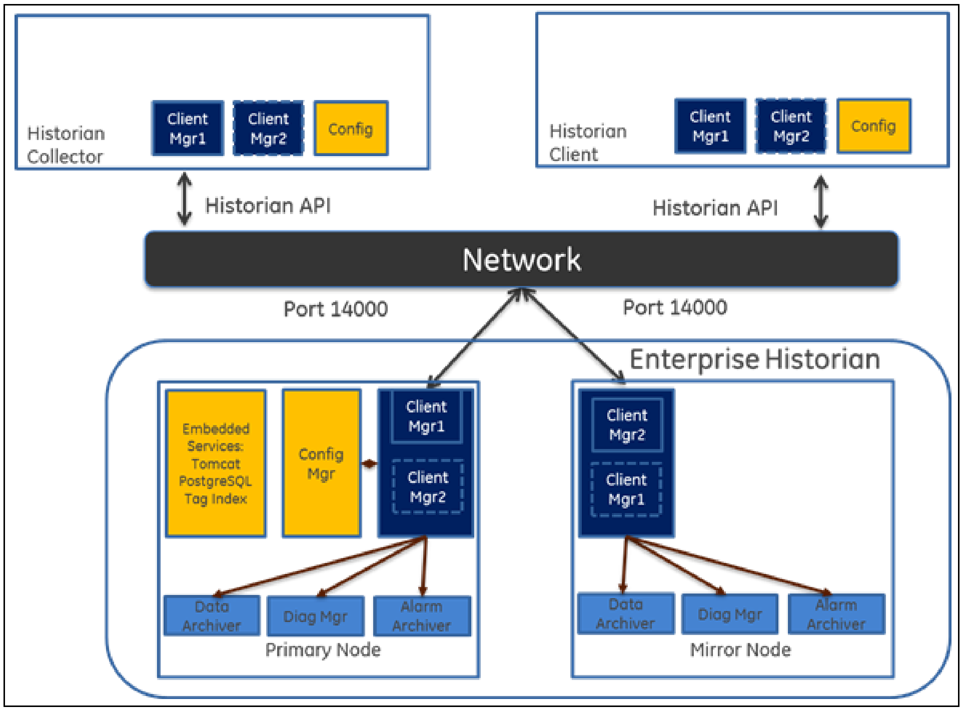
When a client (either a writing collector or reading client) connects to the Client Manager, it gathers information about each Client Manager, along with all archive, tag, and collector configuration information, from the Configuration Manager, and stores this information locally in its Windows Registry.

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.

Read and Write Client with Mirroring



Historian in a Cluster Environment

Historian works with Microsoft Cluster Service Manager to ensure high availability of the Historian server. If the primary Historian node in the cluster experiences difficulties, Historian is automatically started on another node to take over. Server high availability is managed through Microsoft Cluster Service Manager.

- Verify that all the prerequisites are installed.
- Configure a failover cluster in the Windows server. See Installing Historian in a Cluster Environment *(page 78)*.
- To use Historian Alarms and Events in a cluster environment, select the appropriate SQL Server for both the cluster nodes.

Setting Up the Historian Environment

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 Minimum Hardware Requirements for a Standard Historian *(page 30)*, 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 *(page 36)*, 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 Historian Licenses *(page 27)*.
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.

Historian Licenses

Historian Product License Management

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).

If the license is already activated on your system, you must replace it with the new one:

1. Remove the existing license.
2. Using the license client, select **Advanced**, and then select **Clear license information on this computer**.
3. Activate the new license.

Note: 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.

Note:

For all Windows operating systems, ensure that they are updated with the most recent Windows updates before installing Common Licensing.

- 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.
- If you are using Windows 8.1, follow the instructions in KB2999226.

Historian License Editions

Historian is available in three license types: Essentials, Standard, and 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.

You can install all components using the single install media, but the use of specific components and functionality are controlled by the GE license you purchase and install.

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.

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
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

Component	Essentials	Standard	Enterprise	Distributed
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 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
Trend Client	No	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 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

Component	Essentials	Standard	Enterprise	Distributed
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
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

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.

Note: 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.

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).

Minimum Hardware Requirements for a Standard Historian

Table 1. Historian Server

Hardware Component	Requirement
CPU speed, processor type, and RAM	A 2.4 GHz clock-speed Intel Core i3 or i5 or i7 CPU or an equivalent AMD Phenom CPU with a 8 GB RAM for a 64-bit Historian server.
Disk size	An 80 GB free hard-drive space for the data archives, message files, buffer files, and log files used by the system.
Other requirements	• A DVD-ROM drive. • 100 Mbps TCP/IP-compatible network interface adapter for network communication and certain I/O drivers.

Table 2. Data Collector Node

Hardware Component	Requirement
CPU speed, processor type, and RAM	A 2.0 GHz clock-speed Intel Core i3 or i5 or i7 CPU or an equivalent AMD Phenom CPU with a 2 GB RAM.
Disk size	A 40 GB free hard-drive space to store buffer data.
Other requirements	• A DVD-ROM drive. • A TCP/IP-compatible network interface adapter for network communication and certain I/O drivers.

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. **Note:** If you are using single node setup, it is recommended to use 32 GB RAM.
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.

Minimum Hardware Requirements for Historian Enterprise, Mirroring

Hardware Component	Requirement
RAM	16 GB or 32 GB (recommended)
Disk size	250 GB (minimum)
Processor type	Intel Core-i5, i7 family, or equivalent
CPU	Dual/Quad cores
CPU speed	2.8 GHz
Recommended CPU clock	2.8 GHz
Storage type	SAS SSD with RAID Level 0 configured

Hardware Component	Requirement
Operating system	• Microsoft® Windows® Server 2019 (64-bit) • Microsoft® Windows® Server 2016 (64-bit) • 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

Historian Server Sizing Recommendations

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			32 or 64
Disk Size (in GB)	100 or 250	250		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		2-socket	2-socket or 4-socket

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
CPU Speed (in GHz)	2.8	2.8		2.6	
CPU clock speed (in GHz)	2.8	2.8		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 18 million 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.

Sustained Event Rate Example System

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

Hardware Component	For a Medium-Sized Server	For a Large-Sized Server
RAM (in GB)	64	256

Historian Collector Configuration Recommendations

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
Operating system	Any of the following: • Microsoft® Windows® Server 2019 • Microsoft® Windows® Server 2016 • Microsoft® Windows® Server 2012 Standard (64-bit) • Microsoft® Windows® Server 2012 R2 • Microsoft® Windows® 10 IoT • Microsoft® Windows® 10 • Microsoft® Windows® 8.1 Professional (32-bit or 64-bit)

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.

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.

1. Access Control Panel, and then select **System** > **Advanced system settings** > **Advanced**.
2. Under **Performance**, select **Settings** > **Advanced**.
3. Under **Virtual Memory**, select **Change**.
4. In the **Initial size** and **Maximum size**fields, enter a value equal to three times your physical memory.
5. Select **Set**, and then select **OK**.

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 2019 (64-bit)
    - Microsoft® Windows® Server 2016 (64-bit)
    - 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)

  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.
- **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 Express, Standard, or Professional
- Microsoft® SQL Server® 2016 Express, Standard, or Professional
- Microsoft® SQL Server® 2014 SP1 Express, Standard, or Professional
- Microsoft® SQL Server® 2012 SP3

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 later
- **Screen Resolution:** You can access the Web Admin console and Trend Client using the following screen resolutions:
  - 1280 x 1024
  - 1366 x 768
- **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

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. This topic describes how to change these settings to optimize the performance.

1. Access the Control Panel.

2. Double-click **Network and Dial-Up Connections**.
   The **Network and Dial-up Connections** window appears.

3. Right-select **Local Area Connection Properties**, and select **Properties**.

4. Select **File and Printer Sharing for Microsoft Networks**, and select **Properties**.

5. Ensure that the **Maximize Data Throughput for Network Applications** option is selected.

6. Select **OK**.

Archiver Obtaining List of Domain Controllers

If the archiver is configured to use domain group security, the data archiver obtains the list of primary and backup domain controllers at archiver startup. If a domain controller is not available at that time or if you add new domain controllers, they are not seen by the archiver until the next time the archiver is restarted. For example, if your backup domain controller was not available on archiver startup, the archiver will not fail over to the backup domain controller for user authentication.

For more information, refer to the *Working with Security* section in Online Help.

Windows Firewall Enabled by Default

Windows Firewall is enabled by default in Vista, Server 2003, Server 2008, and Server 2012.

If you install Historian on any of the given systems, you will be prompted to allow Historian to reconfigure the Windows Firewall. If you answer **Yes**, Historian is added to the firewall's exception list and set to **Enabled**. If you answer **No**, Historian is added to the list and set to **Disabled**. You can change this setting through the Windows Firewall control panel at any time.

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.

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	10.0, 11.0
iFIX	6.1, 6.5
Plant Applications	8.0, 8.1
Workflow	2.5 SP4, 2.6 SP1
Operations Hub	2.0, 2.1

* 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 *(page 87)*.

! **Important:** Do not install Operations Hub and Web-based Clients on the same machine.

Additional Setup Information

See the topics below for additional setup information.

Regional Settings Support

Historian supports the following regional settings available in the Windows Control Panel:

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

Time and Date Formatting

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. Changing these values to non-standard styles may result in improperly formatted times and dates.

Data Type Support

The following table lists the supported Historian data types and their sizes:

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
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

Enable Trust for Proficy Historian for a Self-signed Certificate on Chrome

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 Files**.

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.

Installing the Historian Server

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 *(page 26)*.
4. On the server node, launch the installer, select **Install Historian**, and follow the on-page instructions to install Historian on a single server *(page 47)* on in a distributed *(page 55)* environment.
5. Activate your product license at http://digitalsupport.ge.com.

6. Install the collectors *(page 104)*.
7. Restart your computer if prompted to do so.
8. As needed, install Web-based Clients *(page 86)*.
9. 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	Installing the Historian server is mandatory to work with Historian. If you want to use Web-based Clients, you must provide the User Account and Authentication (UAA) server details while installing the Historian server. When you install the Historian server, the following components are installed as well: • **The RemoteCollectorConfigurator utility:** A command-line tool, which allows you to manage collectors remotely. • **The UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA server used by Web-based Clients.
Alarms and Events	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.
Collectors	Installing collectors is mandatory to collect and store data in Historian. 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. When you install collectors, if iFIX/CIMPLICITY are installed on the same machine, instances of the following collectors are created automatically: • 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	Install Client Tools if you want the following components: • 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	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. To use Web-based Clients, you need a UAA server to handle user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2. During the Web-based Clients installation, you can choose to install a UAA instance and Configuration Hub, or you can use existing ones.
Excel Add-in for Historian	Install Excel Add-in for Historian make bulk changes to tag parameters using Excel, and then 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	Install Excel Add-in for Operations Hub if you want to query historical data of objects and object types defined in Operations Hub.
Standalone Help	Install Standalone Help to access the Historian product documentation offline.
Historian ETL Tools	Install the Historian Extract, Transform, and Load (ETL) tools if you want to transfer data where there is limited internet connectivity.
Historian Remote Management Agents	Remote Management Agents (RMA) include Remote Collector Manager, which is used to manage collectors remotely. 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.
Historian OPC UA HDA Server	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.

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 nodes.

For all these types of installation, you can use the GUI-based installer or the Command Prompt window. You can also install Historian in a clustered environment.

This topic provides the high-level steps in installing the Historian server for the first time. You can perform the same steps to upgrade the server. However, before you upgrade, refer to the things to remember *(page 141)*.

Note:

- The number of alarms in the Historian Alarms and Eventss 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.
- To add a component, re-run the installer and select the check box for that component. Do not clear the check box for previously installed component. If you do so, it will be uninstalled.
- Collectors will appear in Historian Administrator only when they are started.

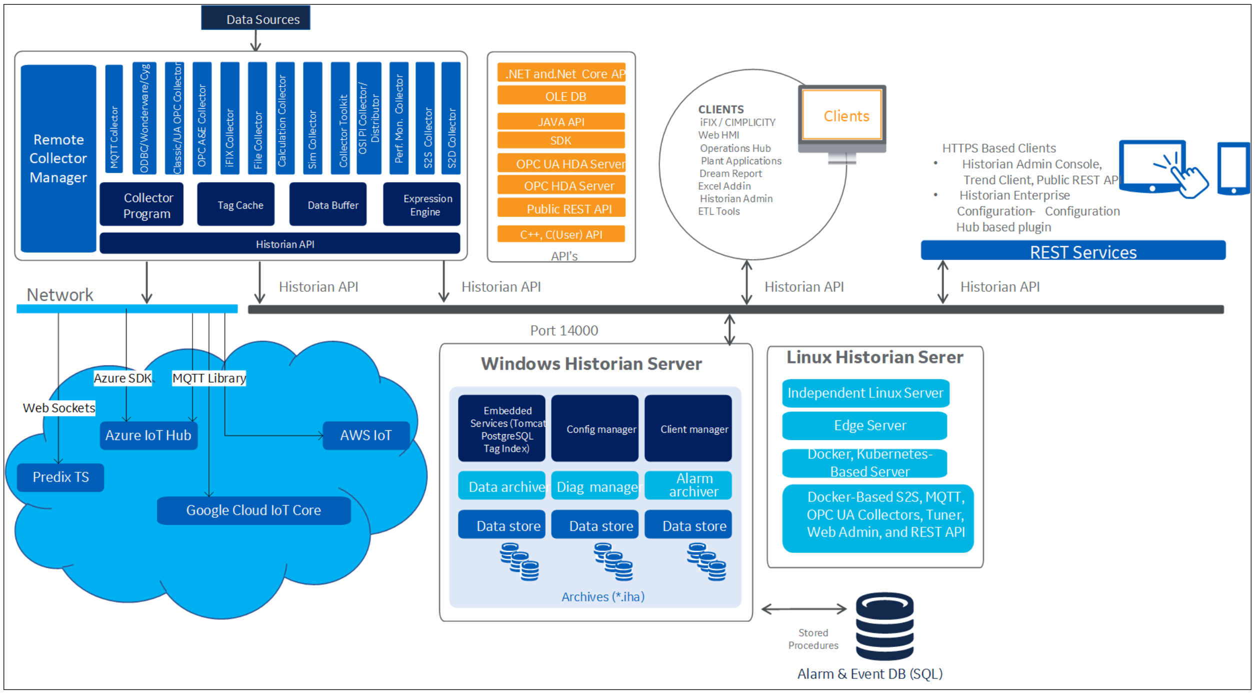
About Historian Log Files

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.

Architecture of Single-Server Historian

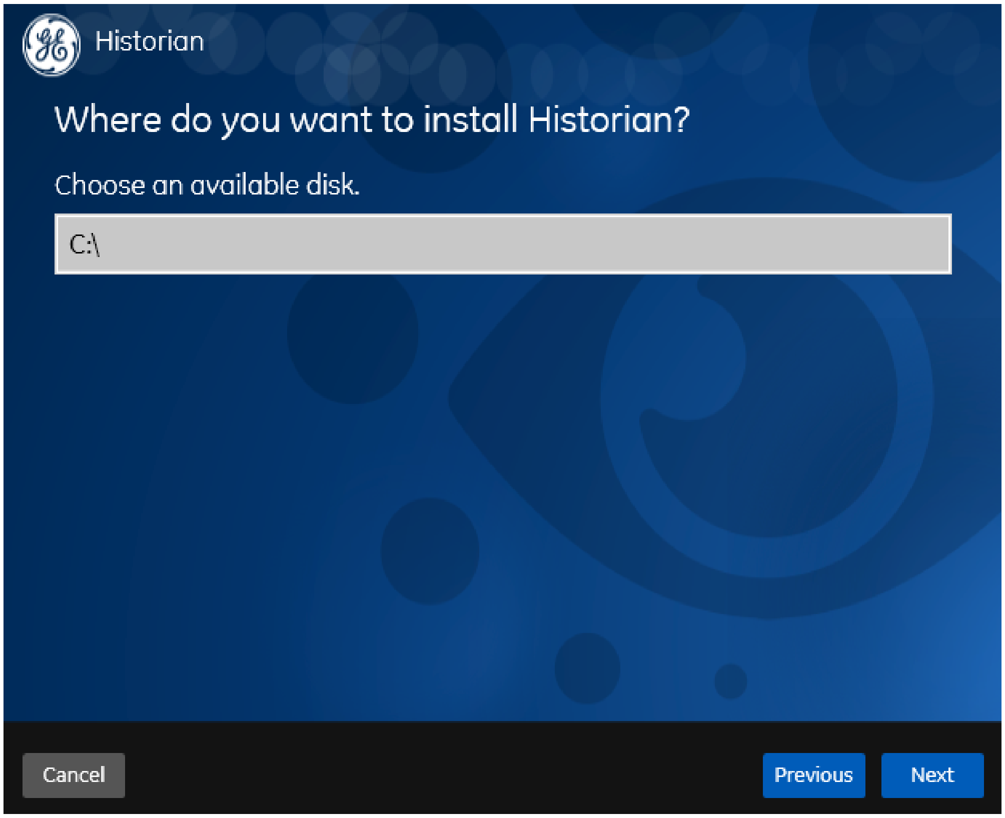


Install Single-Server Historian Using the Installer

- Set up the Historian environment *(page 26)*.
- If you are changing the role of a Historian server that was previously a distributed node in any other configuration (single-server or mirror primary server), you must first uninstall Historian *(page 187)*.

This topic describes how to install single-server Historian using the installer. You can also install single-server Historian at a command prompt *(page 53)*.

1. Log in as an administrator to the machine on which you want to install Historian.
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.



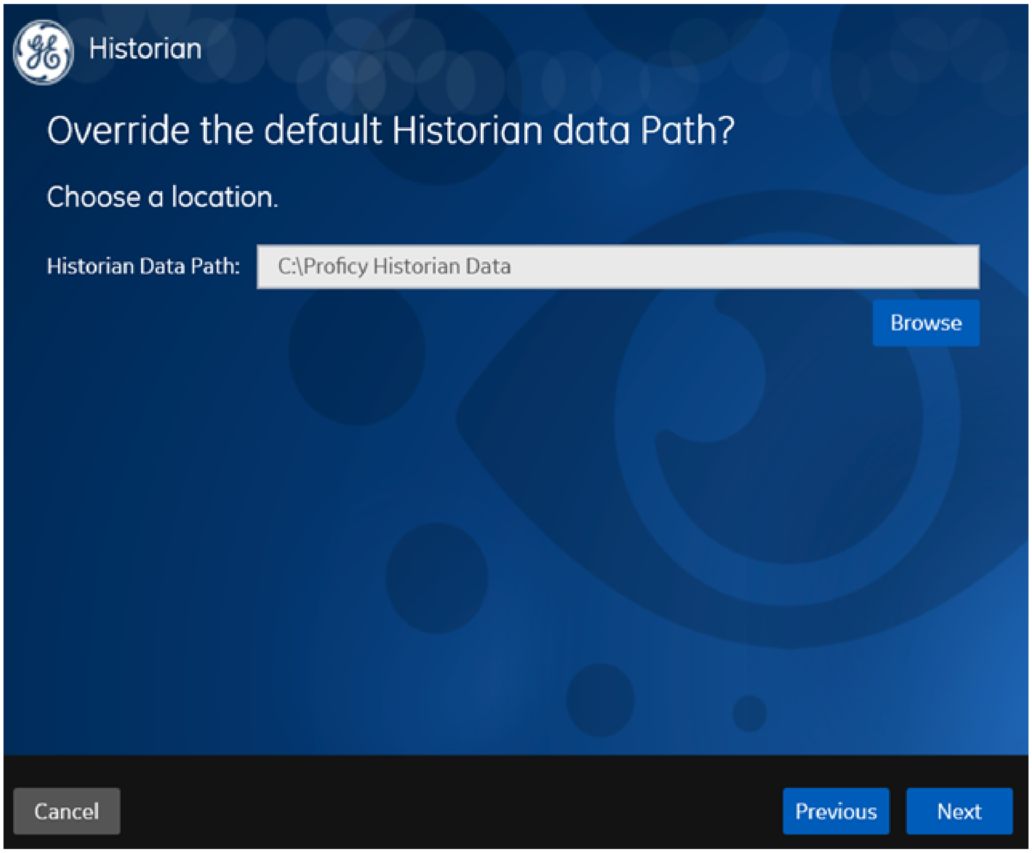
Historian

Where do you want to install Historian?

Choose an available disk.

C:\

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.



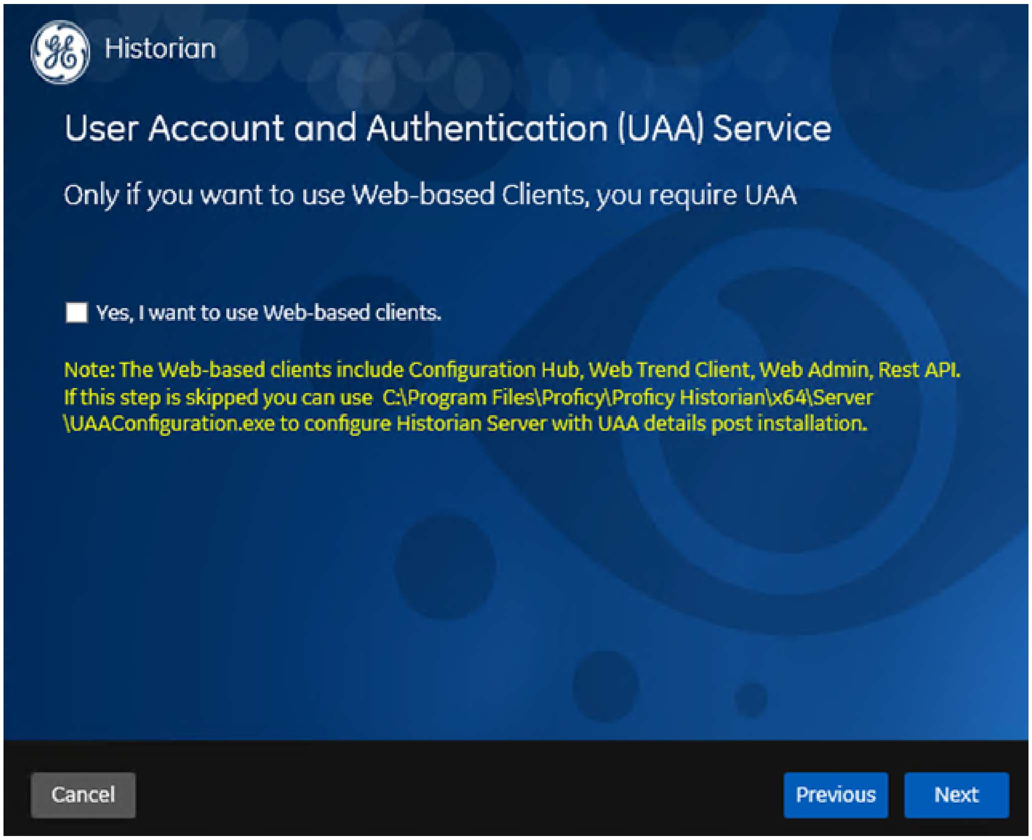
Override the default Historian data Path?

Choose a location.

Historian Data Path: C:\Proficy Historian Data

7. If needed, change the default folder of the log files, and then select **Next**.
   The **User Account and Authentication (UAA) 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 UAA. Otherwise, you can skip this step. If you use Web-based Clients, UAA is required for user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.



User Account and Authentication (UAA) Service

Only if you want to use Web-based Clients, you require UAA

□ Yes, I want to use Web-based clients.

Note: The Web-based clients include Configuration Hub, Web Trend Client, Web Admin, Rest API. If this step is skipped you can use C:\Program Files\Proficy\Proficy Historian\x64\Server \UAAConfiguration.exe to configure Historian Server with UAA details post installation.

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
UAA server name	Enter the name of the machine on which the UAA 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 UAA 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:

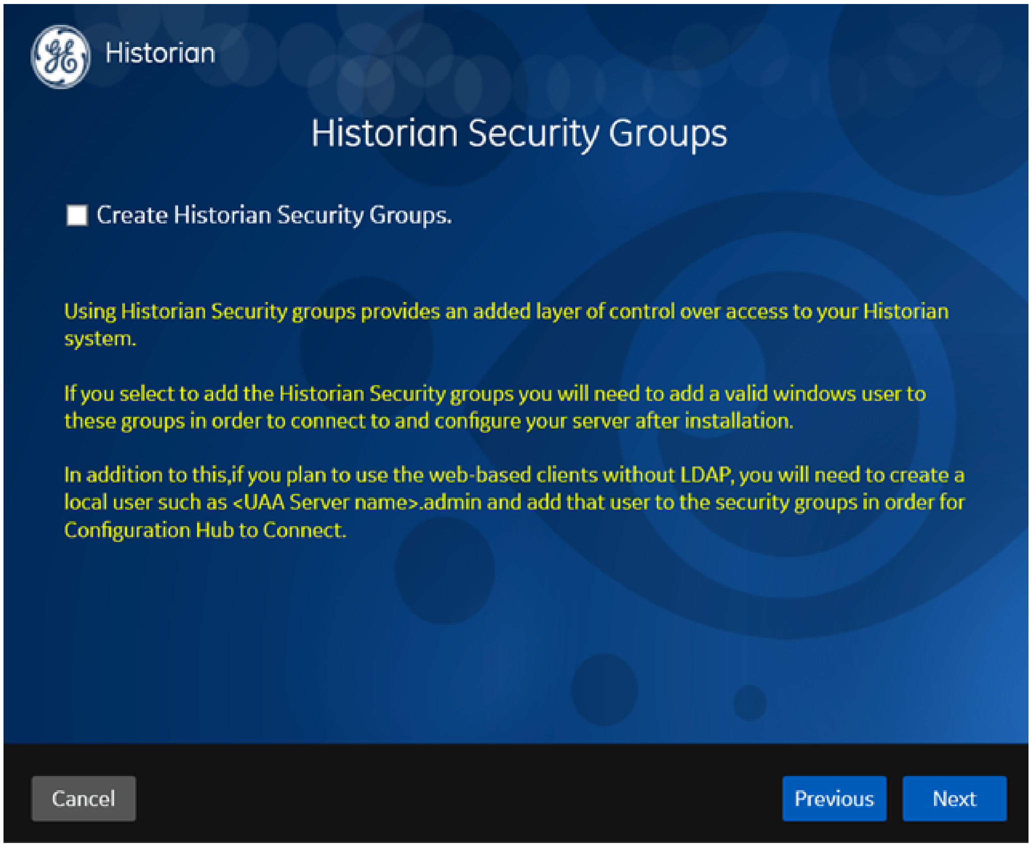
- You can install a UAA service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing UAA instance. Or, if a UAA service is not available, you can install it during Web-based Clients installation.
- If you change the UAA server for Web-based Clients later, you must change the UAA server for the Historian server *(page 75)* as well. You can do so using the UAA 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.



Historian Security Groups

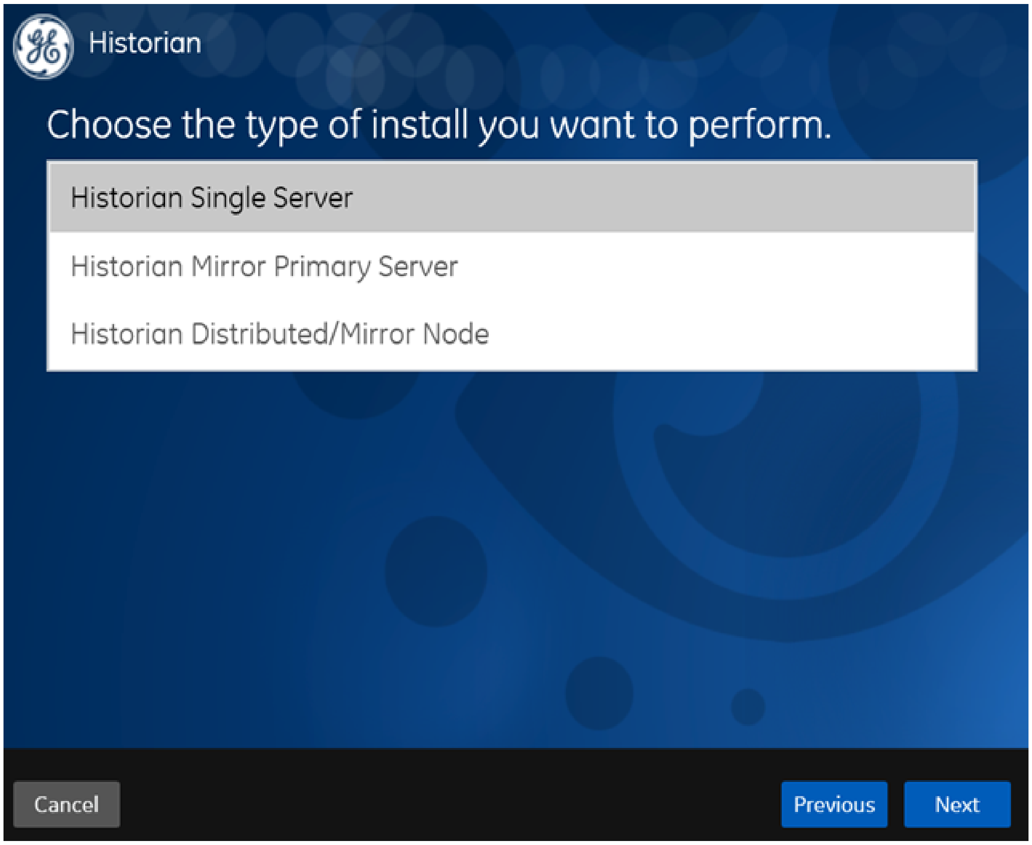
□ Create Historian Security Groups.

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

If you select to add the Historian Security groups you will need to add a valid windows user to these groups in order to connect to and configure your server after installation.

In addition to this,if you plan to use the web-based clients without LDAP, you will need to create a local user such as <UAA Server name>.admin and add that user to the security groups in order for Configuration Hub to Connect.

10. If you want the installer to create Historian security groups *(page 167)*, select the corresponding check box, and then select **Next**.
    The **Choose the type of install you want to perform** page appears.



Historian

Choose the type of install you want to perform.

Historian Single Server

Historian Mirror Primary Server

Historian Distributed/Mirror Node

11. Select **Historian Single Server**, and then select **Next**.
    The **Ready to Install** page appears.

12. Select **Install**.
    The installation begins.

13. When you are asked to reboot your system, select **Yes**.
    Single-Server Historian is installed on your machine. 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 UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA 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 UAA Server.

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.

This user will log in to Web-based Clients.

Alternatively, you can create UAA users in an external UAA and map their security groups. For information, refer to About UAA Groups *(page 129)*.

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

Install Single-Server Historian at a Command Prompt

- If you are changing the role of a Historian server that was previously a distributed node in any other configuration (single-server or mirror primary server), you must first uninstall Historian *(page 187)*.

This topic describes how to install single-server Historian at a command prompt. You can also install single-server Historian using the installer *(page 47)*.

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=StandAlone
   ```

   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.
`HistAdministratorPassword`	The password for the built-in administrator account.

Argument	Description
`ActiveUaaBaseUrl`	The URL to connect to UAA to allow Web-based Clients to access Historian. Only if you want to use Web-based Clients, this parameter is required for user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2. UAA details are required if you want to use Web-based Clients. By default, the local hostname and the port number of 443 are considered. If the UAA service is on the same machine on which you are installing the Historian server, you can accept the default value. If, however, the UAA service is on a different machine or uses a different port number, replace those values in the URL as follows: `https://<local host name>:<port number>/uaa` where: • *<UAA server>* is the name of the machine on which UAA is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. • *<port number>* is the one that you have specified for the public https port in the **TCP Port Assignments** page during Web-based Clients installation. **Note:** You can install a UAA service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing UAA instance. Or, if a UAA service is not available, you can install it during Web-based Clients installation. In that case, provide the server name where UAA is installed.
`CreateHistorianSecurityGroups`	Indicates whether you want the installer to create Historian security groups. Using Historian security groups provides an added layer of control over access to your Historian system. Enter true or false. If you enter true: • You must add a Windows user to the appropriate group *(page 174)* (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 *(page 174)* (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 *(page 163)*.

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.

Flag	Description
`/t`	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. By default, this file is named `Template_Historian.xml`, and it is placed in the `temp` folder, defined by the`%temp%` environment variable. If, however, you want to save the file in another folder as well, enter: `/t TemplateOutputDirectory=<path>`
`/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.

Single-Server Historian is installed on your machine. 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 UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA 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 UAA Server.

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.

This user will log in to Web-based Clients.

Alternatively, you can create UAA users in an external UAA and map their security groups. For information, refer to About UAA Groups *(page 129)*.

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

About Installing Historian in a Distributed Environment

A distributed environment implies 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 *(page 56)*, whereas the others are the distributed nodes *(page 64)*. Configuration Manager and the embedded web services are installed only on the primary server, which are used by the distributed nodes 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.

Install Historian Mirror Primary Server Using the Installer

- Set up the Historian environment *(page 26)*.
- If you are changing the role of a Historian server that was previously a distributed node in any other configuration (single-server or mirror primary server), you must first uninstall Historian *(page 187)*.

This topic describes how to install the Historian mirror primary server using the installer. You can also install it at a command prompt *(page 62)*.

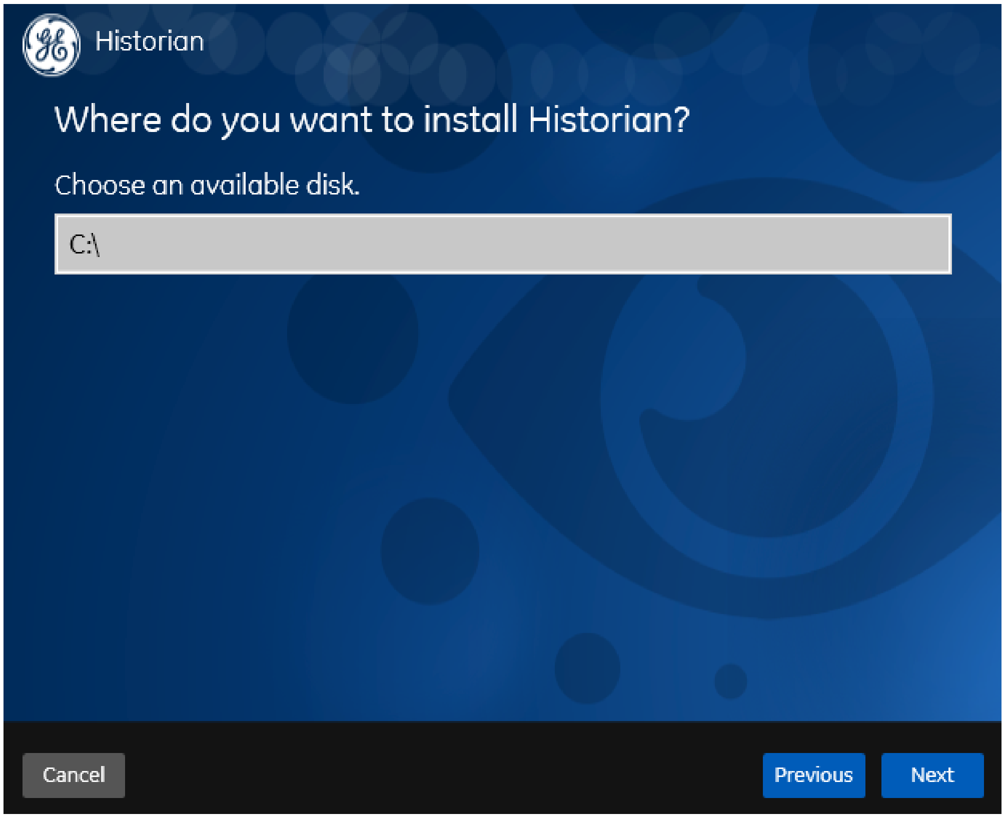
1. Log in as an administrator to the machine on which you want to install Historian.

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.

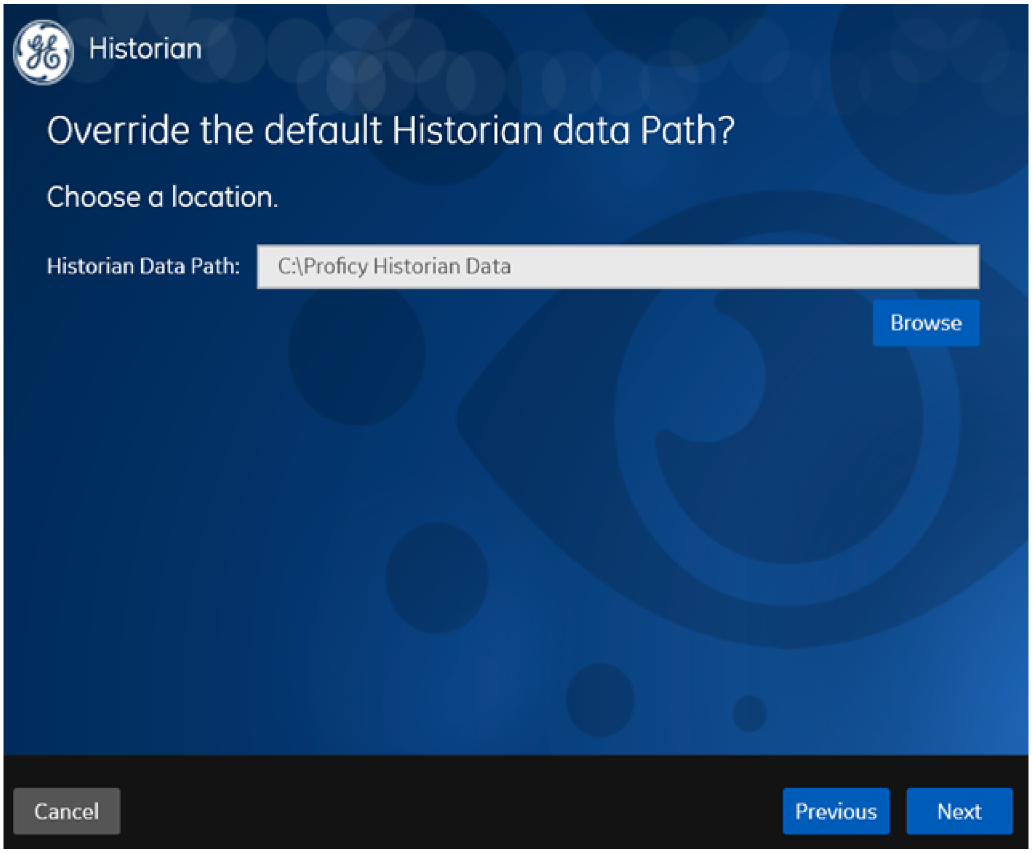


Where do you want to install Historian?

Choose an available disk.

C:\

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.



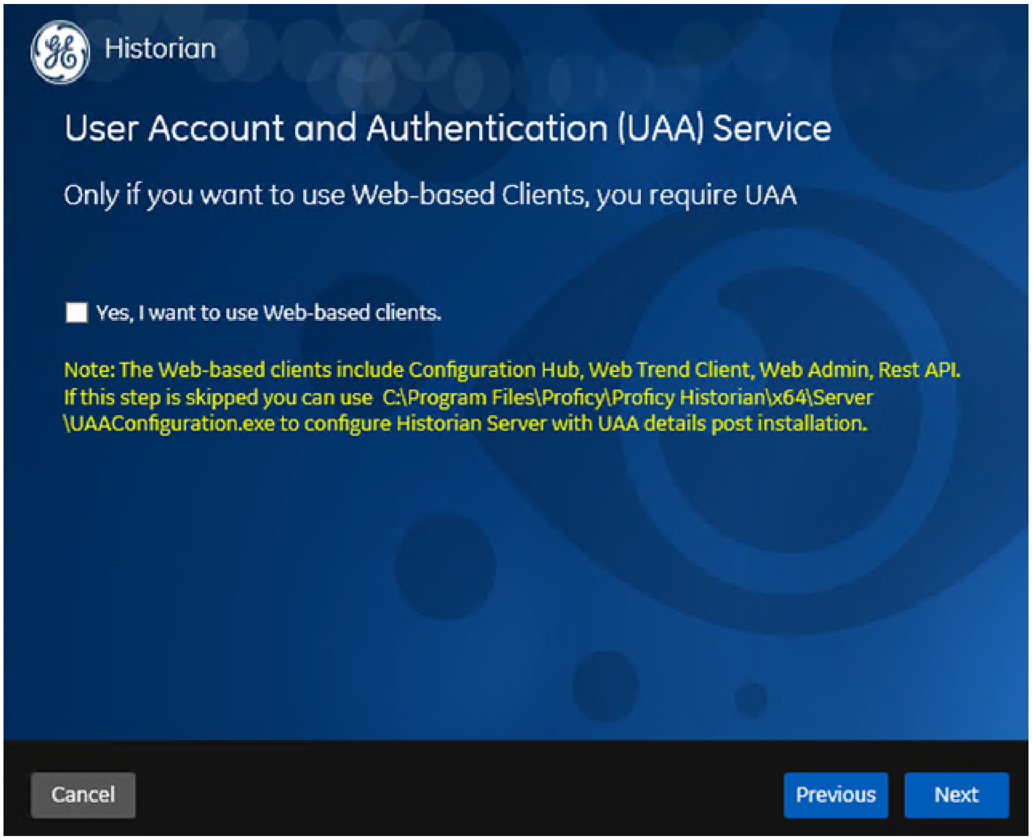
Override the default Historian data Path?

Choose a location.

Historian Data Path: C:\Proficy Historian Data

7. If needed, change the default folder of the log files, and then select **Next**.
   The **User Account and Authentication (UAA) 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 UAA. Otherwise, you can skip this step. If you use Web-based Clients, UAA is required for user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.



User Account and Authentication (UAA) Service

Only if you want to use Web-based Clients, you require UAA

□ Yes, I want to use Web-based clients.

Note: The Web-based clients include Configuration Hub, Web Trend Client, Web Admin, Rest API. If this step is skipped you can use C:\Program Files\Proficy\Proficy Historian\x64\Server \UAAConfiguration.exe to configure Historian Server with UAA details post installation.

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.

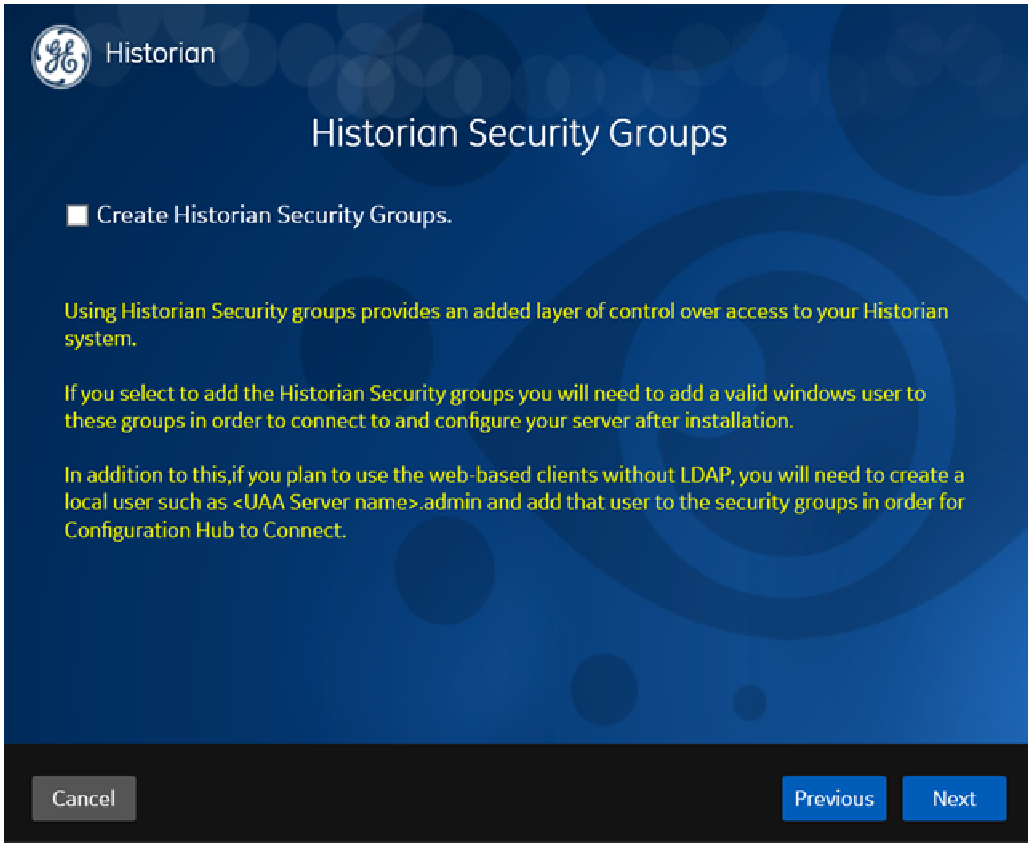
Field	Description
UAA server name	Enter the name of the machine on which the UAA server is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. By default, the local hostname is considered.
Public https port	Enter the port number used by the UAA service. The default 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 UAA service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing UAA instance. Or, if a UAA service is not available, you can install it during Web-based Clients installation.

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.



Historian Security Groups

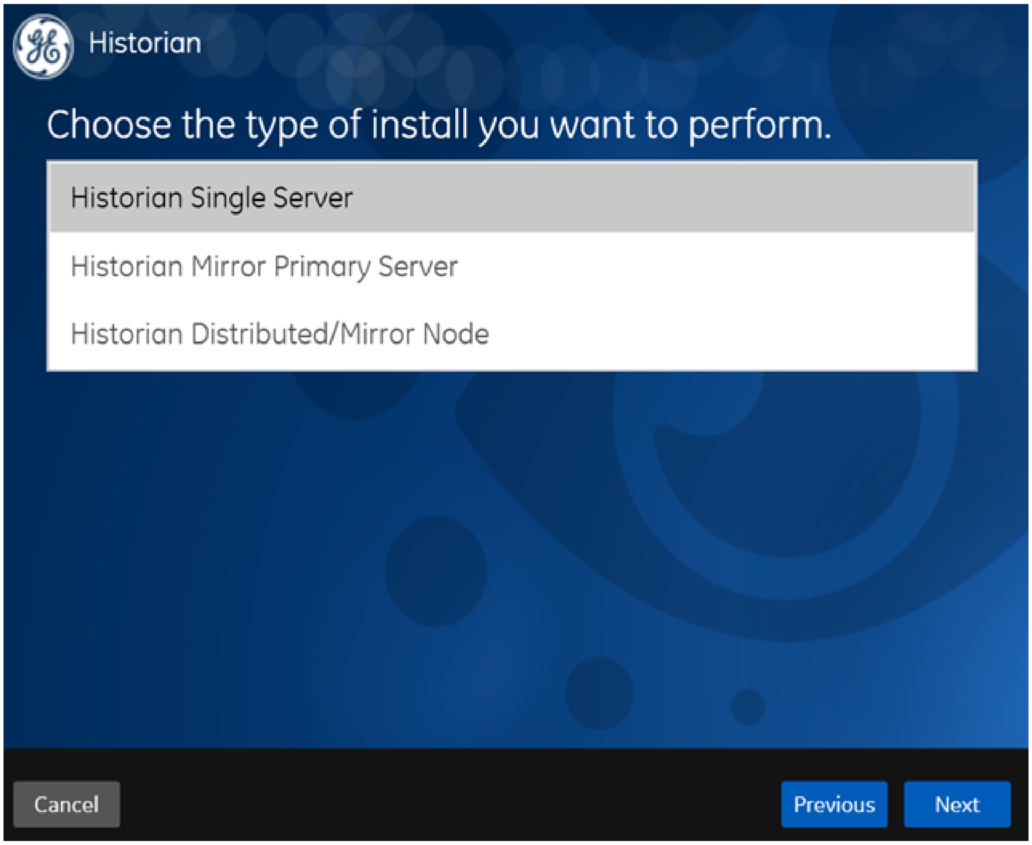
□ Create Historian Security Groups.

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

If you select to add the Historian Security groups you will need to add a valid windows user to these groups in order to connect to and configure your server after installation.

In addition to this,if you plan to use the web-based clients without LDAP, you will need to create a local user such as <UAA Server name>.admin and add that user to the security groups in order for Configuration Hub to Connect.

10. If you want the installer to create Historian security groups *(page 167)*, select the corresponding check box, and then select **Next**.
    The **Choose the type of install you want to perform** page appears.



Choose the type of install you want to perform.

Historian Single Server

Historian Mirror Primary Server

Historian Distributed/Mirror Node

11. Select **Historian Mirror Primary Server**, and then select **Next**.
    The **Ready to Install** page appears.

12. Select **Install**.
    The installation begins.

13. When you are asked to reboot your system, select **Yes**.
    Historian mirror primary server is installed. 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 UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA 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 UAA Server.

1. Install the distributed nodes using the installer *(page 64)* or at a command prompt *(page 70)*.
2. 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.

This user will log in to Web-based Clients.

Alternatively, you can create UAA users in an external UAA and map their security groups. For information, refer to About UAA Groups *(page 129)*.

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

Install Historian Mirror Primary Server at a Command Prompt

- Set up the Historian environment *(page 26)*.
- If you are changing the role of a Historian server that was previously a distributed node in any other configuration (single-server or mirror primary server), you must first uninstall Historian *(page 187)*.

This topic describes how to install the Historian mirror primary server at a command prompt. You can also install it using the installer *(page 56)*.

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 [-q] [-quiet] [-s] [-silent] [-passive]
    HistorianCmd=HistorianCore
   ```

   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.
`HistAdministratorPassword`	The password for the built-in administrator account.

Argument	Description
`ActiveUaaBaseUrl`	The URL to connect to UAA to allow Web-based Clients to access Historian. UAA is required for user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2. UAA details are required if you want to use Web-based Clients. By default, the local hostname and the port number of 443 are considered. If the UAA service is on the same machine on which you are installing the Historian server, you can accept the default value. If, however, the UAA service is on a different machine or uses a different port number, replace those values in the URL as follows: `https://<local host name>:<port number>/uaa` where: • *<UAA server>* is the name of the machine on which UAA is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. • *<port number>* is the one that you have specified for the public https port in the **TCP Port Assignments** page during Web-based Clients installation. **Note:** You can install a UAA service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing UAA instance. Or, if a UAA service is not available, you can install it during Web-based Clients installation. In that case, provide the server name where UAA is installed.
`CreateHistorianSecurityGroups`	Indicates whether you want the installer to create Historian security groups. Using Historian security groups provides an added layer of control over access to your Historian system. Enter true or false. If you enter true: • You must add a Windows user to the appropriate group *(page 174)* (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 *(page 174)* (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 *(page 163)*.

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.

Flag	Description
`/t`	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. By default, this file is named `Template_Historian.xml`, and it is placed in the `temp` folder, defined by the`%temp%` environment variable. If, however, you want to save the file in another folder as well, enter: `/t TemplateOutputDirectory=<path>`
`/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.

Historian mirror primary server is installed. 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 UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA 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 UAA Server.

1. Install the distributed nodes using the installer *(page 64)* or at a command prompt *(page 70)*.
2. 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.

   This user will log in to Web-based Clients.

   Alternatively, you can create UAA users in an external UAA and map their security groups. For information, refer to About UAA Groups *(page 129)*.

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

Install Historian Distributed/Mirror Node Using the Installer

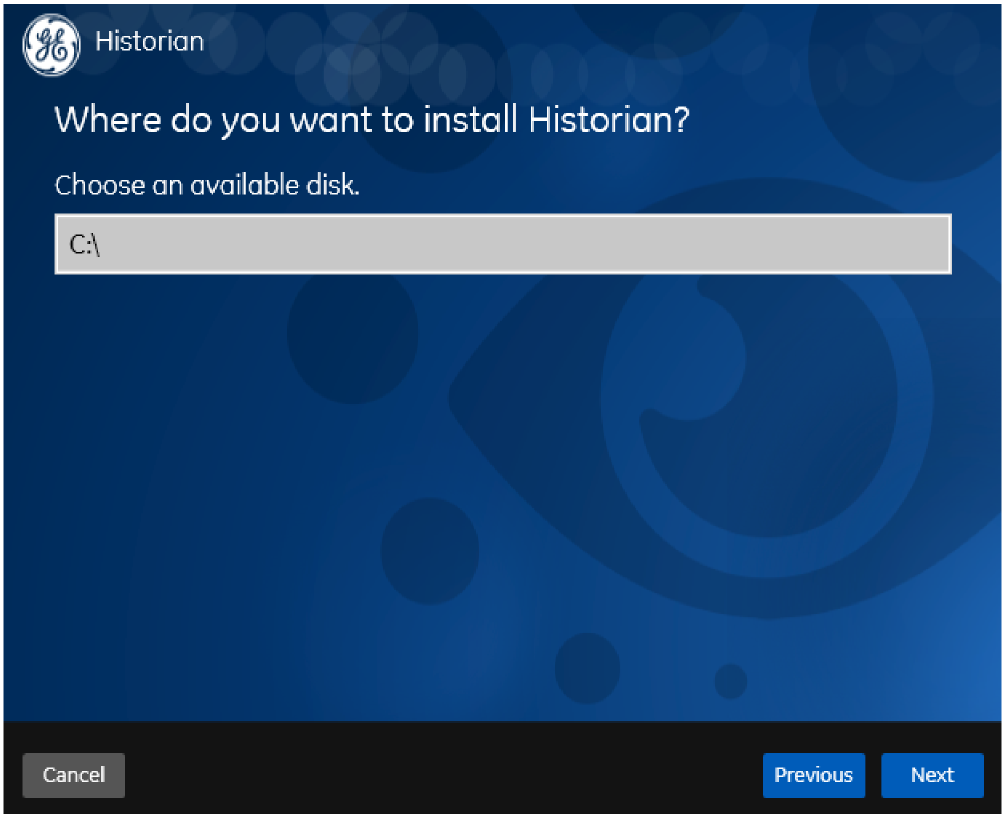
- Install the mirror primary server using the installer *(page 56)* or the command line *(page 62)*. Use the same configuration, license key, installation drive, UAA instance, and domain as the primary server.
- Disable global security (strict client and collector authentication).

- If you are changing the role of a Historian server that was previously a distributed node in any other configuration (single-server or mirror primary server), you must first uninstall Historian *(page 187)*.

Note: If the primary server is down, you cannot add tags using a distributed node because the Configuration Manager is down.

This topic describes how to install Historian distributed node using the installer. You can also install it at a command prompt *(page 70)*.

1. Log in as an administrator to the machine on which you want to install Historian.
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.



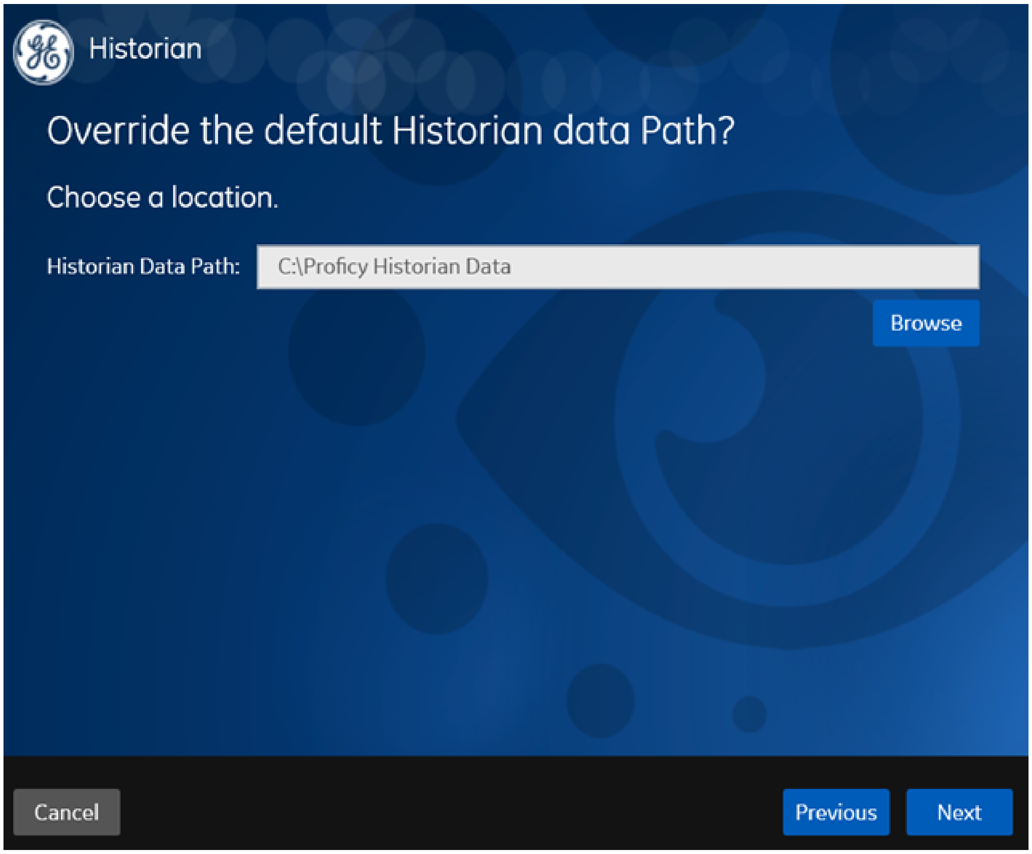
Where do you want to install Historian?

Choose an available disk.

C:\

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.



Historian

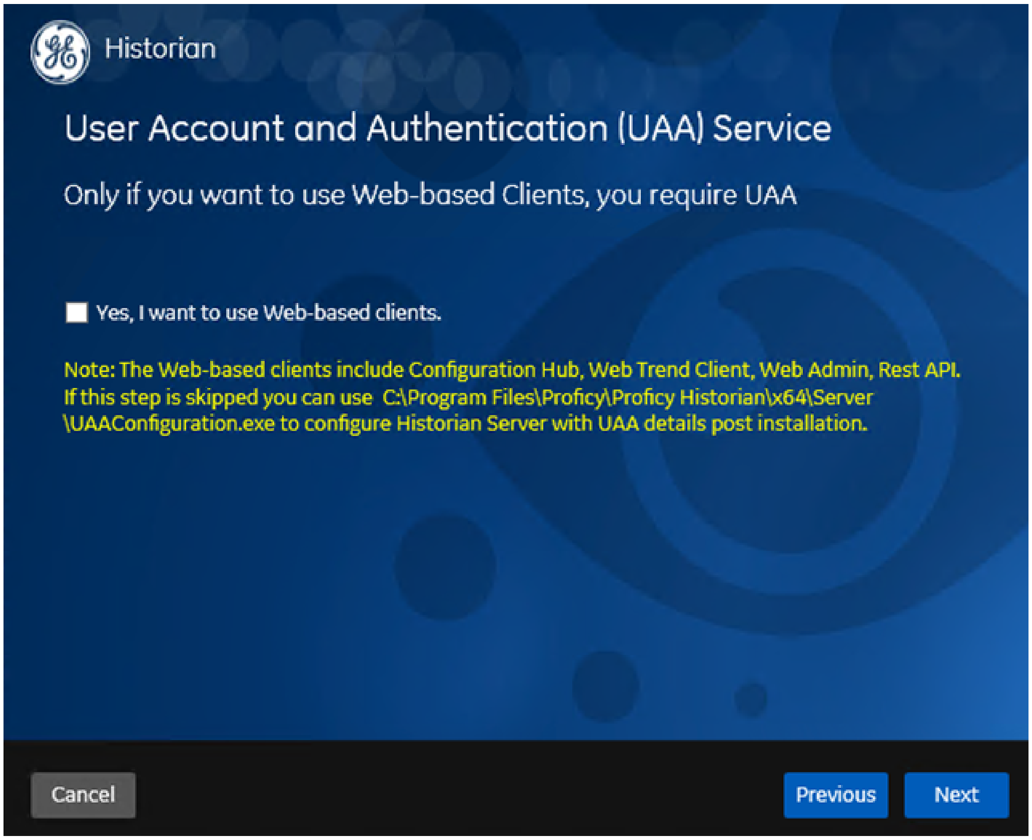
Override the default Historian data Path?

Choose a location.

Historian Data Path: C:\Proficy Historian Data

7. If needed, change the default folder of the log files, and then select **Next**.
   The **User Account and Authentication (UAA) 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 UAA. Otherwise, you can skip this step. If you use Web-based Clients, UAA is required for user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2.



User Account and Authentication (UAA) Service

Only if you want to use Web-based Clients, you require UAA

□ Yes, I want to use Web-based clients.

Note: The Web-based clients include Configuration Hub, Web Trend Client, Web Admin, Rest API. If this step is skipped you can use C:\Program Files\Proficy\Proficy Historian\x64\Server \UAAConfiguration.exe to configure Historian Server with UAA details post installation.

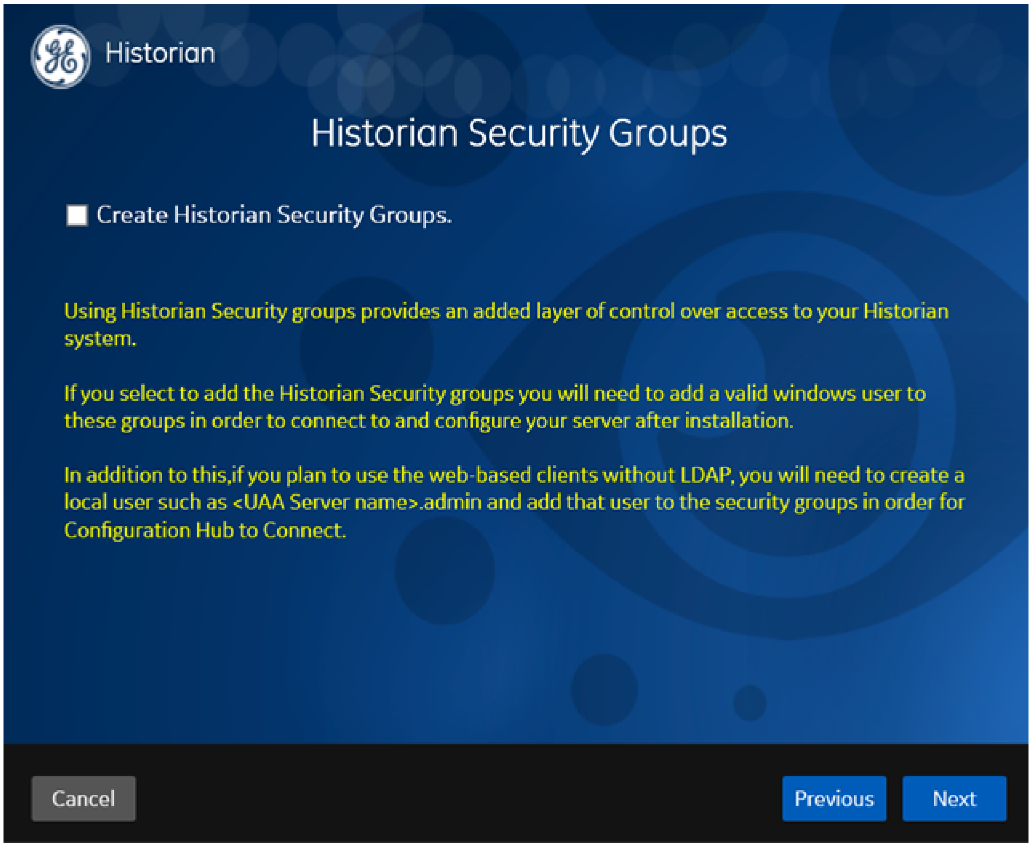
8. If you want to use Web-based Clients, select the **Yes, I want to use Web-based Clients** check box, and provide values as described in the following table.

Field	Description
UAA server name	Enter the name of the machine on which the UAA 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 UAA 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 UAA service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing UAA instance. Or, if a UAA service is not available, you can install it during Web-based Clients installation.

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.



Historian Security Groups

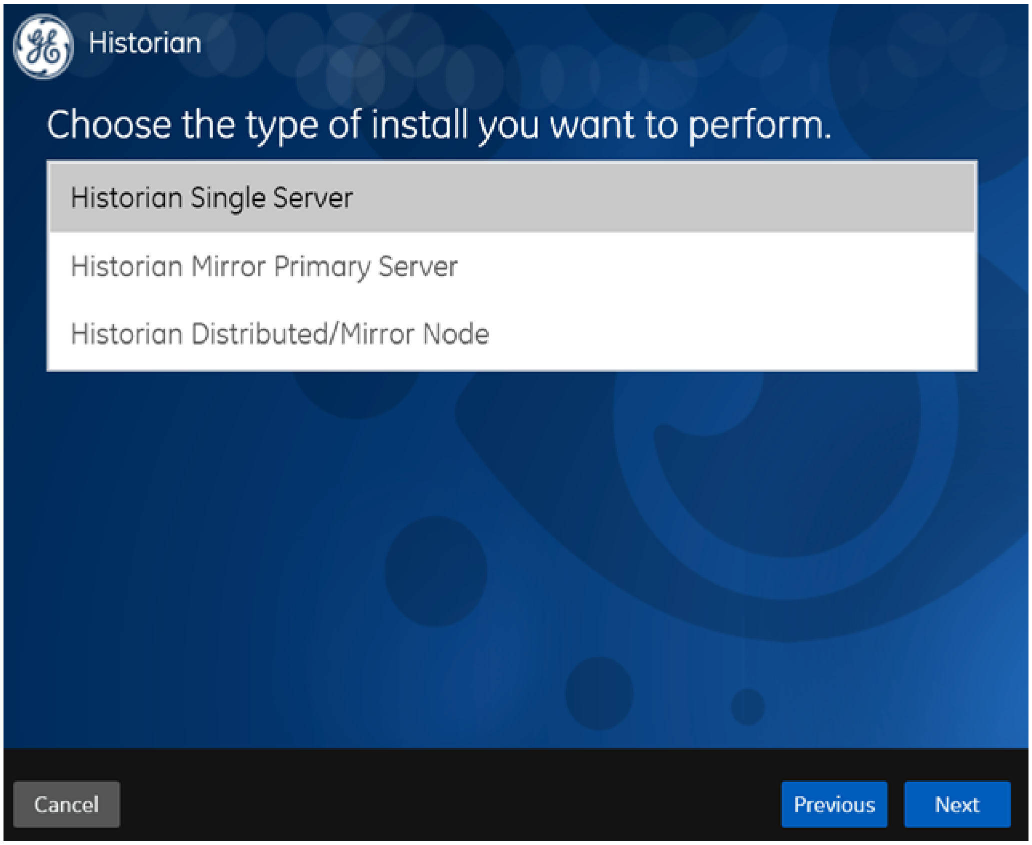
□ Create Historian Security Groups.

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

If you select to add the Historian Security groups you will need to add a valid windows user to these groups in order to connect to and configure your server after installation.

In addition to this,if you plan to use the web-based clients without LDAP, you will need to create a local user such as <UAA Server name>.admin and add that user to the security groups in order for Configuration Hub to Connect.

10. If you want the installer to create Historian security groups *(page 167)*, select the corresponding check box, and then select **Next**.
    The **Choose the type of install you want to perform** page appears.



Choose the type of install you want to perform.

- Historian Single Server
- Historian Mirror Primary Server
- Historian Distributed/Mirror Node

11. Select **Historian Distributed/Mirror Node**, and then select **Next**.
    The **Ready to Install** page appears.

12. Select **Install**.
    The installation begins.

13. When you are asked to reboot your system, select **Yes**.
    Historian distributed/mirror node is installed. 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 UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA 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 UAA Server.

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.

This user will log in to Web-based Clients.

Alternatively, you can create UAA users in an external UAA and map their security groups. For information, refer to About UAA Groups *(page 129)*.

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

Install Historian Distributed/Mirror Node at a Command Prompt

- Install the mirror primary server using the installer *(page 56)* or the command line *(page 62)*. Use the same configuration, license key, installation drive, UAA instance, and domain as the primary server.
- Disable global security (strict client and collector authentication).
- If you are changing the role of a Historian server that was previously a distributed node in any other configuration (single-server or mirror primary server), you must first uninstall Historian *(page 187)*.

Note: If the primary server is down, you cannot add tags using a distributed node because the Configuration Manager is down.

You can install a Historian distributed node at a command prompt. You can also install it using the installer *(page 64)*.

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 [-q] [-quiet] [-s] [-silent] [-passive] HistorianCmd=mirror
   ```

   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.
`HistAdministratorPassword`	The password for the built-in administrator account.

Argument	Description
`ActiveUaaBaseUrl`	The URL to connect to UAA to allow Web-based Clients to access Historian. UAA is required for user authentication. UAA provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2. UAA details are required if you want to use Web-based Clients. By default, the local hostname and the port number of 443 are considered. If the UAA service is on the same machine on which you are installing the Historian server, you can accept the default value. If, however, the UAA service is on a different machine or uses a different port number, replace those values in the URL as follows: `https://<local host name>:<port number>/uaa` where: • *<UAA server>* is the name of the machine on which UAA is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. • *<port number>* is the one that you have specified for the public https port in the **TCP Port Assignments** page during Web-based Clients installation. **Note:** You can install a UAA service using Operations Hub or Historian Web-based Clients. You can provide the URL of an existing UAA instance. Or, if a UAA service is not available, you can install it during Web-based Clients installation. In that case, provide the server name where UAA is installed. **Important:** Provide the same UAA details that you entered while installing the primary server.
`CreateHistorianSecurityGroups`	Indicates whether you want the installer to create Historian security groups. Using Historian security groups provides an added layer of control over access to your Historian system. Enter true or false. If you enter true: • You must add a Windows user to the appropriate group *(page 174)* (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 *(page 174)* (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 *(page 163)*.

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.

Flag	Description
`/t`	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. By default, this file is named `Template_Historian.xml`, and it is placed in the `temp` folder, defined by the`%temp%` environment variable. If, however, you want to save the file in another folder as well, enter: `/t TemplateOutputDirectory=<path>`
`/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.

Historian distributed/mirror node is installed. 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 UAA Configuration tool:** A utility that allows you to specify the UAA server details to match with the UAA 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 UAA Server.

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.

This user will log in to Web-based Clients.

Alternatively, you can create UAA users in an external UAA and map their security groups. For information, refer to About UAA Groups *(page 129)*.

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

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.
- 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 synching?

  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 UAA Server

Install Web-based Clients *(page 86)*, specifying the details of the new UAA server.

The Historian server and Web-based Clients must always point to the same UAA 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 UAA server used by Web-based Clients, the Historian server must point to the same UAA server.

This topic describes how to update the UAA 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 **UAA Configuration tool** window appears, displaying the UAA server name and port number that you specified while installing the Historian server.

2. In the **UAA server name** and **Public https port** fields, provide the values of the UAA 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 UAA 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 UAA server. If you cannot ping the UAA 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 UAA server machine:
  - GE Operations Hub Httpd Reverse Proxy
  - GE Operations Hub UAA Tomcat Web Server
- Verify that the UAA server details provided during Web-based Clients installation match the ones you have specified in the UAA Configuration tool.

Folders and Registry Keys Created During Installation

Historian provides a single install program on a DVD or ISO with options that install each system component.

The following table provides the information about installation locations of various Historian components regarding their root file path and root registry path from Historian 7.0 SP6 onwards.

Component		File path	Registry path
Alarm Archiver		`<`*`installation drive`*`>:\Program Files\Proficy \Proficy Historian \x86\Server`	`HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node\ Intellution, Inc.\iHistorian\Services \AlarmArchiver`

Component		File path	Registry path
Client Tools		<*installation drive*>:\Program Files\Proficy\Proficy Historian\x86\<Client tool name>	None
Collectors – 32 bit		<*installation drive*>:\Program Files (x86)\GE Digital\<collector name>	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ GE Digital\iHistorian\Services\<*collector name*>
Collectors – 64 bit		<*installation drive*>:\Program Files\GE Digital\<*collector name*>	HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\iHistorian\Services\<*collector name*>
The iFIX collector and the iFIX Alarms and Events collector - 32 bit		C:\Program Files\GE\iFIX	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ Intellution, Inc.\iHistorian\Services\<*collector name*>
The OPC Classic DA collector and the OPC Classic Alarms and Events collector – 32 bit		<*installation drive*>:\Program Files (x86)\GE Digital\<*collector name*>	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ Intellution, Inc.\iHistorian\Services\<*collector name*>
Help		C:\Program Files\Proficy\Proficy Historian\ProficyDoc	None
Historian Extract, Transform, and Load (ETL) tools - both 32 bit and 64 bit		• C:\Program Files\GE Digital\Historian ETL Extract • C:\Program Files\GE Digital\Historian ETL PI Extract • C:\Program Files\GE Digital\Historian ETL Load • C:\Program Files\GE Digital\Historian ETL Transform	• HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL Extract • HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL PI Extract • HKEY_LOCAL_MACHINE\SOFTWARE\GE Digital\Historian ETL Load

Component		File path	Registry path
Historian Web-based Clients		• C:\Program Files \GE • C:\Program Files \GE	• HKEY_LOCAL_MACHINE\SOFTWARE \GE Digital • HKEY_LOCAL_MACHINE\SOFTWARE \GE
Remote Collector Management - 32 bit and 64 bit		C:\Program Files\GE Digital\Historian Remote Management Agents\Collector	HKEY_LOCAL_MACHINE\SOFTWARE \GE Digital\Historian Remote Management Agents\Collector Manager
The Historian server		<*installation drive*>:\Program Files\Proficy \Proficy Historian \x64\Server	HKEY_LOCAL_MACHINE\SOFTWARE \Intellution, Inc.\iHistorian \Services

Historian Installation Limitations

- With a Historian install, you are limited to Historian Administrator. If you want to install other clients, use a client-specific install. If you want to install web-admin clients, use a Web-based Clients specific install.
- 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.
- 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.
- Running Historian Web Admin/Trend Client in a cluster setup is not supported.
- With a Historian install, you are limited to Historian Administrator, If you want to install other clients, use a client-specific install and install any Web-based Clients (Historian Web Admin console and the Historian Trend Client)use Historian Web-based Clients.

Installing Historian in a Cluster Environment

Installing Historian in a Cluster Environment

Historian works with Microsoft Cluster Service Manager to ensure high availability of the Historian server. If the primary Historian node in the cluster experiences difficulties, Historian is automatically started on another node to take over. Server high availability is managed through the Microsoft Cluster Service Manager.

- Configure a failover cluster in the Windows server.
- To use Historian Alarms and Events in a cluster environment, select the appropriate SQL server for both the cluster nodes.

1. In Windows, go to **All Programs** > **Administrative Tools** > **Failover Cluster Manager** on any of the cluster nodes and make it the primary node.
2. Install Historian on that node.
3. Change the Historian Data path to the Cluster Shared Disk.
4. Enter valid SQL Server details.
5. Complete the Historian installation.
6. After installing Historian on Cluster Node1, repeat steps from 1 to 5 for the remaining nodes.

Add User-defined Resource Types to the Cluster Instance

If Failover Clustering is enabled on a machine, the Historian install will register two user-defined resource types in the cluster.

To ensure that the user-defined resource types are added to the cluster instance:

1. Access Failover Cluster Manager.
2. Right-click the cluster instance, select **Properties** > **Resource Types**.
3. If the Historian user-defined resource types are not available, select **Add**.
4. Select `[HistorianInstallDir]/x64/Server/Historian.dll` as the resource DLL with `Historian` and `AlarmArchiver` as both the resource type names and display names.

Add Historian Service to the Cluster

1. Access Failover Cluster Manager, right-click the cluster instance, and then select **More Actions > Create Empty Service or Application.**.
2. Rename the newly created service (for example, Historian).
3. Right-click the service, and then select **Add a resource** > **More resources** > **Add Historian**.
4. Right-click the service, and then select **Add a storage**.
5. Create the IP address and network name that allow access to a clustered Historian instance regardless of the actual node on which the Historian server resides.
   a. Right-click the service, and then select **Add a resource** > **Client Access Point**.
   b. Enter the **IP Address** that will be used for clustered Historian.
6. Add Historian resource dependencies:

   a. Right-click **Properties** on the **New Historian** resource in the Historian service summary list.

b. Select **Dependencies**, and then add all the three resources as dependencies to **New Historian**.
   You can now bring the Historian service online.

Add Alarm Archiver Resource to the Cluster

1. Right-click the new service, and then select **Add a resource > More resources > Add Alarm Archiver**.
2. Right-click **Properties** on the **New Alarm Archiver** resource in the Historian service summary list.
3. Select **Dependencies**, and then add **New Historian** as a dependency.
   You can now bring the Alarm Archiver service online.

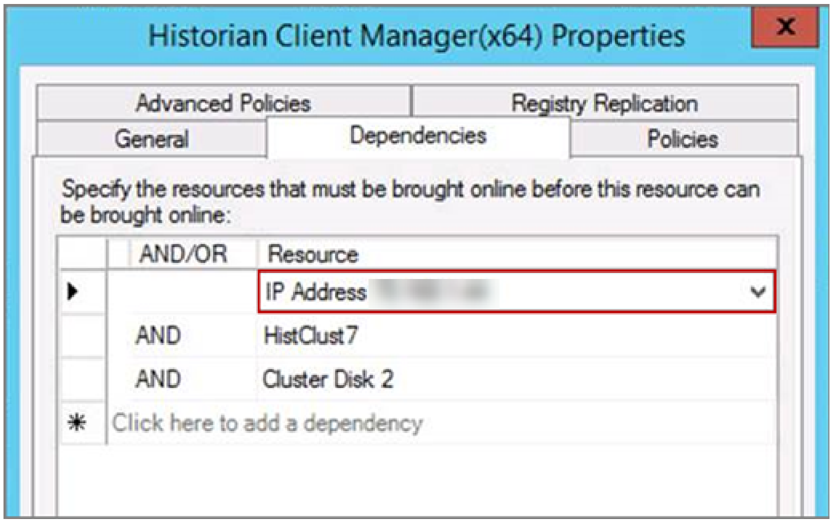
   Note: The Alarm Archiver resource does not require other dependencies like `Cluster Disk` and `IP Address`.

Configure Generic Services

To configure Client Manager, Configuration Manager, Diagnostic Manager, Historian Embedded PostgreSQL Database, Historian Embedded Tomcat Container, and Historian Indexing Service, you must configure them as generic services using Failover Cluster Manager.

Begin with configuring the Client Manager Resource Dependency, and then repeat the steps for the Configuration Manager, Diagnostic Manager, Historian Embedded PostgreSQL Database, Historian Embedded Tomcat Container and Historian Indexing Service.

1. In the Historian service summary list, on the **Client Manager** resource, right-click **Properties**.
2. Select **Dependencies**, and then add the **IP Address** dependency as shown in the following image.



Historian Client Manager(x64) Properties

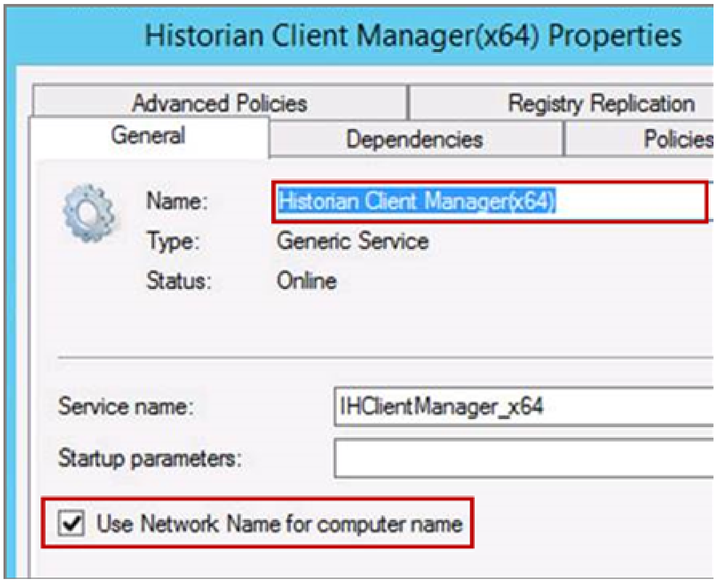
Specify the resources that must be brought online before this resource can be brought online:

	AND/OR	Resource
▶		IP Address [redacted]
	AND	HistClust7
	AND	Cluster Disk 2
✱	Click here to add a dependency	

3. Select **Apply**, and select **OK**.

4. In the Historian service summary list, on the **Client Manager** resource, right-click **Properties**.

5. Select **General**, and then select the **Use Network Name for Computer Name** check box.



Historian Client Manager(x64) Properties

Name: Historian Client Manager(x64)

Type: Generic Service

Status: Online

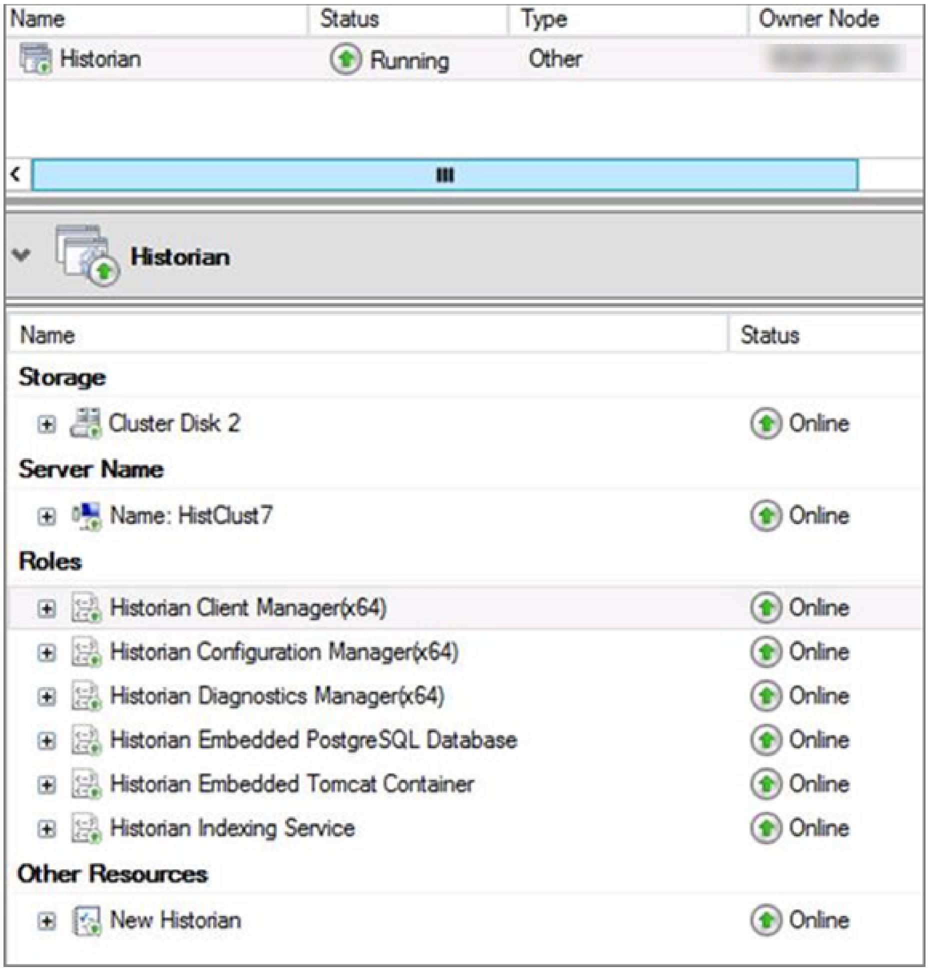
Service name: IHClientManager_x64

Startup parameters:

☑ Use Network Name for computer name

6. Select **OK**.

7. Repeat 1 through 6 for Configuration Manager, Diagnostic Manager, Historian Embedded PostgreSQL Database, Historian Embedded Tomcat Container and Historian Indexing Service. You can now bring the Historian service online.



Name	Status	Type	Owner Node
Historian	Running	Other	[redacted]

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

Installing Historian Components

About Installing Historian Components

After you have installed the Historian server and restarted your system, you can install additional components, such as Client Tools, the Historian Excel add-in, the Web-based Clients, data collectors, and Historian Alarms and Events.

Historian Administrator and the OPC Classic HDA server are installed as part of the Client Tools installation.

Note: On a 64-bit Windows operating system, the default destination folder for all 32-bit components (such as collectors and APIs) is `C:\Program Files\Historian\x86`. Similarly, for all 64-bit components (such as Excel Add-in 64-bit and SQL Server 64-bit), the default destination folder is `C:\Program Files\Historian\x64`.

Install Client Tools

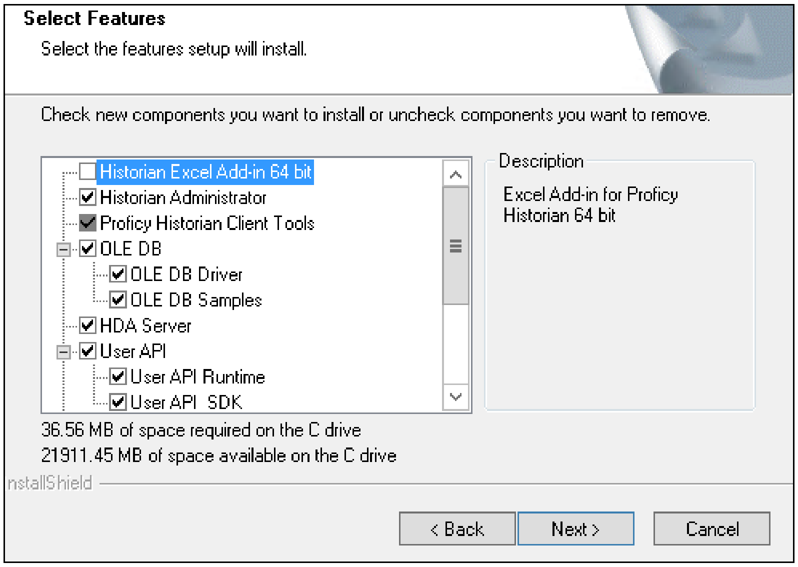
When you install Client Tools, the following components are installed by default:

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

This topic describes how to install Client Tools using the installer. You can also install it at a command prompt *(page 85)*.

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.



Select Features

Select the features setup will install.

Check new components you want to install or uncheck components you want to remove.

□ Historian Excel Add-in 64 bit
☑ Historian Administrator
☑ Proficy Historian Client Tools
☑ OLE DB
  ☑ OLE DB Driver
  ☑ OLE DB Samples
☑ HDA Server
☑ User API
  ☑ User API Runtime
  ☑ User API SDK

Description

Excel Add-in for Proficy Historian 64 bit

36.56 MB of space required on the C drive
21911.45 MB of space available on the C drive

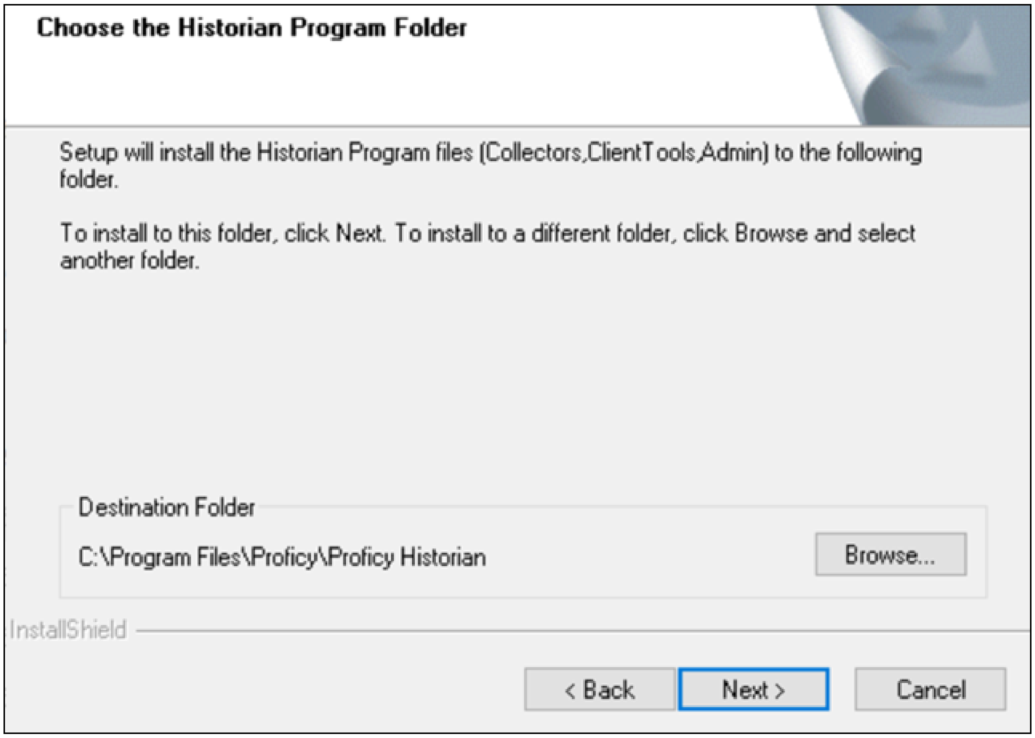
By default, the check boxes for components such as **Historian Administrator**, **HDA Server**, **OLE DB**, and **User API and SDK** are selected. If you do not want to install them at this time, clear the check boxes. You cannot, however, clear the **Proficy Historian Client Tools** check box.

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.



Choose the Historian Program Folder

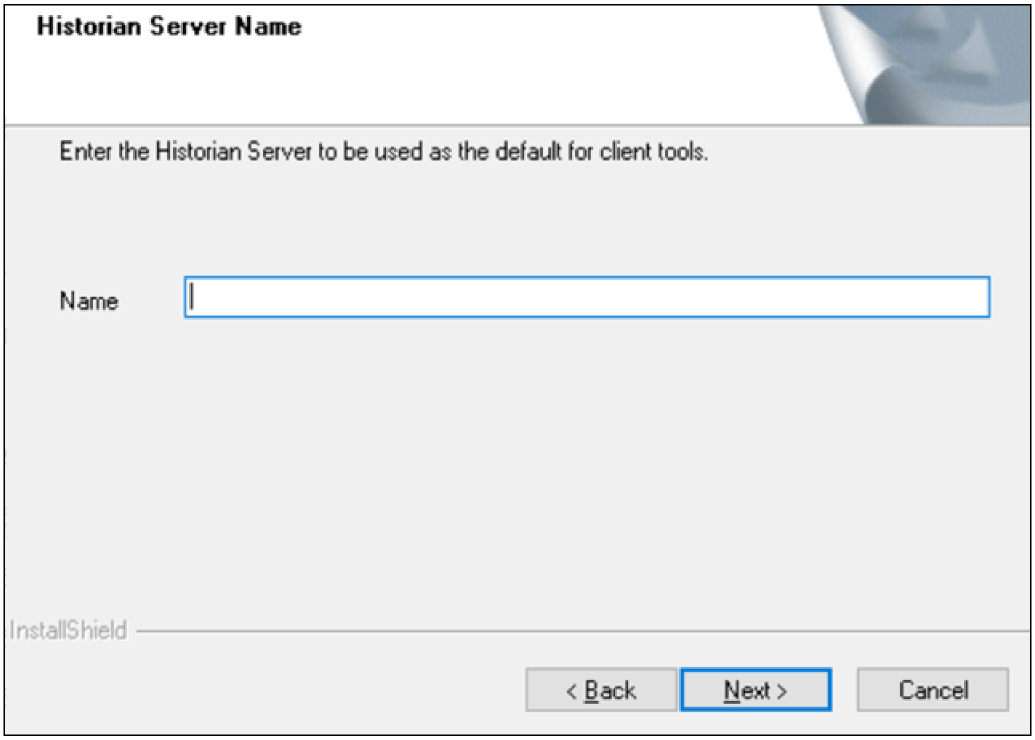
Setup will install the Historian Program files (Collectors,ClientTools,Admin) to the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Proficy\Proficy Historian

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

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. 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 *(page 83)* 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 *(page 121)*.

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 User Account and Authentication (UAA) service (optional): Provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including Oauth2. You can install UAA and Configuration Hub, or you can point to an existing UAA and Configuration Hub.

- Rest APIs: Allow you to query data from a Historian server.

You can install Web-based Clients using a GUI-based installer *(page 87)* or at a command prompt *(page 98)*.

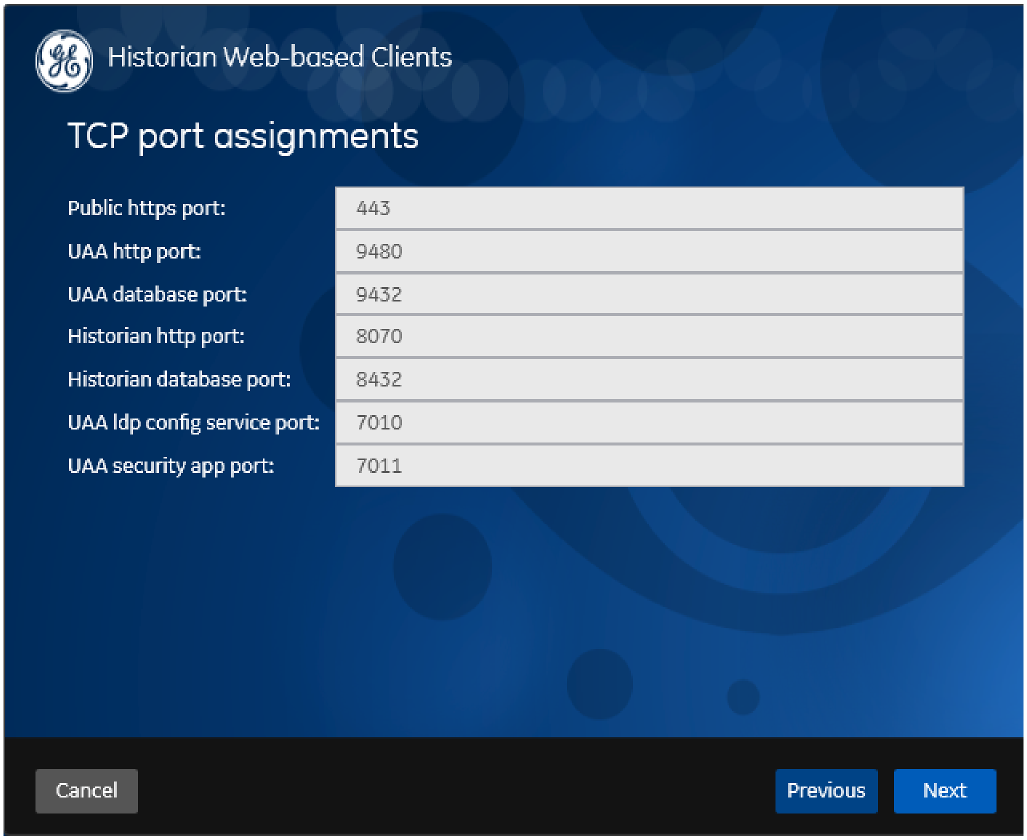
❗ **Important:** When you install Web-based Clients:

- 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.

Install Web-Based Clients Using the Installer

This topic describes how to install Web-based Clients using a GUI-based installer. You can also install Web-based Clients using the command line *(page 98)*.

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.



Historian Web-based Clients

TCP port assignments

Public https port: 443

UAA http port: 9480

UAA database port: 9432

Historian http port: 8070

Historian database port: 8432

UAA ldp config service port: 7010

UAA security app port: 7011

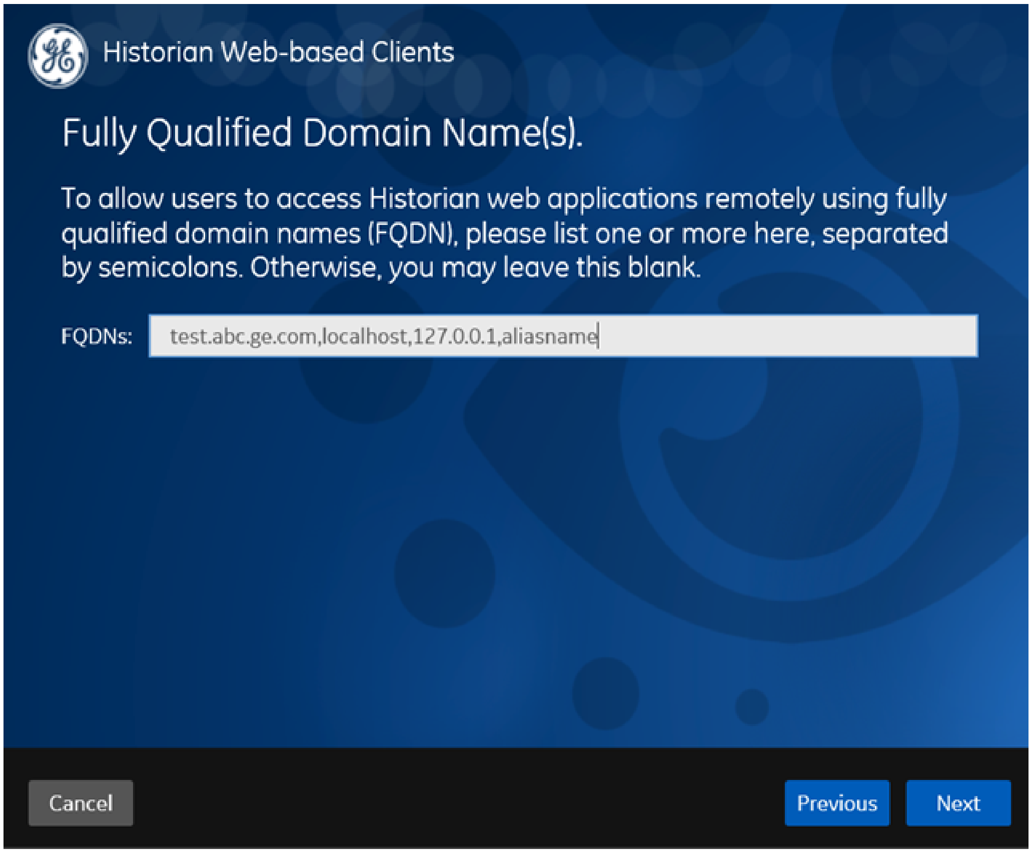
5. As needed, change the values for TCP port assignments as described in the following table, and then select **Next**.

Field	Description
Public https port	Port for https protocol communication used by Web-based Clients. The default value is 443. Ensure that this port number matches the one you specify while installing the Historian server. In addition: • 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.
UAA http port	Port for http protocol communication used by the UAA service. The default value is 9480.
UAA database port	Port for the UAA 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.

Field	Description
UAA Idp config service port	Port for the Configuration Hub identity provider service. The default value is 7010.
UAA security app port	Port for the UAA 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: test.abc.ge.com,localhost,127.0.0.1,aliasname

6. In the **FDQNs** box, 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:// 127.0.0.1 /historian-visualization/hwa
   - https:// aliasName /historian-visualization/hwa
   - https:// localhost /historian-visualization/hwa

Important:

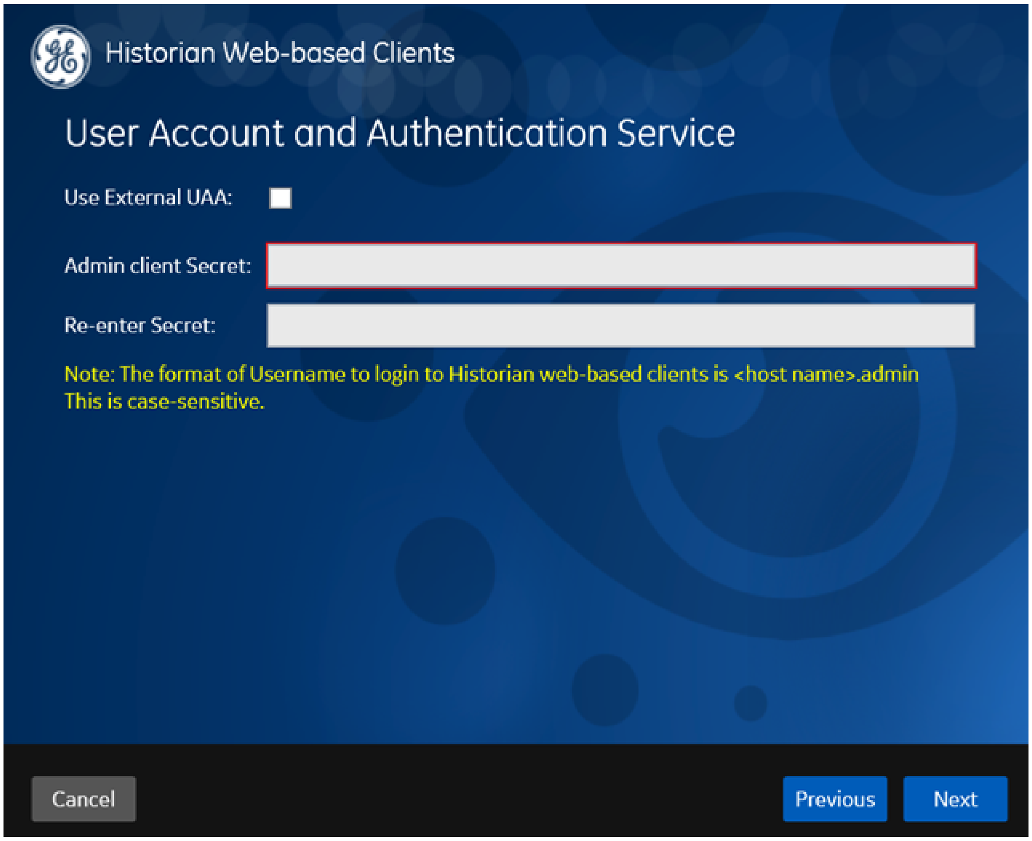
- Do not enter a space between the values.
- You must add the IP address and alias name in the `hosts` file located at `C:\Windows\System32\drivers\etc`. The IP address that you add must be a static or fixed IP address.

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

  Example: `1.2.3.4 myservername`
- FQDN is not supported for Configuration Hub.

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

- If you want to install UAA, clear the **Use External UAA** check box.
- If you want to use an existing UAA, select the **Use External UAA** check box.



User Account and Authentication Service

Use External UAA: □

Admin client Secret:

Re-enter Secret:

Note: The format of Username to login to Historian web-based clients is <host name>.admin This is case-sensitive.

7. If you want to install UAA, enter the **Admin client secret**, re-enter the secret, and then select **Next**.

   The admin client secret must satisfy the following conditions:

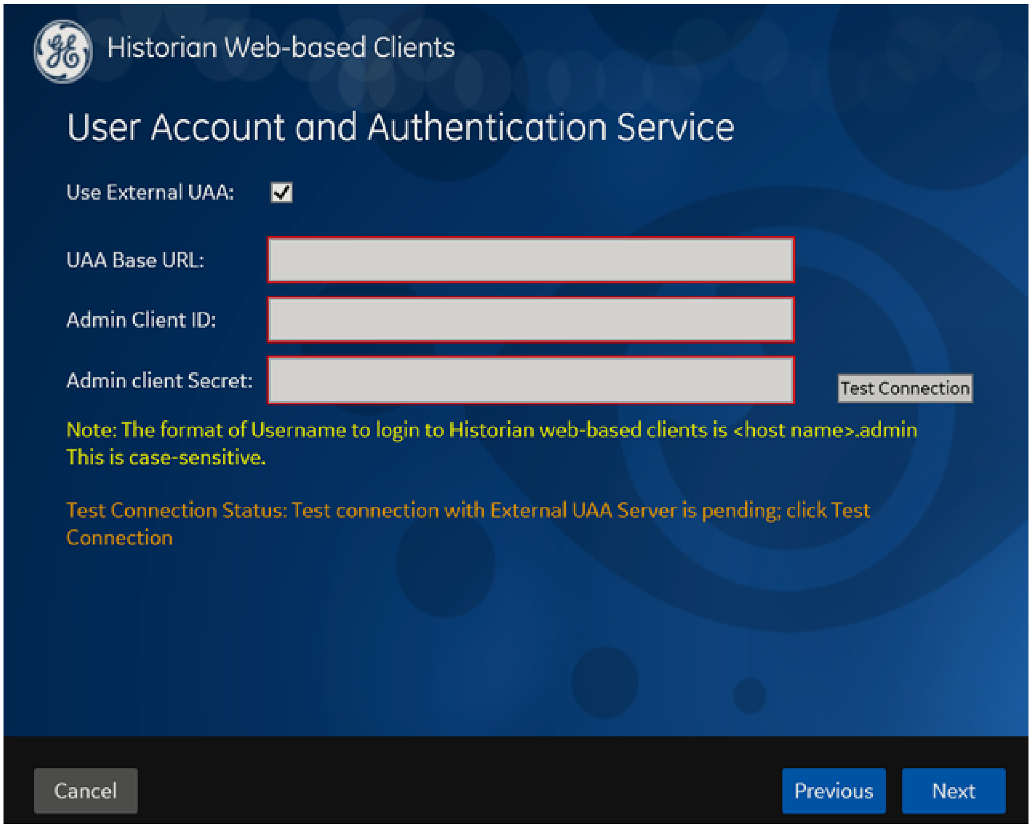
   - Must not contain only numbers.
   - Must not begin or end with a special character.
   - Must not contain curly braces.

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 UAA 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 UAA user, and then create the corresponding Windows user *(page 179)*, using the uaa_config_tool utility.

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

   a. Select the **Use External UAA** check box.
   The fields for the external UAA service appear.


Historian Web-based Clients
User Account and Authentication Service

Use External UAA: ☑

UAA Base URL:

Admin Client ID:

Admin client Secret:

Note: The format of Username to login to Historian web-based clients is <host name>.admin
This is case-sensitive.

Test Connection Status: Test connection with External UAA Server is pending; click Test Connection

   b. Enter values as described in the following table.

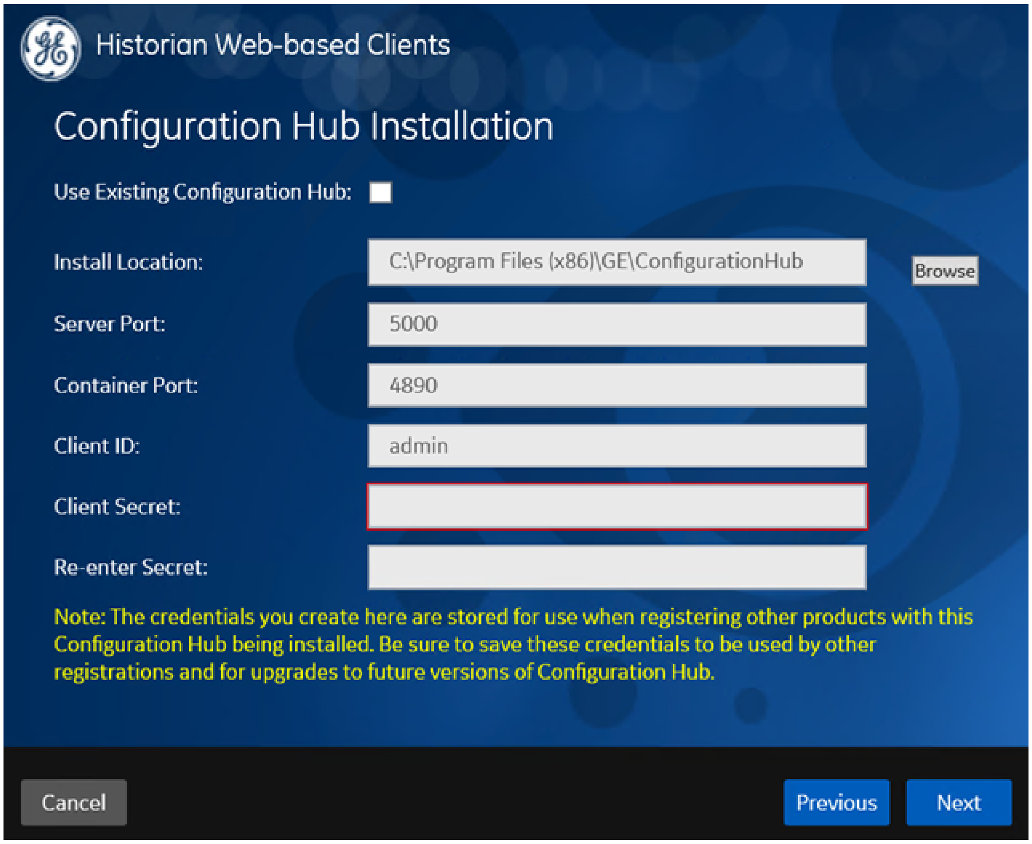
Field	Description
UAA Base URL	Enter the URL of the external UAA server in the following format: https://<*UAA server name*>:<*port number*>, where <*UAA server name*> is the FQDN or hostname of the machine on which UAA is installed. By default, the port number is 443. **Note:** Do not enter a trailing slash character.
Admin Client ID	Enter the client name that you provided while installing the external UAA. The default value is admin.
Admin client secret	Enter the client secret that you provided while installing the external UAA.

c. Select **Test Connection**.
The results of the connection test appear. You cannot proceed until the connection is successful.

d. 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, which is installed with iFIX.

Configuration Hub allows you to add and manage a collector instance remotely. For more information, refer to About Configuration Hub.



Historian Web-based Clients

Configuration Hub Installation

Use Existing Configuration Hub: □

Install Location:	C:\Program Files (x86)\GE\ConfigurationHub
Server Port:	5000
Container Port:	4890
Client ID:	admin
Client Secret:	
Re-enter Secret:	

Note: The credentials you create here are stored for use when registering other products with this Configuration Hub being installed. Be sure to save these credentials to be used by other registrations and for upgrades to future versions of 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. If that happens, skip to step 10.

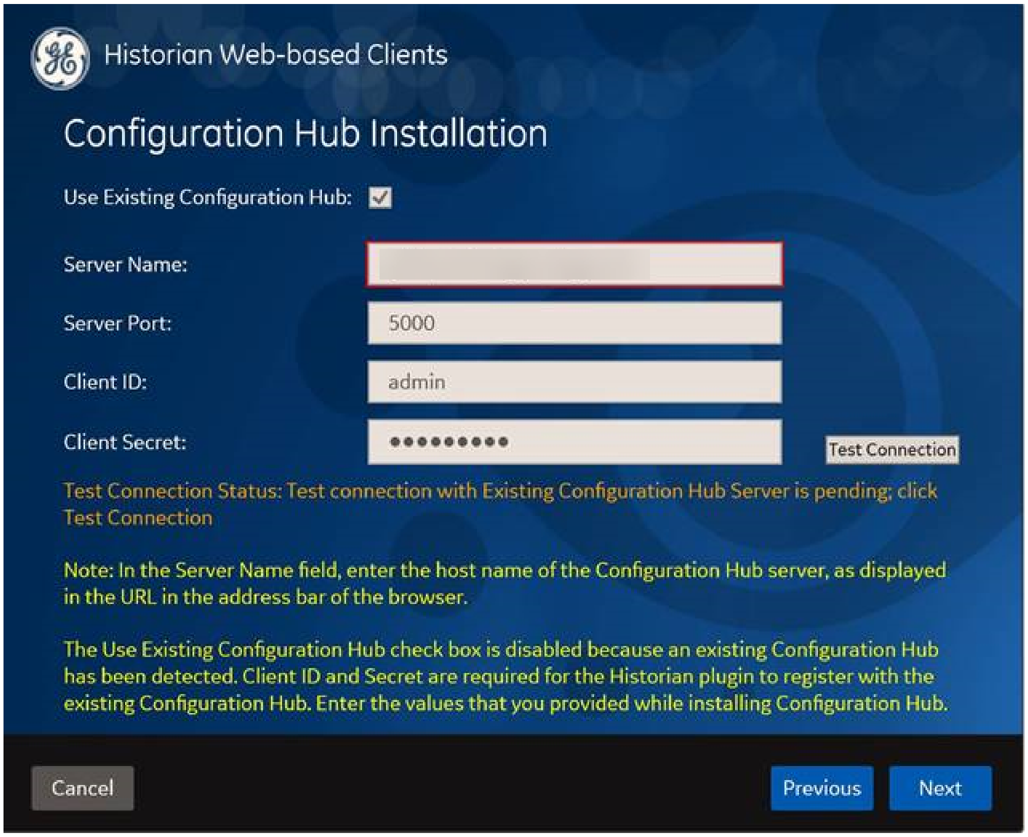
9. If you want to install Configuration Hub, ensure that the **Use Existing Configuration Hub** check box is cleared, and then provide values as described in the following table.

Field	Description
Install Location	If needed, modify the installation folder for Configuration Hub. ❗ **Important:** You can install Configuration Hub only in the C drive. If, however, you want to install it in a different drive: a. Create Configuration Hub server certificates. b. Start the ConfigHubNGINXService service. c. Using the Web Based Clients Configuration tool *(page 103)*, provide the UAA and Configuration Hub details, test the connection, and select **Resgister** to re-register the Historian plugin with Configuration Hub.
Server Port	If needed, modify the port number that you want to use for the web server (NGINX). The default value is 5000.
Container Port	If needed, modify the port number for the Configuration Hub container. The default value is 4890.

Field	Description
Client ID	Enter the username to connect to Configuration Hub. The default value is admin. The value that you enter can contain: • All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVXYZ abcdefghijklmnopqrstuvwxyz_0123456789) • The following special characters: ><:~!@#$%^&*?|
Client Secret	Enter the password to connect to Configuration Hub. The value that you enter can contain: • Must contain at least eight characters. • All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVXYZ abcdefghijklmnopqrstuvwxyz_0123456789) • The following special characters: ><:~!@#$%^&*?|
Re-enter Secret	Re-enter the password to connect to Configuration Hub.

10. 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.



Historian Web-based Clients

Configuration Hub Installation

Use Existing Configuration Hub: ☑

Server Name:

Server Port: 5000

Client ID: admin

Client Secret: ●●●●●●●●●

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

Note: In the Server Name field, enter the host name of the Configuration Hub server, as displayed in the URL in the address bar of the browser.

The Use Existing Configuration Hub check box is disabled because an existing Configuration Hub has been detected. Client ID and Secret are required for the Historian plugin to register with the existing Configuration Hub. Enter the values that you provided while installing Configuration Hub.

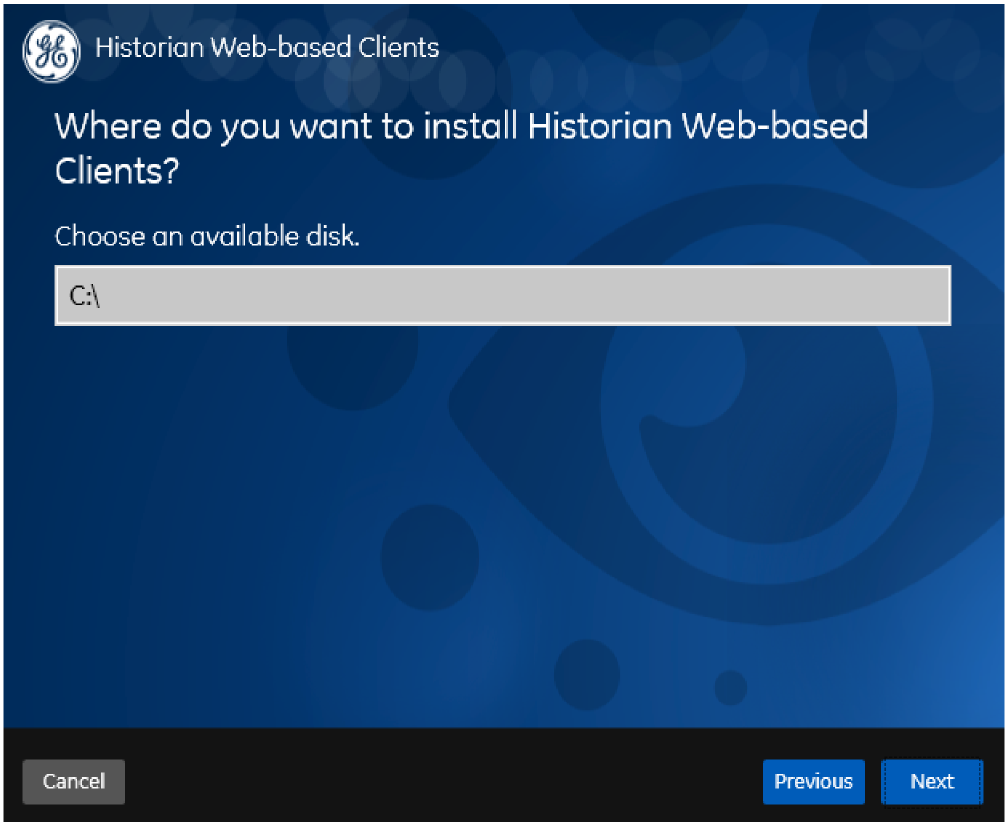
   b. Provide values as described in the following table.

Field	Description
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.

d. Select **Next**.

The default installation drive appears.



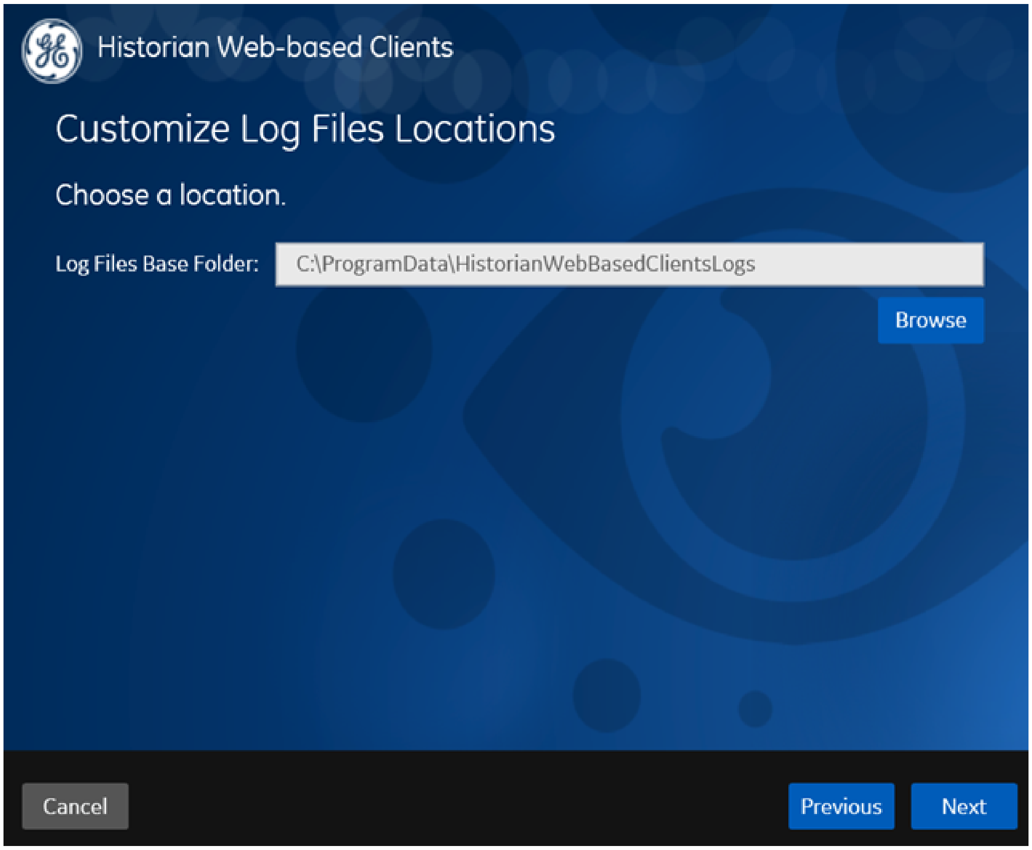
Historian Web-based Clients

Where do you want to install Historian Web-based Clients?

Choose an available disk.

C:\

11. If needed, change the installation drive for Web-based Clients, and then select **Next**.
The **Customize Log Files Locations** page appears.

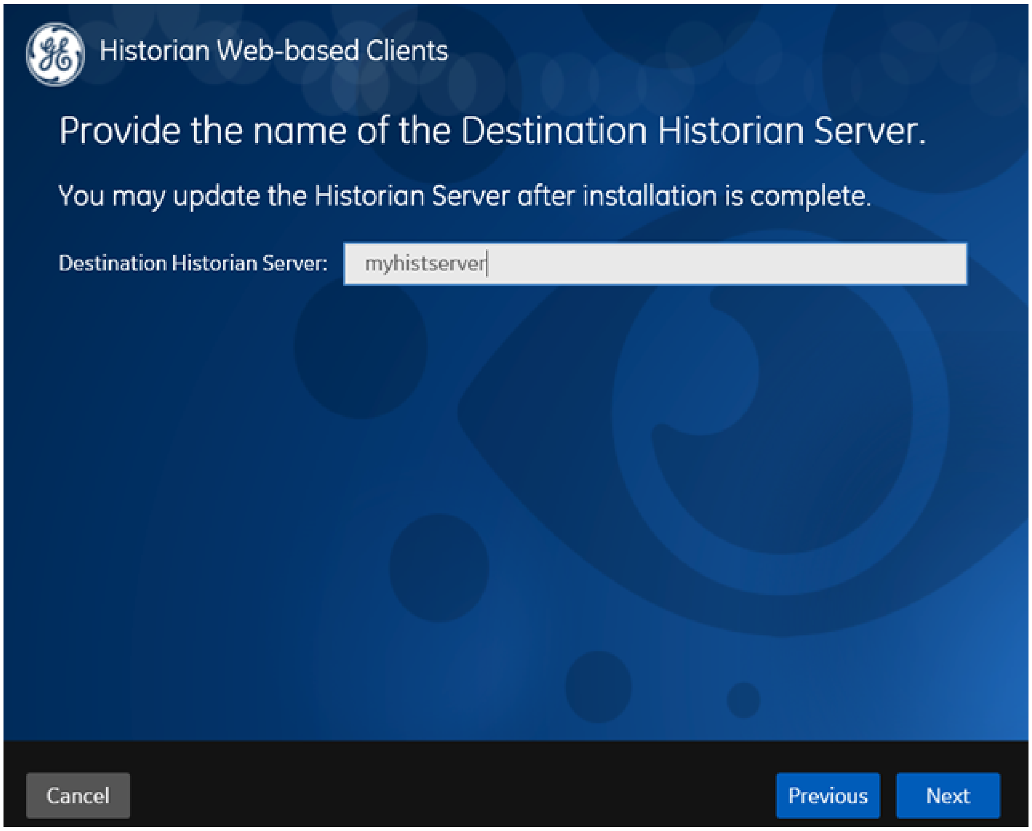


Customize Log Files Locations

Choose a location.

Log Files Base Folder: C:\ProgramData\HistorianWebBasedClientsLogs

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



Historian Web-based Clients

Provide the name of the Destination Historian Server.

You may update the Historian Server after installation is complete.

Destination Historian Server: myhistserver

13. 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.

14. Select **Next**.

    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.

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

15. Select **Install**. Restart your system if prompted to do so.
    The Web-based Clients installation begins.

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

Historian Web-based Clients are installed.

Install Web-Based Clients at a Command Prompt

This topic describes how to install Web-based Clients at a command prompt. You can also install Web-based Clients using an installer *(page 86)*.

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

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

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

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

   The following table describes the installation parameters.

Parameter	Description	Default Value
PublicPort	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: • 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 UAA service.	9480
UAADatabasePort	Port for the UAA database.	9432
HistorianHttpPort	Port for the http protocol communication used by Web-based Clients.	8070
HistorianDatabasePort	Port for the PostgreSQL Historian database.	8432
UAAIdpConfigPort	Port for the Configuration Hub identity provider service.	7010
UAASecurityAppPort	Port for the UAA Configuration tool.	7011

Parameter	Description	Default Value
EmbeddedWebServerAlternativeNames	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. For example, 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:// 127.0.0.1 /historian-visualization/hwa • https:// aliasName /historian-visualization/hwa • https:// localhost /historian-visualization/hwa **Important:** • Do not enter a space between the values. • If you have already installed Operations Hub on the same machine, enter the same value that you have provided while installing Operations Hub. • 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. • 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.	
AdminClientId	The client ID to connect to the UAA service.	

Parameter	Description	Default Value
AdminClientSecret	The password to connect to the UAA service. The password must satisfy the following conditions: • Must not contain only numbers. • Must not begin or end with a special character. • Must not contain curly braces. If the password does not satisfy these conditions, the installation may be successful, but Web-based Clients will not work. **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 UAA 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 UAA user, and then create the corresponding Windows user, using the uaa_config_tool utility.	Not applicable
UseExternalUaa	Identifies whether you want to use an external UAA service (that is, a UAA instance already installed by an external application such as Operations Hub). If you want to use an external UAA, enter 1.	0
ActiveUaaBaseUrl	The base URL to connect to an external UAA. A value is required only if you want to connect to an external UAA service. Enter a value in the following format: https://<*UAA server machine name*>:<*public https port number*>. By default, the port number is 443.	
ConfigHubPort	The web server (NGINX) port that you want to use for Configuration Hub.	5000
ConfigHubContainerPort	The port for the Configuration Hub container.	4890

Parameter	Description	Default Value
ConfigHubInstallFolder	The installation folder for Configuration Hub. **Important:** You can install Configuration Hub only in the C drive. If, however, you want to install it in a different drive: a. Create Configuration Hub server certificates. b. Start the ConfigHubNGINXService service. c. Using the Web Based Clients Configuration tool *(page 103)*, provide the UAA and Configuration Hub details, test the connection, and select **Resgister** to re-register the Historian plugin with Configuration Hub.	`C:\Program Files (x86)\GE\ConfigurationHub`
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
ExternalConfigHubMachineName	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.	
ConfigHubClientId	The username to connect to Configuration Hub. The value that you enter can contain: • All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVXYZ abcdefghijklmnopqrstuvwxyz_0123456789) • The following special characters: ><:~!@#$%^&*?|	admin
ConfigHubClientSecret	The password to connect to Configuration Hub. The value that you enter can contain: • Must contain at least eight characters. • All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVXYZ abcdefghijklmnopqrstuvwxyz_0123456789) • The following special characters: ><:~!@#$%^&*?|	

Parameter	Description	Default Value
DataPath	The path to the log files.	`C:\ProgramData\HistorianWebBasedClientsLogs`
DestinationHistorian	The name of the destination Historian server. **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.	

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

```
Install.exe /quiet PublicPort=443 UAAHttpPort=9480 UAADatabasePort=9432
 HistorianHttpPort=8070
HistorianDatabasePort=8432 UAAIdpConfigPort=7010
 UAASecurityAppPort=7011 AdminClientId=admin AdminClientSecret=abc
ConfigHubPort=5000 ConfigHubContainerPort=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 UAAIdpConfigPort=7010
 UAASecurityAppPort=7011 AdminClientId=admin AdminClientSecret=abc
UseExternalConfigHub=1 ExternalConfigHubMachineName=abc123
 ConfigHubClientId=admin
ConfigHubClientSecret=xyz DataPath="C:\ProgramData
\HistorianWebBasedClientsLogs"
```

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

```
Install.exe /quiet PublicPort=443 UAAHttpPort=9480 UAADatabasePort=9432
 HistorianHttpPort=8070
HistorianDatabasePort=8432 UAAIdpConfigPort=7010
 UAASecurityAppPort=7011 AdminClientId=admin
AdminClientSecret=abc UseExternalUaa=1
 ActiveUaaBaseUrl=https://<extrenal UAA machine hostname>:443
ConfigHubPort=5000 ConfigHubContainerPort=4890
 ConfigHubInstallFolder="C:\Program Files (x86)\GE\ConfigurationHub"
ConfigHubClientId=admin ConfigHubClientSecret=xyz
```

```
DataPath="C:\ProgramData\HistorianWebBasedClientsLogs"
```

Connect to the Remote UAA Service

Provide the details of the external UAA while installing Web-based Clients *(page 86)*.

To host a UAA 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 UAA 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.

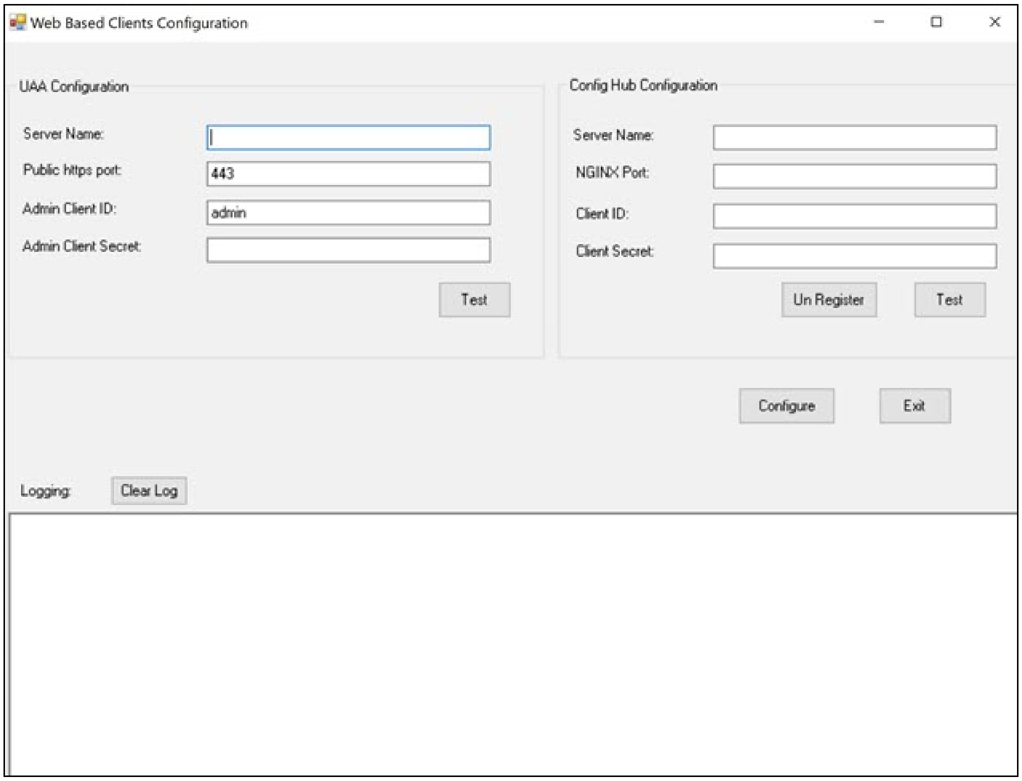
Map the user groups of the remote UAA service with the Historian UAA group *(page 130)*

Configure Web-based Clients

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

- Reconfigure UAA to point to a different UAA server.
- Reconfigure the same UAA 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.



Public https port: 443

Admin Client ID: admin

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`

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

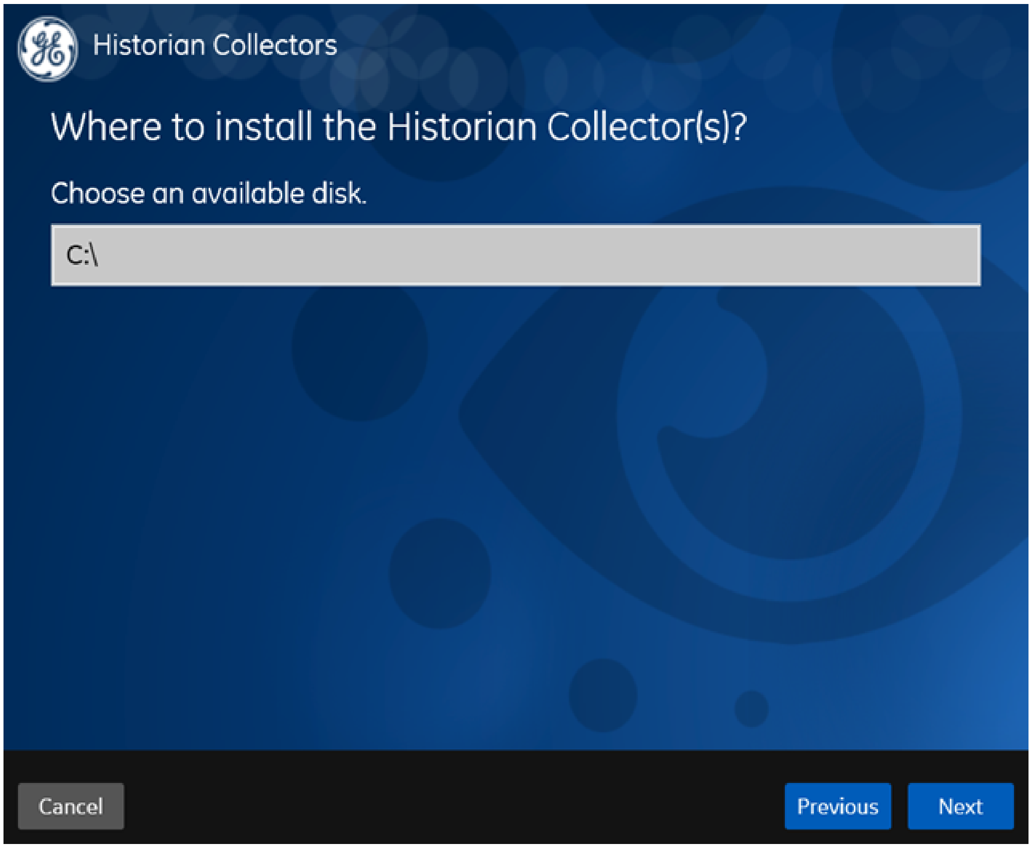
After you install collectors, the following artefacts will be available:

- **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.

Using Configuration Hub, you will then add a collector instance and begin using the collector.
This topic describes how to install collectors using a GUI-based installer. You can also install them at a command prompt *(page 109)*.

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.

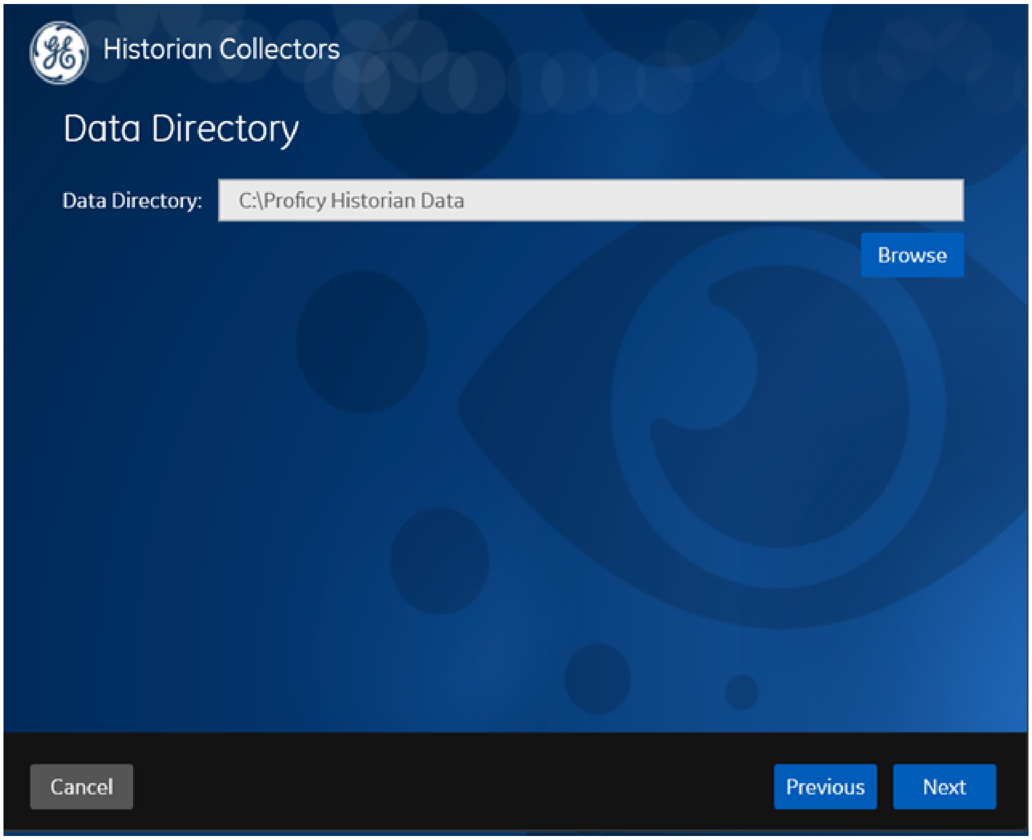


Where to install the Historian Collector(s)?

Choose an available disk.

C:\

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

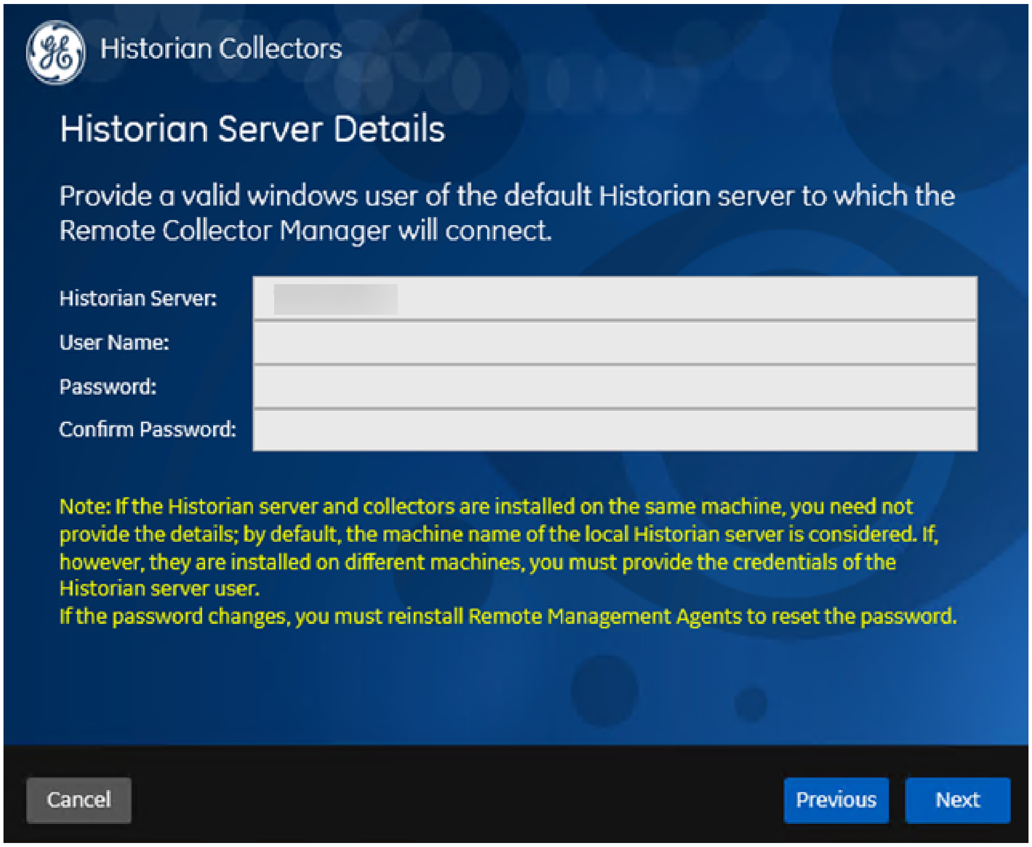


Historian Collectors

Data Directory

Data Directory: C:\Proficy Historian Data

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: [redacted]

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 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 *(page 42)*.
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.

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 *(page 105)*.

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:\`
DataPath	The folder for storing the collector log files.	`C:\Proficy Historian Data`

Parameter	Description	Default Value
DestinationServerName	The host name of the destination Historian server to which you want collectors to send data. 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.	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 server and collectors are on different machines.	

For example: `Collectors_Install.exe -s RootDrive=C:\ DestinationServerName=myservername DataPath=C:\Proficy Historian Data UserName1=user123 Password=xyz123`

3. 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 *(page 42)*.
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.

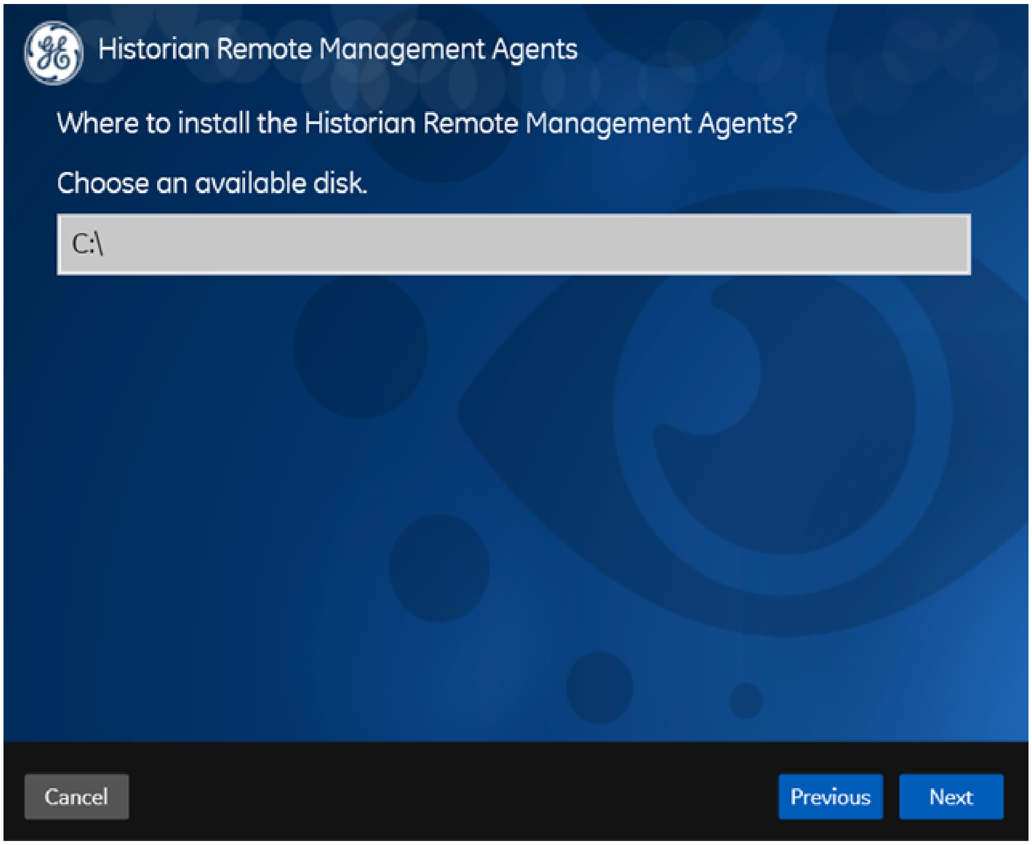
Install Remote Management Agent Using the Installer

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 *(page 114)*.

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.



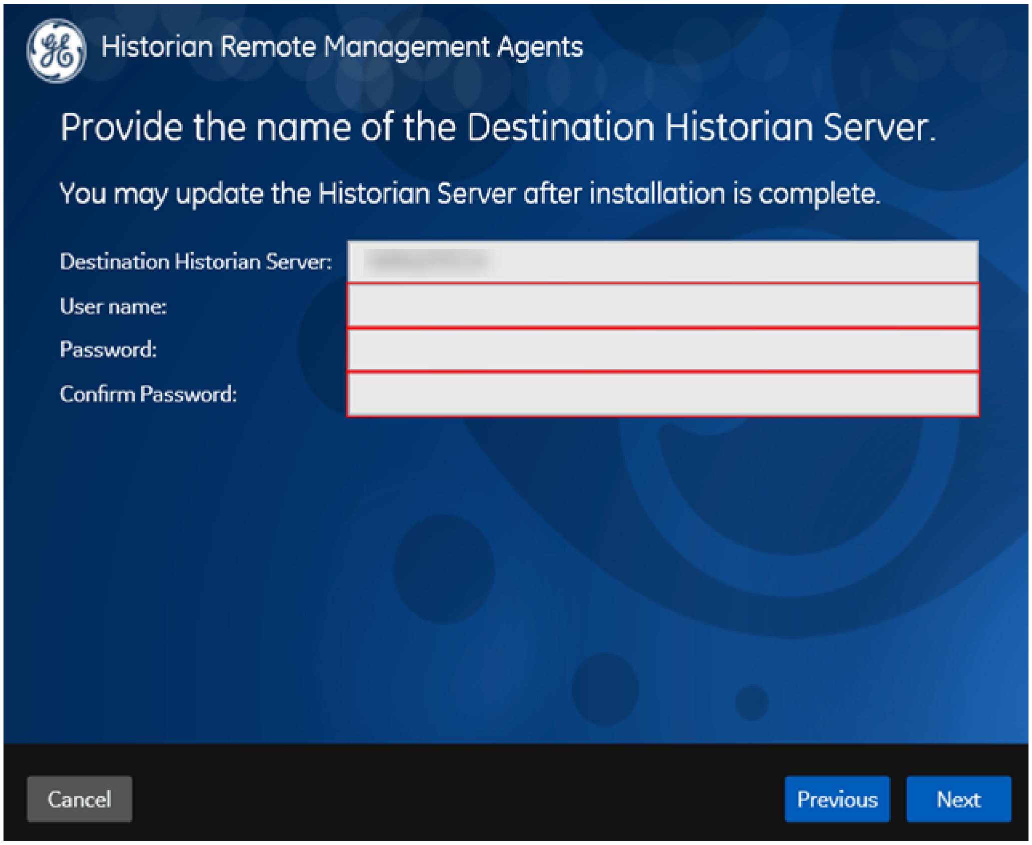
Historian Remote Management Agents

Where to install the Historian Remote Management Agents?

Choose an available disk.

C:\

5. If needed, modify the installation drive, and then select **Next**.
   The destination Historian server page appears.



Historian Remote Management Agents

Provide the name of the Destination Historian Server.

You may update the Historian Server after installation is complete.

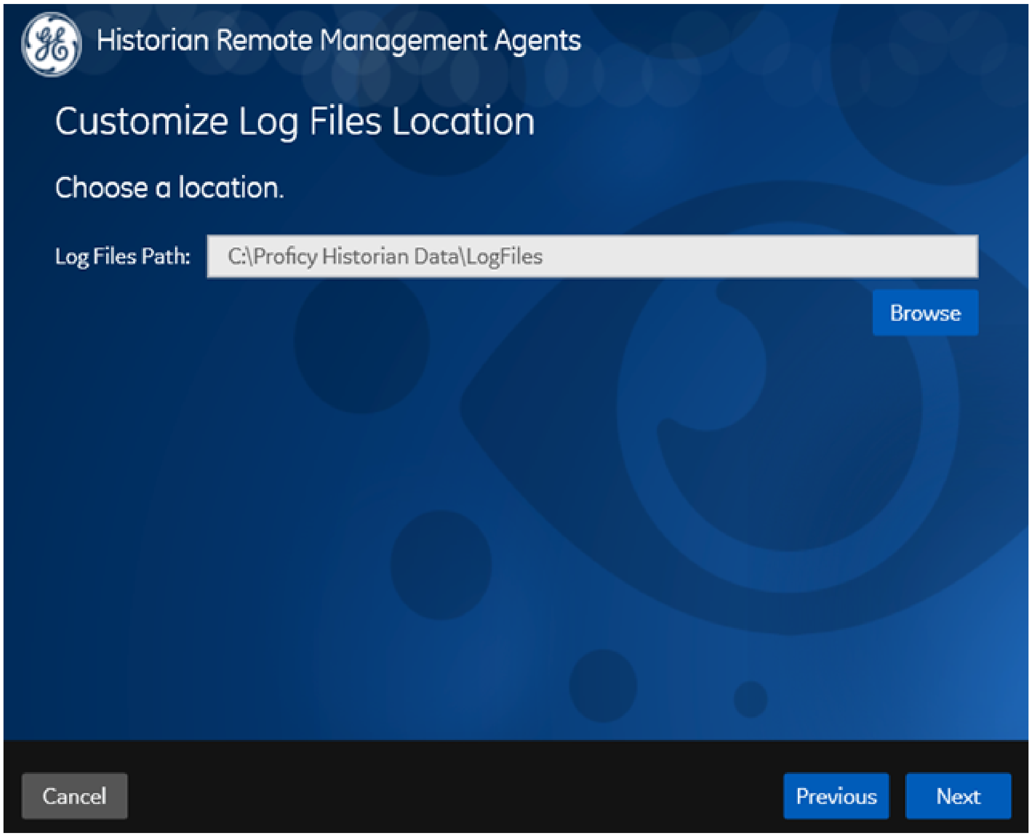
Destination Historian Server: [redacted]

User name:

Password:

Confirm Password:

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.



Historian Remote Management Agents

Customize Log Files Location

Choose a location.

Log Files Path: C:\Proficy Historian Data\LogFiles

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 *(page 192)*.

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 *(page 111)*.

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>
 UserName=<Windows username> Password=<Windows password> DataPath="C:
\Proficy Historian Data\LogFiles"
```

```
HistorianRMA_Install.exe -s RootDrive=C:\ UserName=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 *(page 192)*.

Install the OPC UA HDA Server

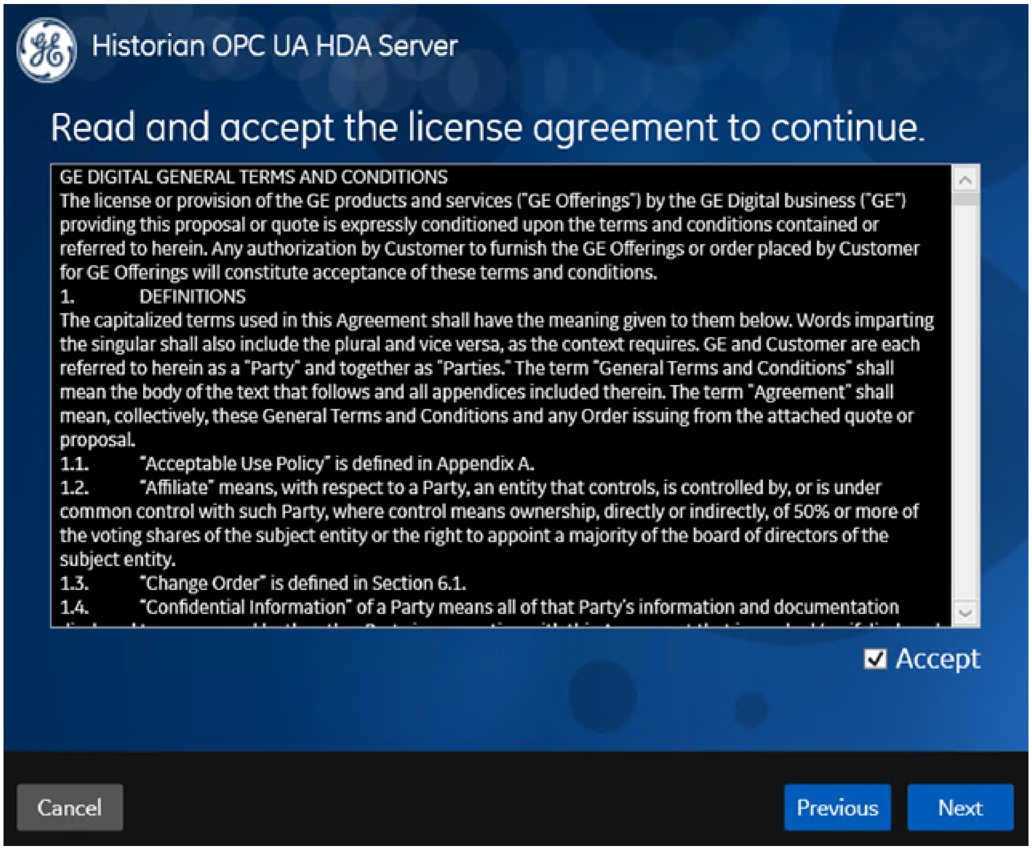
Install Historian *(page 46)*.

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.



Read and accept the license agreement to continue.

GE DIGITAL GENERAL TERMS AND CONDITIONS

The license or provision of the GE products and services ("GE Offerings") by the GE Digital business ("GE") providing this proposal or quote is expressly conditioned upon the terms and conditions contained or referred to herein. Any authorization by Customer to furnish the GE Offerings or order placed by Customer for GE Offerings will constitute acceptance of these terms and conditions.

1. DEFINITIONS

The capitalized terms used in this Agreement shall have the meaning given to them below. Words imparting the singular shall also include the plural and vice versa, as the context requires. GE and Customer are each referred to herein as a "Party" and together as "Parties." The term "General Terms and Conditions" shall mean the body of the text that follows and all appendices included therein. The term "Agreement" shall mean, collectively, these General Terms and Conditions and any Order issuing from the attached quote or proposal.

1.1. "Acceptable Use Policy" is defined in Appendix A.

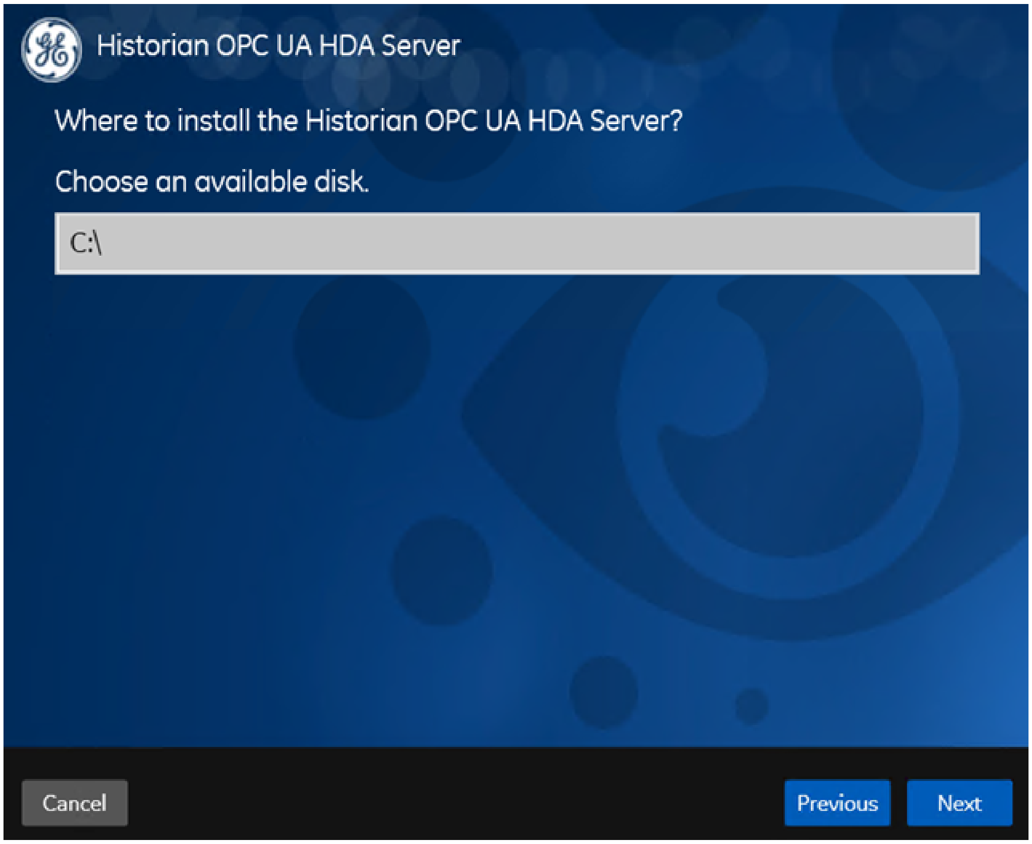
1.2. "Affiliate" means, with respect to a Party, an entity that controls, is controlled by, or is under common control with such Party, where control means ownership, directly or indirectly, of 50% or more of the voting shares of the subject entity or the right to appoint a majority of the board of directors of the subject entity.

1.3. "Change Order" is defined in Section 6.1.

1.4. "Confidential Information" of a Party means all of that Party's information and documentation

☑ Accept

4. Select the **Accept** check box, and then select **Next**.
   The following page appears, asking you to select the installation drive.



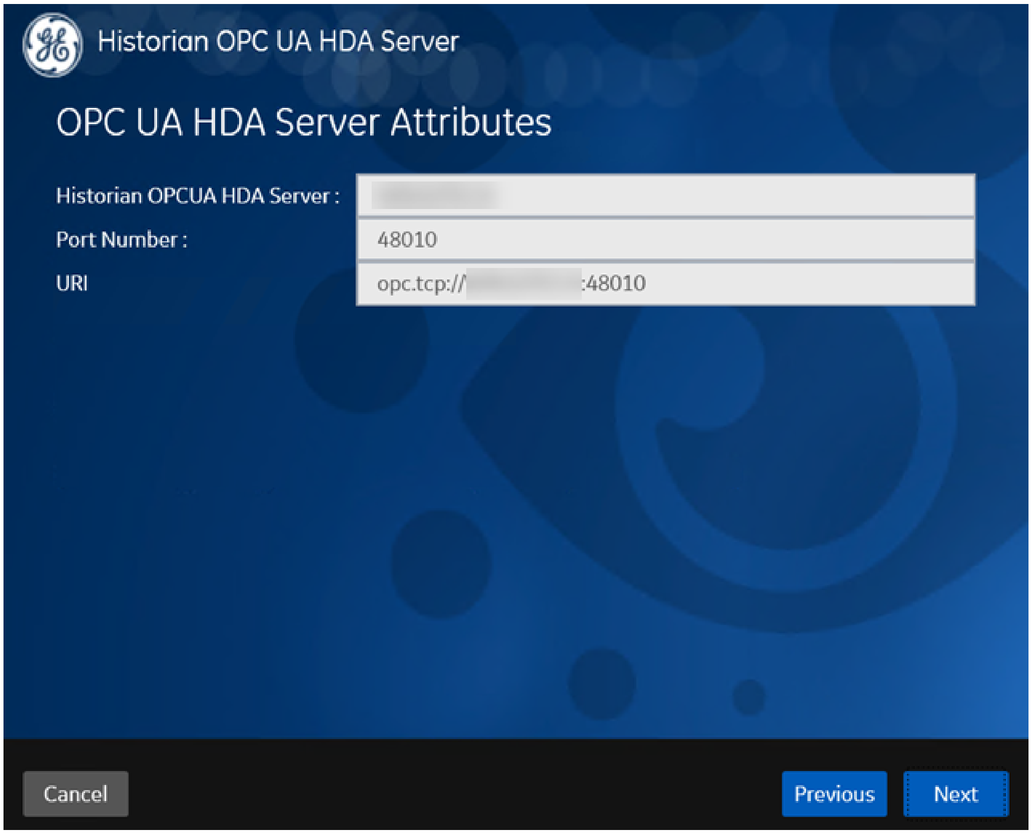
Historian OPC UA HDA Server

Where to install the Historian OPC UA HDA Server?

Choose an available disk.

C:\

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.



Historian OPC UA HDA Server

OPC UA HDA Server Attributes

Historian OPCUA HDA Server : [redacted]

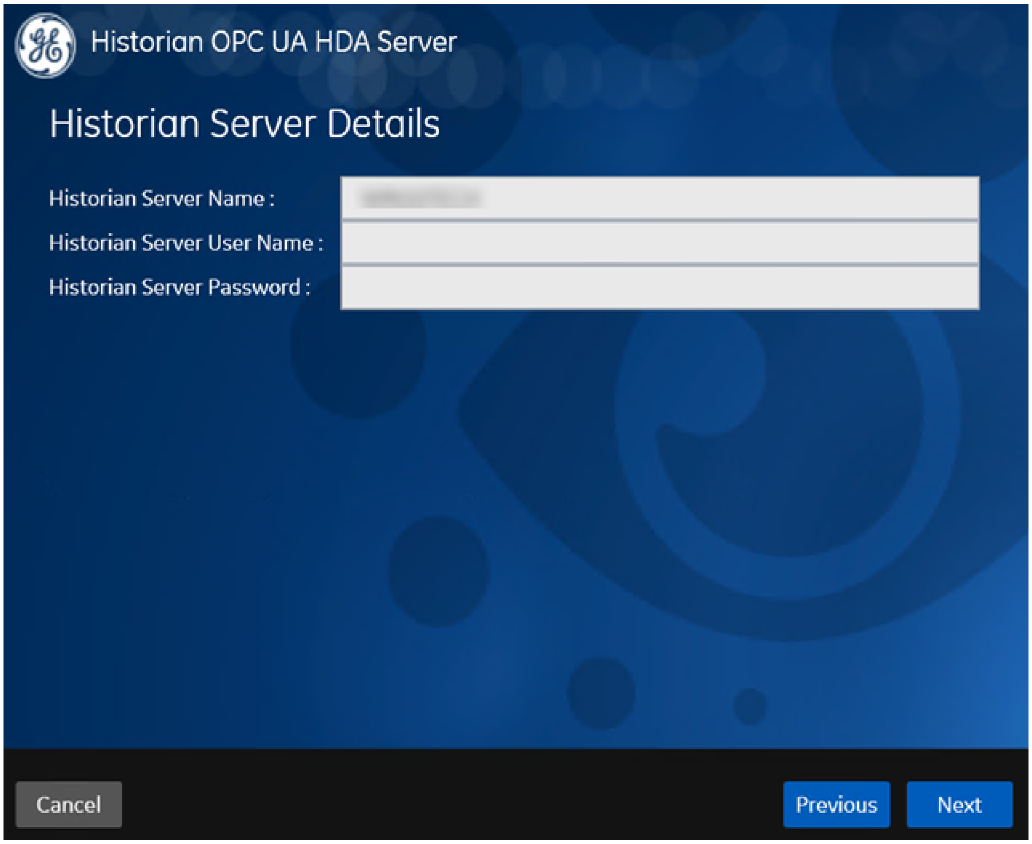
Port Number : 48010

URI opc.tcp://[redacted]:48010

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: opc.tcp://<*host name*>:<*port number*>, where <*host name*> and <*port number*> are the values that you have entered in the preceding fields.

The **Historian Server Details** page appears.


Historian OPC UA HDA Server
Historian Server Details
Historian Server Name :
Historian Server User Name :
Historian Server Password :
Cancel
Previous
Next

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.

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 *(page 120)*. 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 *(page 121)*.

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 *(page 119)* 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**.

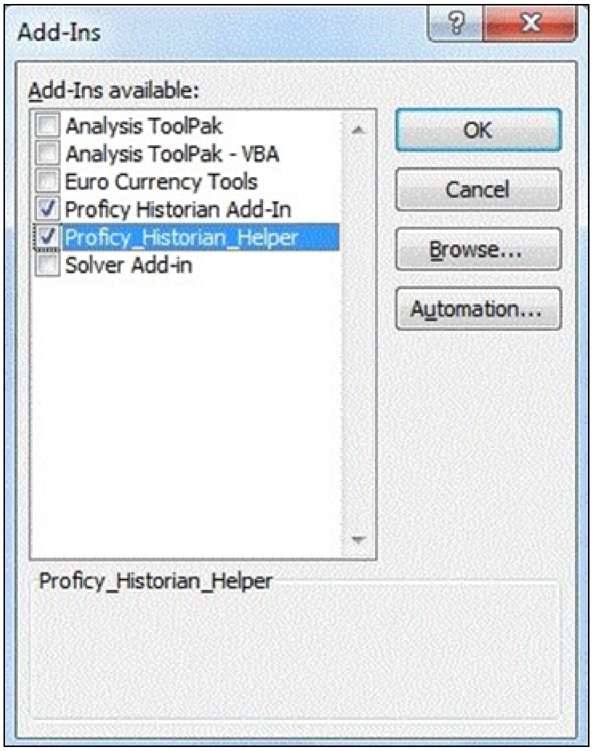
Excel Add-In is installed.

Activate Excel Add-In *(page 121)*.

Activate Excel Add-In

Install Excel Add-In *(page 119)*.

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.

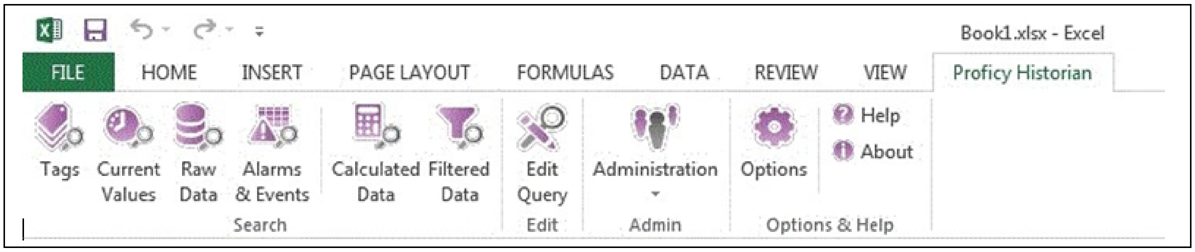


Add-Ins available:

- ☐ Analysis ToolPak
- ☐ Analysis ToolPak - VBA
- ☐ Euro Currency Tools
- ☑ Proficy Historian Add-In
- ☑ Proficy_Historian_Helper
- ☐ Solver Add-in

Proficy_Historian_Helper

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.



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 *(page 123)*.

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 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.

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 *(page 123)*.

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:

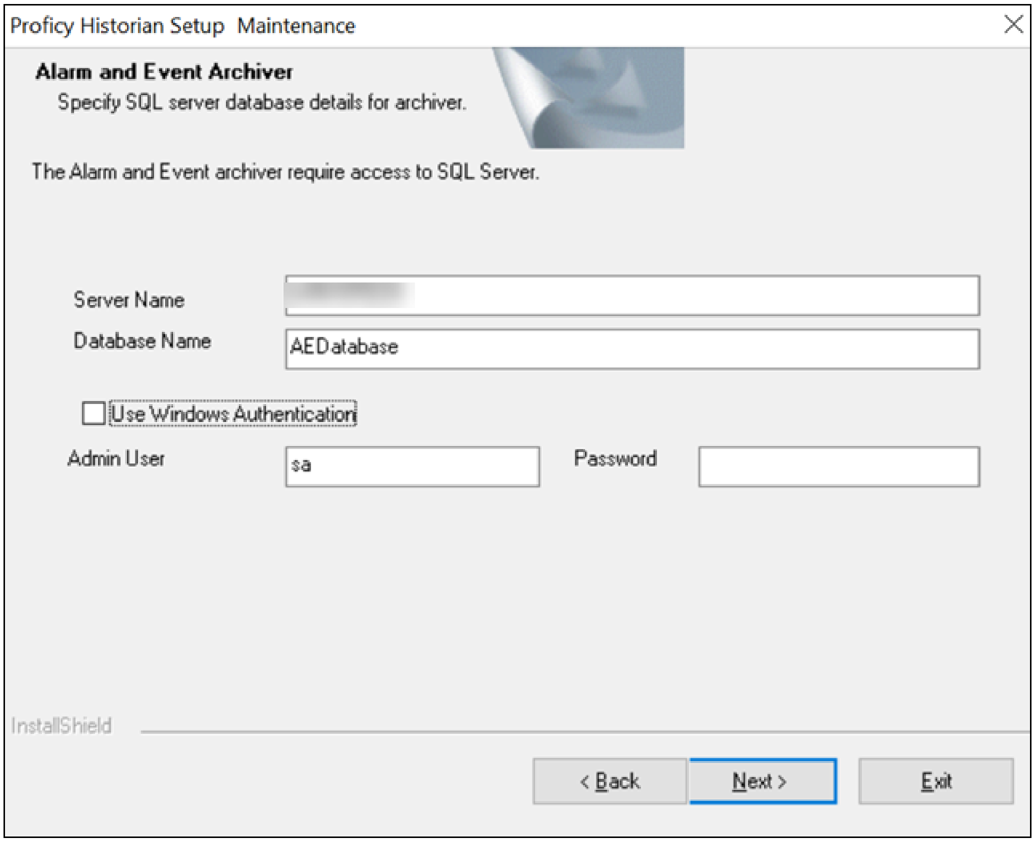
```
Help_Install.exe -s RootDrive=<installation drive> PortNumber=<port
 number>
```

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.

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: [redacted]

Database Name: AEDatabase

□ Use Windows Authentication

Admin User: sa

Password:

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.

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.

Install the Historian ETL Tools

If you want to use the Historian ETL tools to transfer data from a PI Historian server, you must install the PI SDK package.

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).

Note: If you want to upgrade Historian ETL:

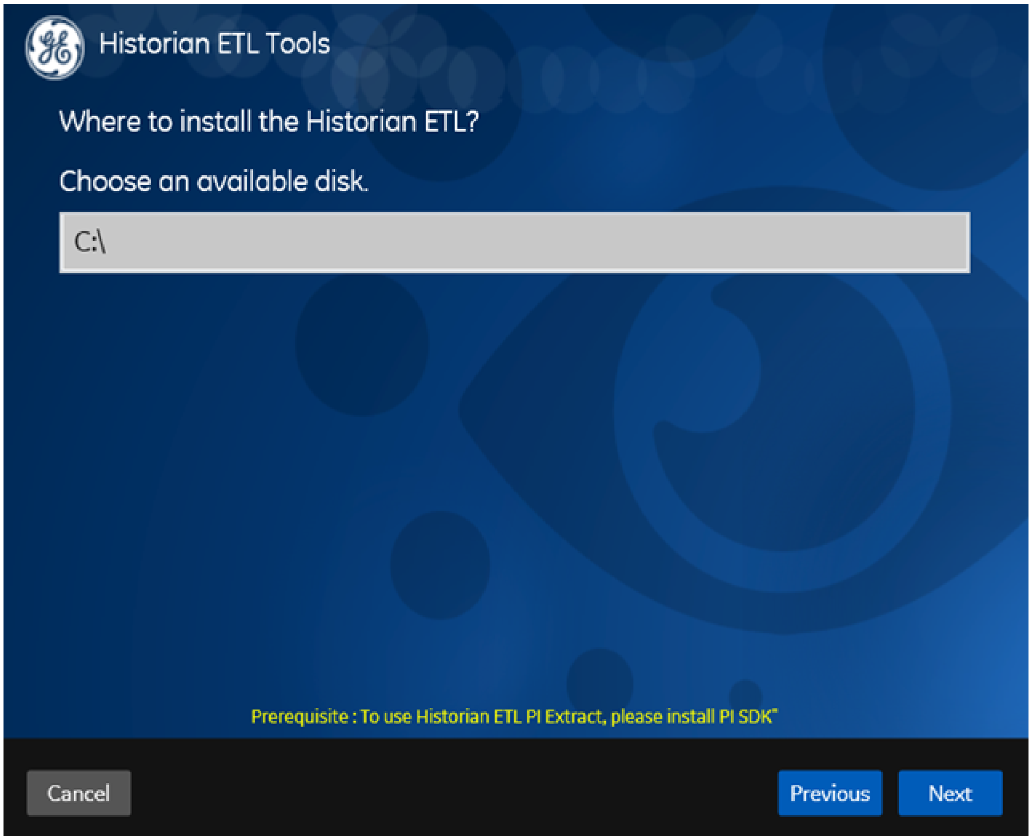
1. Uninstall the existing version of Historian ETL.
2. Backup the configuration files, and delete them.
3. Install the latest version of Historian ETL.

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.



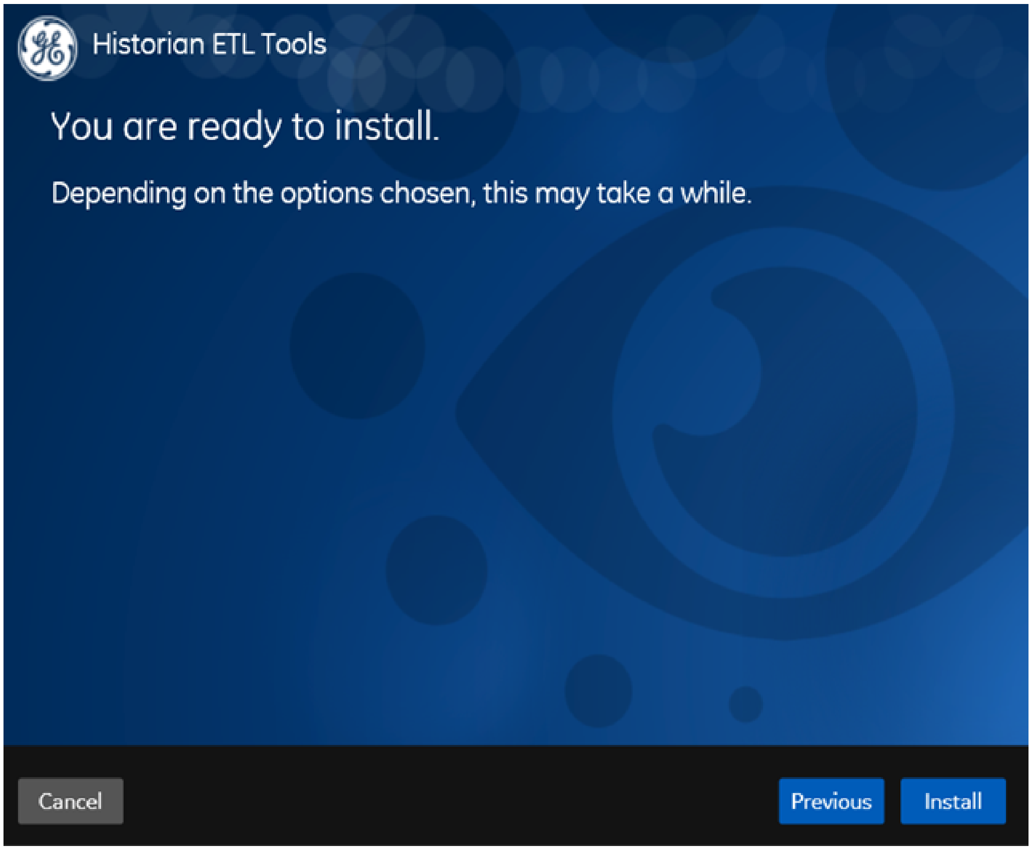
Where to install the Historian ETL?

Choose an available disk.

C:\

Prerequisite : To use Historian ETL PI Extract, please install PI SDK"

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.



Historian ETL Tools

You are ready to install.

Depending on the options chosen, this may take a while.

6. Select **Install**.

The Historian ETL tools are installed on your machine.

- The following folders are created in the `GE Digital` folder in the installation drive that you specified:
    - `Historian ETL Extract`
    - `Historian ETL Load`
    - `Historian ETL PI Extract`
    - `Historian ETL Transform`
- The following services are installed:
    - Historian ETL Extract
    - Historian ETL Load
    - Historian ETL PI Extract

Using External UAA or LDAP Groups with Historian

About User Account and Authentication (UAA)

In Historian, user authentication is handled using User Account and Authentication (UAA). UAA 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 UAA 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 UAA, you can choose between the following options while installing Web-based Clients:

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

This section describes how to use the UAA IdP Configuration tool to map remote UAA groups, LDAP groups, and LDAPS groups with the Historian UAA groups. For information on creating UAA groups and users using the UAA 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 UAA Groups

A UAA 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 UAA service, you can use them with Historian using the UAA LDAP Integration tool. This section describes how to map the groups in the remote UAA service with Historian UAA groups. By default, Historian contains the following UAA 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 UAA Users Using the UAA Config Tool *(page 179)*.

Workflow

1. Provide the details of the remote UAA service while installing Web-based Clients *(page 86)*.
2. Connect to the remote UAA service *(page 103)*.
3. Map the UAA groups *(page 130)* with that of the Historian UAA instance. You can map the groups in LDAP *(page 132)* and LDAPS *(page 134)* (LDAP via SSL) as well.

   Tip: To create UAA groups and users, refer to

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 UAA Groups With Historian UAA

Connect to the remote UAA service *(page 103)*.

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

1. Double-click the UAA IdP Configuration tool icon (), and log in the UAA 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 UAA Groups** check box.
3. In the **UAA 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 UAA.
   - Web-based Clients work only with a single instance of UAA, which is specified during Web-based Clients installation. After installation, you cannot change the instance of UAA that Web-based Clients will use.

Box	Description
URL	Enter the authorization server URL of the UAA service that you specified in the **UAA 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 UAA server is established, a message appears, confirming the same.
5. Select **Continue**.
   In the **UAA Mapping** section, the drop-down list box contains a list of groups in

   Historian UAA. In the **Filter** box, a list of groups in the existing UAA instance appear.
6. In the drop-down list box, select the Historian UAA group to which you want to map the existing UAA groups.
7. In the **Filter** box, select the check boxes corresponding to the existing UAA groups that you want to map.

   Note: If a group is already mapped to the UAA group that you have selected, the check box is already selected.
8. Select **Map Members**.

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

The existing UAA groups are mapped with the Historian UAA groups.

Map LDAP Groups with Historian UAA

- 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 UAA 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.

  ℹ **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 UAA groups with a Historian UAA 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 UAA *(page 134)*.

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 UAA IdP Configuration tool icon (), and log in the UAA client ID and secret.

   ℹ **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 **UAA Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL that you have specified in the **UAA Base URL** box during installation (for example: https://localhost/). For an external or a shared UAA instance, enter: https://<*UAA 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 UAA 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 UAA, enter the client secret of the external UAA.

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 if you have installed Web-based Clients in the domain controller machine. Otherwise, enter: ldap://<*domain server*>:389
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 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=scopes,dc=developers,dc=com).

7. Select **Test**.

8. After the connection is successful, select **Continue**.
   In the **UAA Mapping** section, the **UAA Group** field contains a list of groups in Historian UAA.

> ⓘ **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 **UAA Group** field, select the Historian Visualization UAA 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 UAA 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 UAA group is mapped with the LDAP groups that you have selected.

The LDAP groups are mapped with the Historian UAA groups.

Map LDAPS (LDAP via SSL) Groups with Historian UAA

- 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 UAA 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 UAA groups with a Historian UAA group, which is created using Web-based Clients installation. If you want to use LDAP without SSL, refer to Map LDAP Groups with Historian UAA *(page 132)*.

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 UAA 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/microsoftrservertigerteam/step-by-step-guide-to-setup-ldaps-on-windows-server

1. Double-click the UAA IdP Configuration tool icon (⚙), and log in the UAA 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 **UAA Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL that you have specified in the **UAA Base URL** box during installation (for example: https://localhost/). For an external or a shared UAA instance, enter: https://<*UAA 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 UAA 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 UAA, enter the client secret of the external UAA.

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, ldaps://localhost:636/). Use localhost if you have installed Web-based Clients in the domain controller machine. Otherwise, enter: ldaps://<*domain server*>:636 • 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).
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=scopes,dc=developers,dc=com).

7. Select **Test**.

8. After the connection is successful, select **Continue**.
   In the **UAA Mapping** section, the **UAA Group** field contains a list of groups in Historian UAA.

   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 UAA 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 UAA 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 UAA group is mapped with the LDAP groups that you have selected.

The LDAP groups are mapped with the Historian UAA groups.

Restart the GE Operations Hub UAA Tomcat Web Server service.

Remove Mapping Between Historian UAA 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 UAA group of Historian and LDAP. If you want to stop integration between the Historian UAA and LDAP altogether, you must remove the mapping for all the groups of the UAA instance.

1. Double-click the UAA IdP Configuration tool icon (), and log in the UAA 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 UAA Groups** check box.
3. In the **UAA Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL of the LDAP server. For example: `https://localhost/`

Box	Description
Client ID	Enter the UAA 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 UAA, enter the client secret of the external UAA.

4. Select **Test**.
   If connection to the UAA 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 UAA. In the **Filter** box, a list of LDAP groups appears.

8. In the drop-down list box, select the Historian UAA group whose mapping you want to remove.
   In the **Filter** box, check boxes for the UAA groups that are mapped to the selected Historian UAA 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 UAA groups of Historian UAA and LDAP is removed.

11. Repeat steps 8 through 10 for all the Historian UAA groups for which you want to remove the mapping.

Mapping between the UAA Groups of Historian and LDAP has been removed.

Remove Mapping Between UAA Groups of Historian and an Existing UAA Instance

If you want to stop users from a UAA group of an existing UAA instance from using Historian Web-based Clients, you can remove the mapping between the UAA group of Historian and the existing UAA instance. If you want to stop integration between the Historian UAA and the existing UAA instance altogether, you must remove the mapping for all the groups of the UAA instance.

1. Double-click the UAA IdP Configuration tool icon ( ), and log in the UAA 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 UAA Groups** check box.

3. In the **UAA Connection** section, provide values as specified in the following table.

Box	Description
URL	Enter the authorization server URL that you specified in the **UAA 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 UAA server is established, a message appears, confirming the same, and the **Continue** button is enabled.

5. Select **Continue**.
   In the **UAA Mapping** section, the drop-down list box contains a list of groups in Historian UAA. In the **Filter** box, a list of groups in the existing UAA instance appear.

6. In the drop-down list box, select the UAA group for which you want to remove the mapping.
   In the **Filter** box, check boxes for the UAA groups that are mapped to the selected Historian UAA group are selected.

7. In the **Filter** box, clear the check boxes corresponding to the UAA groups for which you want to remove the mapping.

8. Select **Map Members**.
   The mapping between the UAA groups of Historian UAA and the existing UAA instance is removed.

9. Repeat steps 6 through 8 for all the Historian UAA groups for which you want to remove the mapping.

Mapping between the UAA groups of Historian and the existing UAA instance has been removed.

Change the Log Levels of UAA

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 UAA Tomcat Wen 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 UAA Tomcat Web Server service.
4. If you want to change the Tomcat log level:

   a. Stop the GE Operations Hub UAA 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 UAA Tomcat Web Server service.

Upgrading Historian

Upgrade Historian

Procedure

To upgrade a Historian component, run the installer for the component. The component is upgraded automatically. For example, if you want to upgrade the Historian server, install the Historian server.

Things to Remember

- If you are upgrading from either Historian 6.0 Enterprise or previous releases of Historian 7.2 (including any of the service packs), this installation option will remove both Client Manager and Configuration Manager. This will have no impact on your data or use of Historian unless you intend to use a distributed system.
- If you want to upgrade Web-based Clients:
    - When you upgrade, Web-based Clients and associated data will be lost. Therefore, back up the 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 UAA Service *(page 161)*.

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

    - When you upgrade Web-based Clients, if 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 instead of installing Configuration Hub again.
    - 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, if you want to upgrade Web-based Clients, you must do either of the following:
        - ■ Install Web-based Clients on a new machine.

        - Uninstall the Historian server (remember to back up the UAA using the UAA_config_tool), 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 UAA server from the previous one, you must manually migrate the UAA data to new UAA server using the `uaa_config_tool` utility.
    - If you want to switch from using a local UAA to using an external UAA (or vice versa), you must manually change the UAA details.
- If you want to 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.
- If you want to upgrade Historian 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.
- If you install Web-based Clients before uninstalling the previous version, you cannot modify the Configuration Hub credentials.
- If an earlier version of Configuration Hub is available on the same machine, you will be allowed to use the same; you cannot install Configuration Hub again.

Retrieving Data from Historian

About Retrieving Data from Historian

After data collection, the Historian Server compresses and stores the information in a Data Archive or a `*.iha` file. Any client application can retrieve archived data through 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.

You can retrieve data from Historian using any number of clients, including but not limited to:

- Historian Analysis
- Knowledge Center

- iFIX
- CIMPLICITY
- Real-Time Information Portal
- Dream Reports
- Excel Add-In
- Custom SDK Applications
- OLE DB

Historian exposes various sampling and calculation modes that are used on retrieval of data that has already been collected to the archive. These modes do not effect data collection. Some sampling modes are suited to compressed data and should be used when collector compression or archive compression is used.

Sampling Modes

Sampling modes are used to specify how the data will be retrieved from Historian. Several modes are available, such as CurrentValue, Interpolated, Calculated and RawByTime. Sampling modes are specified in the client you use to retrieve data from Historian.

For more information, refer to the *Advanced Topics* section in the online help.

- For the Trend sampling mode, Historian ignores any leftover values at the end, rather than putting them into a smaller interval.
- For the Trend2 sampling mode, Historian creates as many intervals of the interval length as will fit into the sampling period, and then creates a remainder interval from whatever time is left.

- Spacing of timestamps returned:
  - For the Trend sampling mode, Historian returns evenly-spaced interval timestamps.
  - For the Trend2 sampling mode, Historian returns raw sample timestamps. These timestamps can be unevenly spaced, since raw data can be unevenly spaced.
- Inclusion of start and end times entered:
  - The Trend sampling mode is start time exclusive and end time inclusive.
  - The Trend2 sampling mode is start time inclusive and end time inclusive.

Trend sampling mode is more suitable for plotting applications that prefer evenly-spaced data.

Trend2 sampling mode is more suitable for analysis of mins and maxes and for plotting programs that can handle unevenly spaced data.

TrendtoRaw2: The TrendtoRaw2 sampling mode is a modified version of the TrendtoRaw sampling mode.

The TrendtoRaw2 sampling mode almost always produces the same results as the Trend2 sampling mode. The exception is that, when more samples are requested than there are raw data points, the TrendtoRaw2 sampling mode returns all of the available raw data points with no further processing.

Calculated: Returns samples based on a selected Calculation mode.

RawByFilterToggle: RawByFilterToggle returns filtered time ranges. The values returned are 0 and 1. If the value is 1, then the condition is true and 0 means false.

This sampling mode is used with the time range and filter tag conditions. The result starts with a starting time stamp and ends with an ending timestamp

Calculation Modes

Calculation modes are used when the sampling mode is set to Calculated. The data type of all calculated values will be DoubleFloat except for MinimumTime, MaximumTime, FirstRawTime and LastRawTime which will be a Date. The data type of the values of FirstRawValue and LastRawValue will be the same as that of the selected tag.

Calculation Mode	Results
Count	Displays the number of raw samples in the specified interval. This only indicates the count and does not display the actual values or qualities of the samples. The Count calculation mode is useful for analyzing the distribution of raw data samples. If you have a higher number of raw samples than expected, you may decide to implement collector or archive compression. If samples are missing, then you may want to slow your collection rates.
State Count	Displays the number of times a tag has transitioned to another state from a previous state. A state transition is counted when the previous good sample is not equal to the state value and the next good sample is equal to state value.
State Time	Displays the duration that a tag was in a given state within an interval.
Minimum	Displays the minimum value in a specified interval with good data quality. This value may be raw or interpolated. **Note:** The Minimum and MinimumTime calculation retrieve two additional samples per interval; one is interpolated at the interval start time and the other is interpolated at the interval end time. These samples are used to determine the min or max just like any raw value.
MinimumTime	Displays the time stamp of the minimum value in a specified interval. See the note in Minimum for additional information.
Maximum	Displays the maximum value in a specified interval. **Note:** The Maximum and MaximumTime calculation internally retrieve two additional samples per interval; one is interpolated at the interval start time and the other is interpolated at the interval end time. These samples are used in the min or max just like any raw or interpolated value.
MaximumTime	Displays the time stamp of the maximum value in a specified interval. See the note in Maximum for additional information.

Calculation Mode	Results
RawAverage	Displays the arithmetic average of the raw values in a specified interval with good data quality. This is useful only when a sufficient number of raw data values are collected.
Average	Similar to RawAverage, but performs a special logic for time weighting and for computing the value at the start of the interval. This is useful for computing an average on compressed data.
OPCQOr and OPCQAnd	The OPCQOr is a bit wise OR operation of all the 16 bit OPC qualities of the raw samples stored in the specified interval. The OPCQAnd is a bit wise AND operation of all the 16 bit OPC qualities of the raw samples stored in the specified interval.
Total	Retrieves the time-weighted total of raw and interpolated values for each calculation interval. The collected value must be a rate per 24 hours. This calculation mode determines a count from the collected rate.
RawTotal	Displays the arithmetic sum of raw values in a specified interval.
StandardDeviation	Displays the time-weighted standard deviation of raw values for a specified interval.
RawStandardDeviation	Displays the arithmetic standard deviation of raw values for a specified interval.
TimeGood	Displays the amount of time (in milliseconds) during an interval when the data is of good quality and matches filter conditions if the filter tag is used.
FirstRawValue	Returns the first good raw value for a specified time interval.
FirstRawTime	Returns the timestamp of the first good raw for a specified time interval.
LastRawValue	Returns the last good raw value for a specified time interval.
LastRawTime	Returns the timestamp of the last good raw for a specified time interval.
TagStats	Allows you to return multiple calculation modes for a tag in a single query.

Note: You can also use INCLUDEBAD or FILTERINCLUDEBAD as query modifiers to include bad quality data. For more information, refer INLUDEBAD and FILTERINCLUDEBAD sections in Advanced Topics.

Query Modifiers

Query Modifiers are used for retrieving data that has been stored in the archive. They are used along with sampling and calculation modes to get a specific set of data.

- The time interval is great than 1 minute.
- The collection interval is greater than 1 second.
- The data node size is greater than the default 1400 bytes.
- The data type of the tags is String or Blob.

Query performance varies depending on all of the above factors.

Use this query modifier only with FirstRawValue, FirstRawTime, LastRawValue, and LastRawTime calculation modes.

EXCLUDESTALE:

- Stale tags are tags that have no new data samples within a specified period of time, and which have the potential to add to system overhead and slow down user queries.
- The EXCLUDESTALE query modifier allows for exclusion of stale tags in data queries.
- Unless permanently deleted, stale tags from the archiver are not removed but are simply marked as stale. Use the query without this query modifier to retrieve the sample values.
- Data is not returned for stale tags. An ihSTATUS_STALED_TAG error is returned instead.

Filtered Data Queries

Filtered data queries enhance Historian by adding filter tags and additional filtering criteria to standard queries. Unfiltered data queries in Historian allow you to specify a start and end time for the query, then return all data samples within that interval. A filtered data query, however, will allow you to specify a condition to filter the results by, as well as calculation modes to perform on the returned data. Filtered data queries are performed on the Historian server.

For example, a filtered data query is useful when trying to retrieve all data for a specific Batch ID, Lot Number, or Product Code and for filtering data where certain limits were exceeded, such as all data where a temperature exceeded a certain value. Rather than filtering a full day's worth of process data in the client application, you can filter data in the Historian archiver, and only return the matching results to the client application. The result is a smaller, more relevant data set.

You can use filter criteria with raw, interpolated, and calculated sampling modes. You cannot use it with current value sampling. The logic of selecting intervals is always interpolated, even when the data retrieval is raw or calculated. The value that triggers a transition from false to true can be a raw value or interpolated value.

You cannot use a filtered data query in an iFIX chart. For more information, refer to Advanced Topics section in the online help.

Filter Parameters for Data Queries

Use of filter parameters with a data query is optional.

- AND Condition
- OR Condition
- Combination of both AND and OR

Filter Expression can be used instead of FilterTag, FilterComparisonMode and FilterValue parameters. While using FilterExpression, the expression is passed within single quotes and for complex expressions we write the conditions within a parenthesis. There is no maximum length for a filter expression, but if it is called using OLEDB or Excel, they may have their own limitations.

Filter Mode: The type of time filter.

The Filter Mode defines how time periods before and after transitions in the filter condition should be handled.

For example, AfterTime indicates that the filter condition should be True starting at the timestamp of the archive value that triggered the True condition and leading up to the timestamp of the archive value that triggered the False condition.

ExactTime

Retrieves data for the exact times that the filter condition is True (only True).

BeforeTime

Retrieves data from the time of the last False filter condition up until the time of the True condition (False until True).

AfterTime

Retrieves data from the time of the True filter condition up until the time of next False condition (True until False).

BeforeAndAfterTime

Retrieves data from the time of the last False filter condition up until the time of next False condition (While True).

Filter Comparison Mode: Filter Comparison Mode is only used if Filter Tag is filled in. The Filter Comparison Mode defines how archive values for the Filter Tag should be compared to the Filter Value to establish the state of the filter condition. If a Filter Tag and Filter Comparison Value are supplied, time periods are filtered from the results where the filter condition is False.

The type of comparison to be made on the filter comparison value:

Equal

Filter condition is True when the Filter Tag is equal to the comparison value.

EqualFirst

Filter condition is True when the Filter Tag is equal to the first comparison value.

EqualLast

Filter condition is True when the Filter Tag is equal to the last comparison value.

NotEqual

Filter condition is True when the Filter Tag is NOT equal to the comparison value.

LessThan

Filter condition is True when the Filter Tag is less than the comparison value.

GreaterThan

Filter condition is True when the Filter Tag is greater than the comparison value.

LessThanEqual

Filter condition is True when the Filter Tag is less than or equal to the comparison value.

GreaterThanEqual

Filter condition is True when the Filter Tag is greater than or equal to the comparison value.

AllBitsSet

Filter condition is True when the binary value of the Filter Tag is equal to all the bits in the condition. It is represented as ^ to be used in Filter Expression.

AnyBitSet

Filter condition is True when the binary value of the Filter Tag is equal to any of the bits in the condition. It is represented as ~ to be used in Filter Expression.

AnyBitNotSet

Filter condition is True when the binary value of the Filter Tag is not equal to any one of the bits in the condition. It is represented as !~ to be used in Filter Expression.

AllBitsNotSet

Filter condition is True when the binary value of the Filter Tag is not equal to all the bits in the condition. It is represented as !^ to be used in Filter Expression.

Alarm Condition

Specifies an alarm condition to filter data by. For example, Level.

Alarm SubCondition

Specifies an alarm sub-condition to filter data by. For example, HIHI.

Filter Comparison Value: Filter Comparison Value is only used if Filter Tag is filled in. The value to compare the filter tag with when applying the appropriate filter to the data record set query (to determine the appropriate filter times).

Filtered Queries in the Excel Add-in Example

This example shows how a filtered data query returns specific data from the Historian archive. The example uses two tags: `batchid` and ramp. The `batchid` tag is updated before a new batch is produced with the new batch's ID. The `ramp` tag contains raw data sent by a device in the process. In this example, it is requested that Historian return data samples at ten second intervals for the `ramp` tag during the period that the `batchid` tag is set to B1.

A standard query in Historian for the ramp tag's values between 08:00 and 08:01, at ten second intervals, would look like this:

Time Stamp	Value	Data Quality
07/30/2003 08:00:00	B0	Good
07/30/2003 08:00:20	B1	Good
07/30/2003 08:00:45	B2	Good

Filtering Data Queries in the Excel Add-in

You can enter your filter conditions using Filter tag, Filter Comparison Mode, and Filter Comparison Value or you can put that all that information in a single FilterExpression. You can enter the filter conditions in the FilterExpression field of the **Historian Data Query** window. The filter conditions are passed within single quotes.

To find the values of the `ramp` tag for the B1 batch, enter the following values into the **Historian Filtered Data Query** window:

1. In the `Tag Name(s)` field, enter the tag you want to receive results from - the `ramp` tag in this example.
2. Select a start and end time for your query.
3. In the `Filter Tag` field, enter the tag you want to enable filtering with - `batchid` in this example.
4. In the `Filter Comparison` field, select your comparison condition.
5. n the `Include Data Where Value Is` field, enter your filter condition value.
6. In the `Include Times` field, select your filter mode.
7. In the `Sampling Type` field, select your sampling mode.
8. In the `Calculation` field, select your calculation mode.
9. Select your `Sampling Interval`.
10. In the `Output Display` field, select the tag values you want to display.

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 *(page 46)*
   b. Alarms and Events *(page 124)*
   c. Collectors *(page 104)*
   d. Client Tools *(page 83)*
   e. Standalone Help *(page 123)*
2. Back up the alarms and events data *(page 151)*.
3. Install Microsoft SQL on the target machine. Refer to Software Requirements *(page 36)* 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 *(page 46)*
    b. Alarms and Events *(page 124)*
    c. Collectors *(page 104)*
    d. Client Tools *(page 83)*
    e. Standalone Help *(page 123)*
7. Back up the alarms and events data *(page 151)* that you have restored in step 3.
8. Install a supported version of Microsoft SQL on the target machine. Refer to Software Requirements *(page 36)* 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 *(page 46)*
2. Alarms and Events *(page 124)*
3. Collectors *(page 104)*
4. Client Tools *(page 83)*
5. Standalone Help *(page 123)*

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 *(page 152)* that you have backed up. Refer to Software Requirements *(page 36)* for a list of supported versions.

Restore the Alarms and Events Data

Install Microsoft SQL. Refer to Software Requirements *(page 36)* 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 *(page 154)*.)

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`.

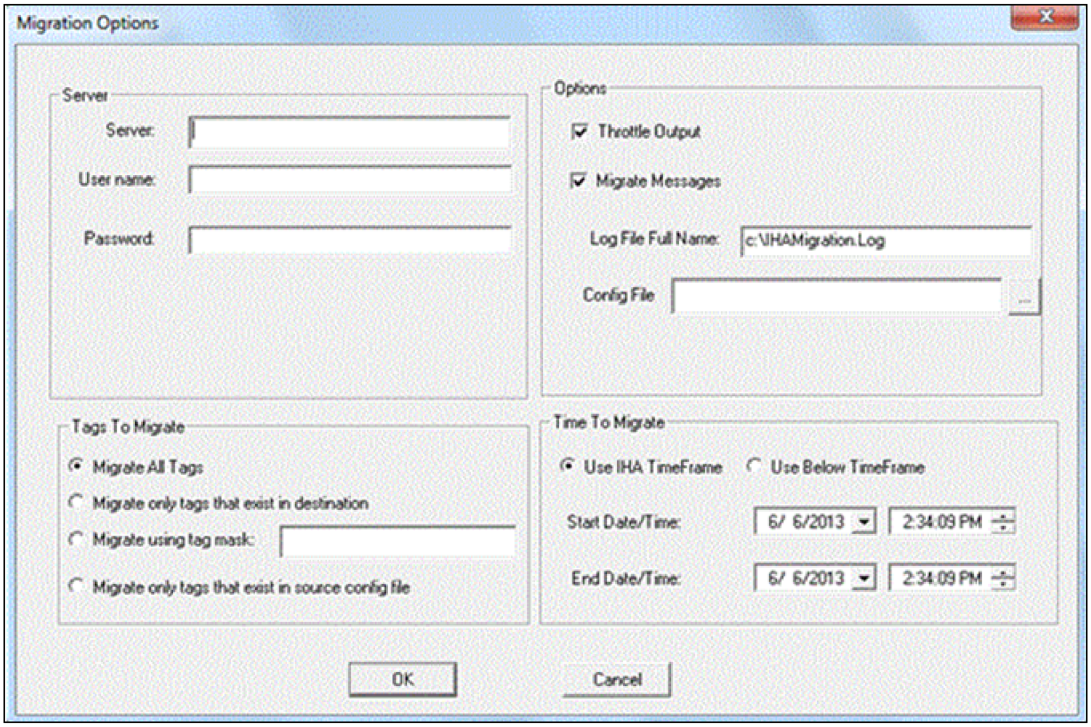
6. Optionally, perform these steps:
    a. You can upgrade the older version's archive files to the latest version by selecting the bulk upgrade option.
    Stop the Data Archiver service and select **File > Bulk Upgrade Historical Data**.

       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.



Migration Options

Server

Server:

User name:

Password:

Options

☑ Throttle Output

☑ Migrate Messages

Log File Full Name: c:\IHAMigration.Log

Config File

Tags To Migrate

● Migrate All Tags

○ Migrate only tags that exist in destination

○ Migrate using tag mask:

○ Migrate only tags that exist in source config file

Time To Migrate

● Use IHA TimeFrame ○ Use Below TimeFrame

Start Date/Time: 6/ 6/2013 2:34:09 PM

End Date/Time: 6/ 6/2013 2:34:09 PM

2. Enter options the following options.

Related reference

[Server Pane *(page 155)*](#)
[Options Pane *(page 155)*](#)
[Tags to Migrate Pane *(page 155)*](#)
[Time to Migrate Pane *(page 156)*](#)

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
`/NOTHROTTLE`	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.
`/NOMESSAGES`	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.
`/EXISTINGTAGS`	This will migrate data for only those tags that exist in the destination archiver.

Option	Description
`/b`	This option of the `start.exe` 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.
`/wait`	This option of the `start.exe` file allows each instance of the IHA Migration tool to complete the migration before starting the next migration in the sequence.
`/NOIHC`	This option skips verifying for IHC file and proceed with the migration. IHC file is not required, if batch command have /NOIHC 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 UAA Service

Starting Historian 8.0 version, you can use the common User Account and Authentication (UAA) service.

Note: You can either choose the common UAA deployed by any other products such as, Operations Hub, Plant Apps; or the common UAA deployed by Historian.

To use the common UAA service, you must migrate the UAA data should from Historian to the new local or external UAA.

To enable this migration of data the `uaa_config_tool` is introduced.

Note:

- While migrating UAA details, we are setting default password as user123 for all the users. You should change it using UAA 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 UAA 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 UAA data.
2. Migrate the data to an existing common UAA 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 UAA. 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 UAA 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 UAA 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 of 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 *(page)*.

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 execute UAA commands, refer to Managing UAA Users Using the UAA Config Tool *(page 179)*.

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 OLEDB program, user written programs, or any other Proficy software.
Enabled	Disabled	Use this if you are unable to upgrade collectors to the latest version if there is no SIM update for your collector.
Disabled	Enabled	Use this if you have to support legacy clients and you are unable to install the SIM update on all clients.
Disabled	Disabled	Use this for maximum compatibility with existing systems.

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 *(page 167)*.

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 UnAudited Writers	iH UnAudited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
Create Tags: • Excel Add-In • SDK • Historian Admins • File collector	X						X	
Remove Tags: • Historian Admins • SDK	X						X	
Modify Tags: • Excel Add-In • SDK • Historian Admins • File collector	X						X	
Modify Archive Security: • SDK • Historian Admins	X							
Backup Archive: • SDK • Historian Admins	X					X		

Function	iH Security Admins	iH UnAudited Writers	iH UnAudited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
Restore Backup: • SDK • Historian Admins	X					X		
Create Archive: • SDK • Historian Admins	X					X		
Start/Stop Collector: • SDK • Historian Admins • Mission Control (iFIX)	X							X
Browse Collector: • Historian Admins	X							X
Read Data: • Chart Object • Excel Add-In • SDK	X				X			
Write Data (UnAudited): • Excel Add-In • SDK	X	X	X					

Function	iH Security Admins	iH UnAudited Writers	iH UnAudited Login	iH Audited Writers	iH Readers	iH Archive Admins	iH Tag Admins	iH Collector Admins
Write Data (Audited): • Excel Add-In • SDK	X			X				
Modify Data: • Excel Add-In • SDK	X	X	X	X				
Update Security for Tag: • Excel Add-In • SDK • Historian Admins	X							
Migrate: • Migration Tools	X							
Login Connection Messages	X	X		X	X	X	X	X

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

User	Needs	Added to Security Group
USER2 USER3 USER5 USER6 USER8	• Read/Write Data (no messages). • Create, modify, and delete tags. • Backup, restore, and create archives. • Connect to Data Archiver without creating login successful audit messages	• iH UnAudited Writers • iH Tag Admins • iH Archive Admins • iH UnAudited Logins
USER4 USER7	• iRead/Write Data (no messages). • iCreate, modify, and delete tags. • iStart/Stop Collectors. • iBackup, restore, and create archives.	• 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 *(page 167)*.

   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**.

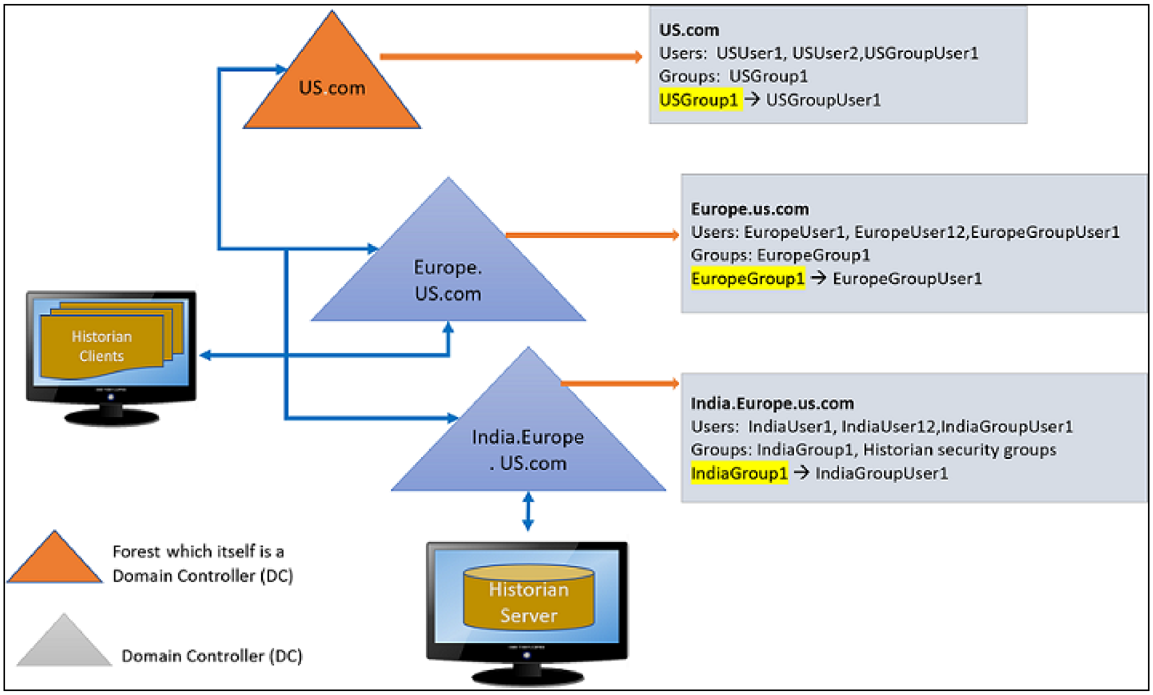
Active Directory Setup - an Overview

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:


US.com
US.com
Users: USUser1, USUser2,USGroupUser1
Groups: USGroup1
USGroup1 → USGroupUser1
Europe.
US.com
Europe.us.com
Users: EuropeUser1, EuropeUser12,EuropeGroupUser1
Groups: EuropeGroup1
EuropeGroup1 → EuropeGroupUser1
Historian
Clients
India.Europe
. US.com
India.Europe.us.com
Users: IndiaUser1, IndiaUser12,IndiaGroupUser1
Groups: IndiaGroup1, Historian security groups
IndiaGroup1 → IndiaGroupUser1
Forest which itself is a
Domain Controller (DC)
Historian
Server
Domain Controller (DC)

Configuring the Domain Users for active directory setup

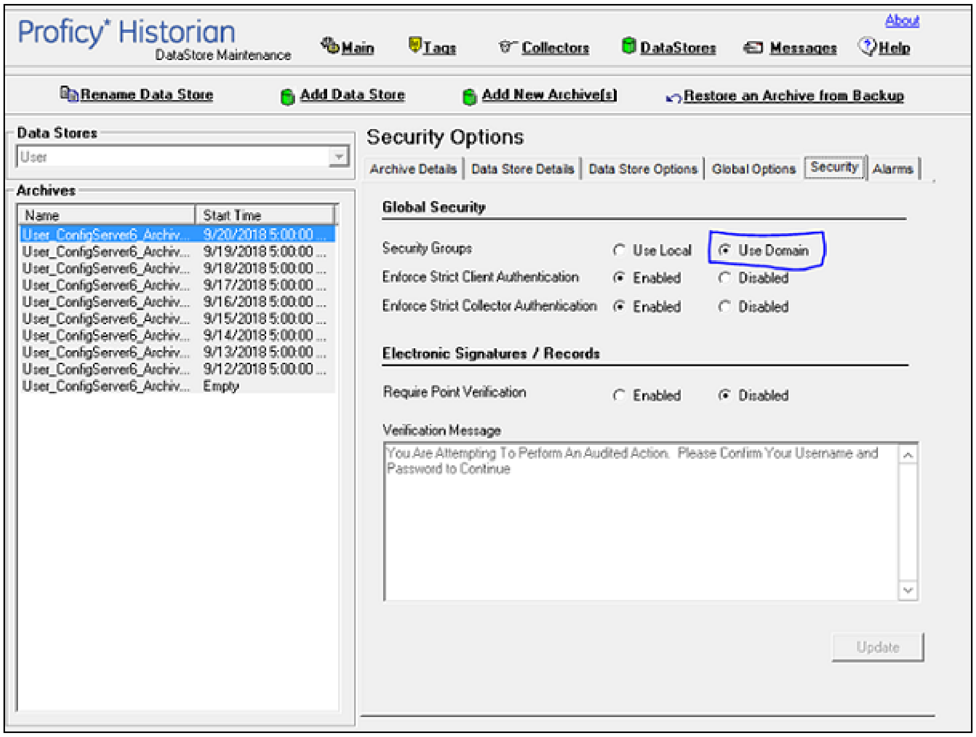
To configure the domain (single\multi) environment in Historian Administrator:

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 contains 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.



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 ...
User_ConfigServer6_Archiv...	Empty

Global Security

Security Groups ○ Use Local ● Use Domain

Enforce Strict Client Authentication ● Enabled ○ Disabled

Enforce Strict Collector Authentication ● Enabled ○ Disabled

Electronic Signatures / Records

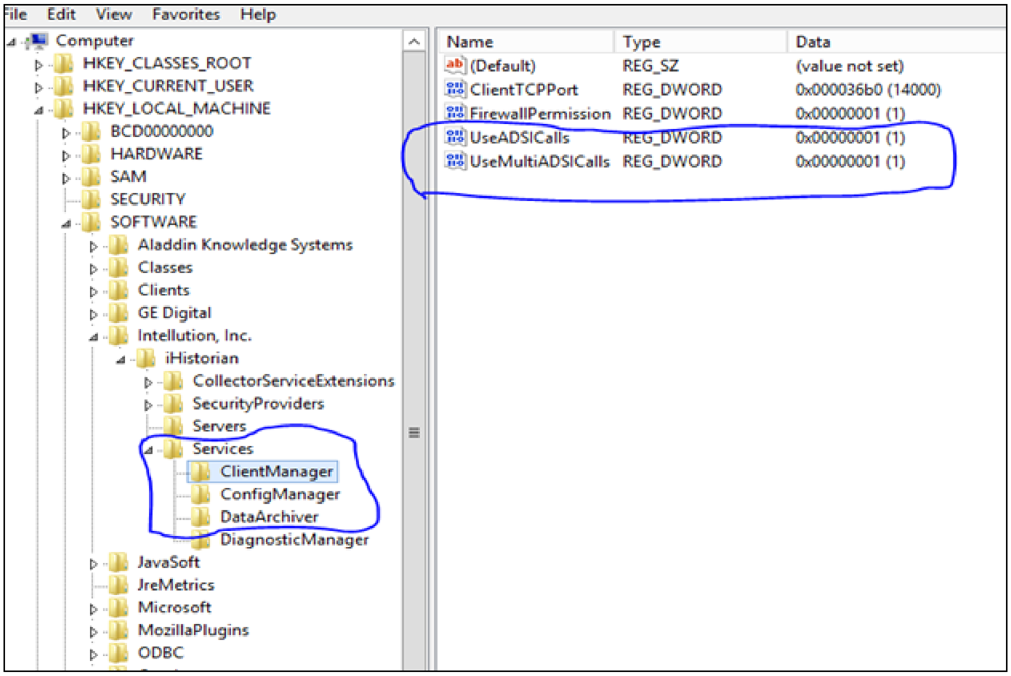
Require Point Verification ○ Enabled ● Disabled

Verification Message

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

2. Stop the Historian Services.

3. Add the Registry Entries for ClientManager, ConfigManager and DataArchiver as shown below. Registry path: *\HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\Services\*



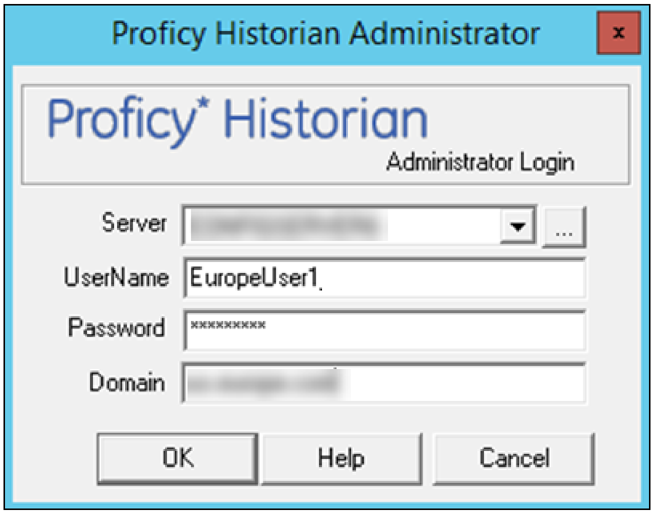
Name	Type	Data
(Default)	REG_SZ	(value not set)
ClientTCPPort	REG_DWORD	0x000036b0 (14000)
FirewallPermission	REG_DWORD	0x00000001 (1)
UseADSICalls	REG_DWORD	0x00000001 (1)
UseMultiADSICalls	REG_DWORD	0x00000001 (1)

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.



Server [redacted]

UserName EuropeUser1

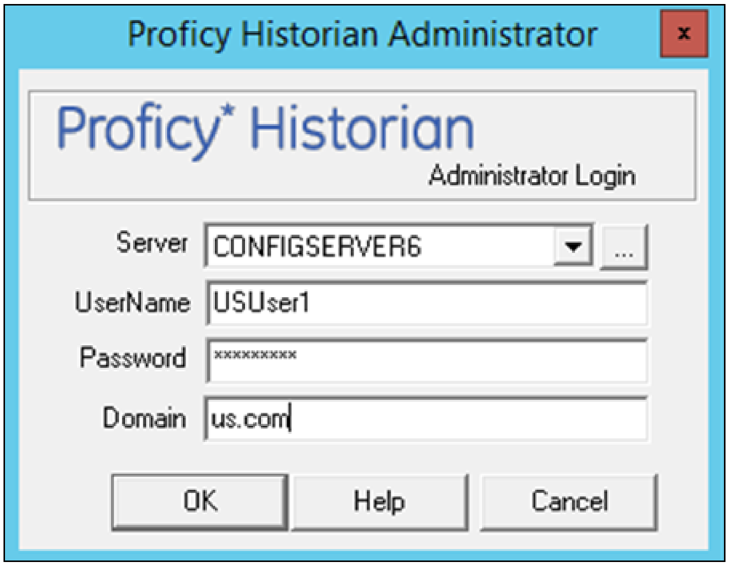
Password **********

Domain [redacted]

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.



Server CONFIGSERVER6

UserName USUser1

Password **********

Domain us.com

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 EuropGroupUser1 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 UAA Users Using the UAA Config Tool

Use the UAA Config tool to perform the following tasks:

- Add a local UAA user.

  Note: Here a local UAA user means a user defined by UAA, not by an external identity provider such as LDAP.

- Remove a local UAA user.
- Reset the password for a local UAA user.
- Add a local UAA user to an existing UAA group.

  Since OAuth2 scopes are implemented as UAA groups, this means the same as adding a scope to a user.
- Remove a local UAA user from an existing UAA group.

A user who performs these functions is acting 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 HTTS 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

`-t`	`--Target`	URL of the UAA instance that the command should be performed on. Typically, the URL is `https://localhost:8443/uaa`, which is the default value. This option is optional and is only needed when the user wants to run the command against a remote UAA instance (which is not recommended due to security concerns).
`-n`	`--ClientId`	ID of the client that the user is acting as. By default, it is `admin`. This option is optional and is only needed when the admin has set up the UAA to delegate certain operations to others.
`-s`	`--ClientSecret`	This is the secret used to authenticate the user for acting as the admin client (or an alternative client given in a `--ClientId` option). If the user has elected to cache the secret previously, then this option can be omitted. Otherwise, it has to be provided. The password must satisfy the following conditions: • Must not contain only numbers. • Must not begin or end with a special character. • Must not contain curly braces.
`-c`	`--CacheSecret`	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.
`-u`	`--UserName`	Name of the user that the tool is being invoked for. For example, the user that is being added or removed.
`-p`	`--UserPassword`	The password for the user being added or whose password is being reset. The option is only needed for the `add_user` and `set_user_password` commands.
`-g`	`--Group`	Name of the UAA group (scope) that the user is being added to or removed from. The option is only needed for the `add_user_to_group` and `remove_user_from_group` commands.

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 UAA 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 UAA 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 UAA user.
2. Add the new user to the appropriate Historian Security group on the local historian machine or on the domain server.

Create a UAA Reader Client Using the UAA Config Tool

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 UAA client. The UAA client will be automatically added to the iH Readers security group. Therefore, you can use the client to fetch Historian data using REST APIs.

1. Access the UAA Config tool, which is located in the following folder y default: `C:\Program files\GE Digital\Historian Config`

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://<UAA 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://UAAURI2010:443/uaa
```

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

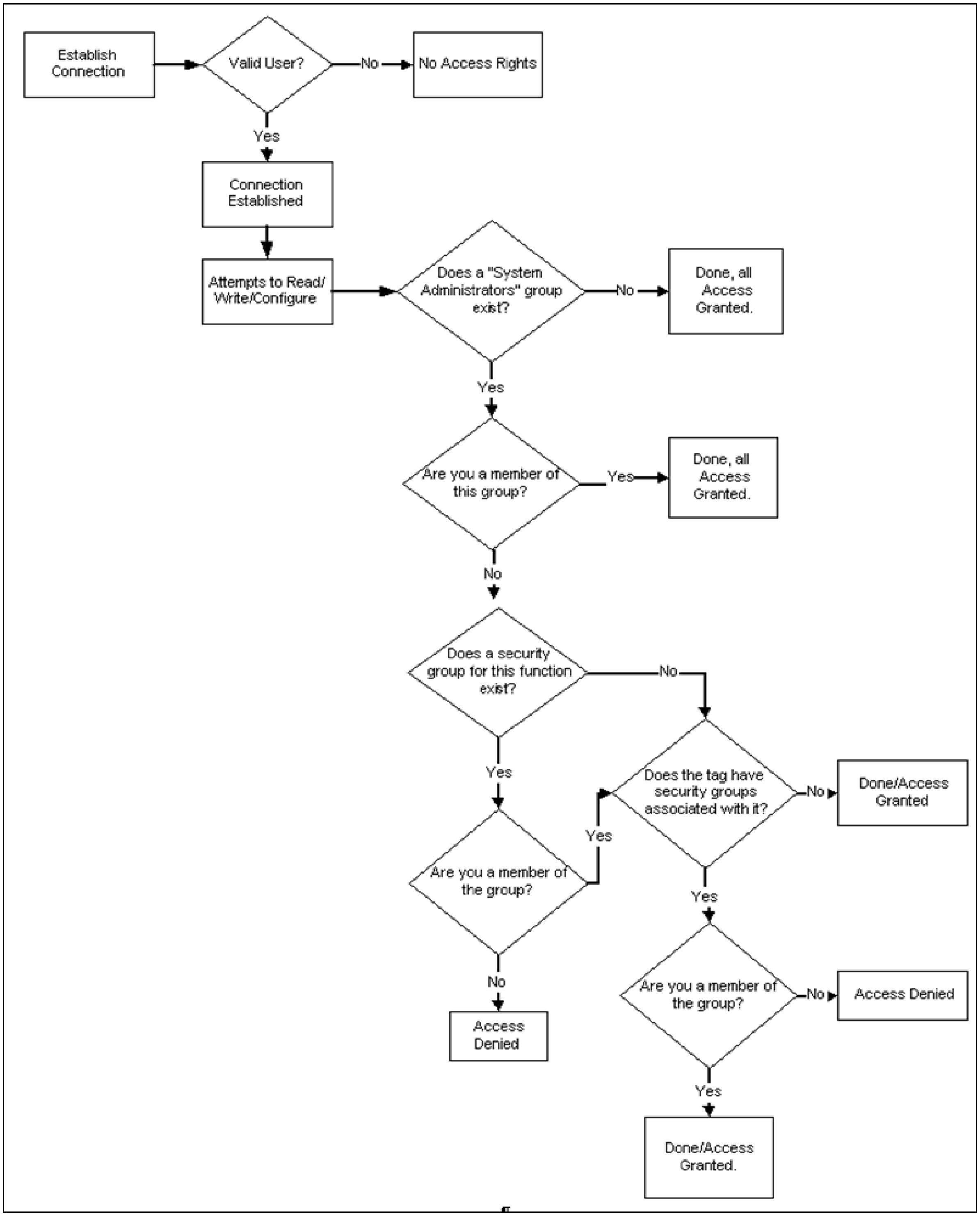
checks that user. If username and password are not supplied and you are on a Windows 2003 or Windows 2008 machine or higher, security checks the currently logged in user.

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: Security Checking Process


Establish Connection
Valid User?
No
No Access Rights
Yes
Connection Established
Attempts to Read/ Write/Configure
Does a "System Administrators" group exist?
No
Done, all Access Granted.
Yes
Are you a member of this group?
Yes
Done, all Access Granted.
No
Does a security group for this function exist?
No
Yes
Does the tag have security groups associated with it?
No
Done/Access Granted
Yes
Are you a member of the group?
Yes
No
Access Denied
Are you a member of the group?
No
Access Denied
Yes
Done/Access Granted.

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 *(page 173)*.

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. Open Historian Administrator.
2. Select the **Tags** link.
   The **Tag Maintenance** page appears.
3. Select a tag (or group of tags) from the **Tag Name** section of the **Tag Maintenance** page.
4. Select **Advanced** to display the advanced tag options.
5. In the **Read Group**, **Write Group**, or **Admin Group** field, select the security group that you wish to assign to the tag from the drop-down list.
   The drop-down list automatically lists all security groups that are defined in your Windows security environment.

   For example, if an iH Security Admins user selects a tag and chooses power users from the **Read Group** drop-down list, 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.

   Note: If you are using domain groups (instead of local groups), the **Read Group**, **Write Group**, and **Admin 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 UAA details, favourites, and so on. Therefore, if you want to retain UAA details, do not select that check box.
    - If you have installed Operations Hub on the same machine, and if there is a shared UAA 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 UAA package will not be deleted in that case.

- 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.
- If you want to uninstall collectors, delete all the instances of the collectors that you have created. You can do so using Configuration Hub or Remote Collector Management. The following instances of collectors (the ones that were created during the installation of collectors) are deleted automatically:
    - 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

  Even after you uninstall collectors and Web-based Clients, the corresponding Windows services and registry entries are not removed.

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**.

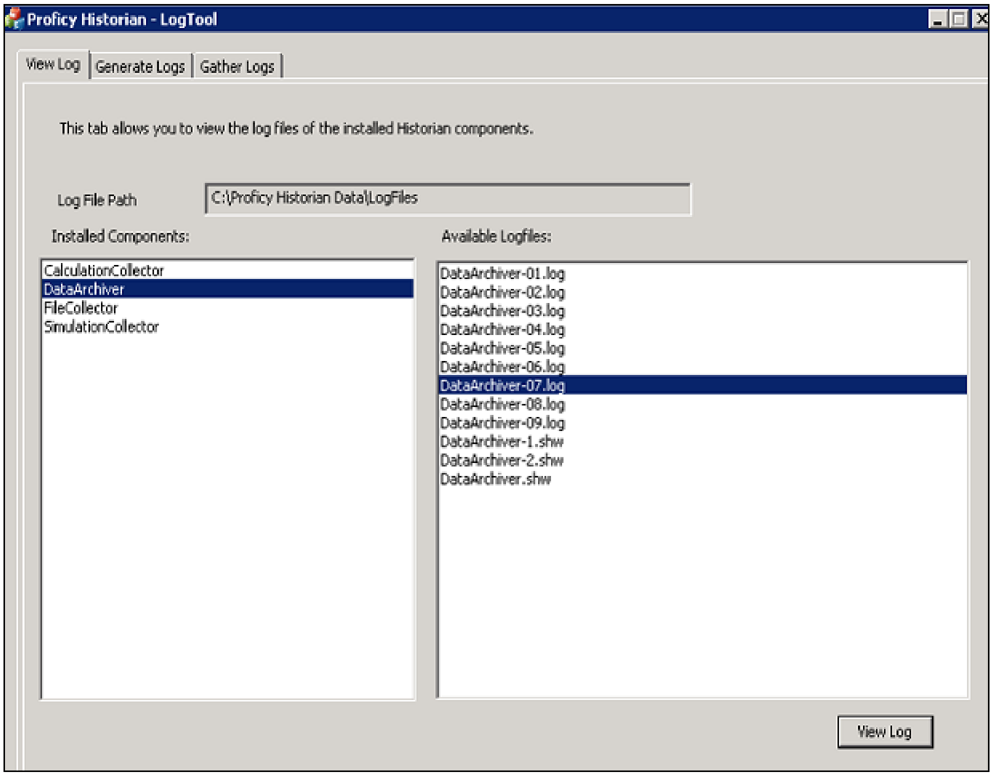
2. To remove all related software from your computer:
    a. Double-click the **Programs / Uninstall a Program** link in the Control Panel.
    b. Select **Proficy Common Licensing**, and select **Uninstall**.

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 \Proficy\Proficy Historian\X64`.

1. Go to your installation directory and execute the `Logtool.exe` file.
   The **LogTool** opens, displaying the **View Log** section.



This tab allows you to view the log files of the installed Historian components.

Log File Path: C:\Proficy Historian Data\LogFiles

Installed Components:

CalculationCollector
DataArchiver
FileCollector
SimulationCollector

Available Logfiles:

DataArchiver-01.log
DataArchiver-02.log
DataArchiver-03.log
DataArchiver-04.log
DataArchiver-05.log
DataArchiver-06.log
DataArchiver-07.log
DataArchiver-08.log
DataArchiver-09.log
DataArchiver-1.shw
DataArchiver-2.shw
DataArchiver.shw

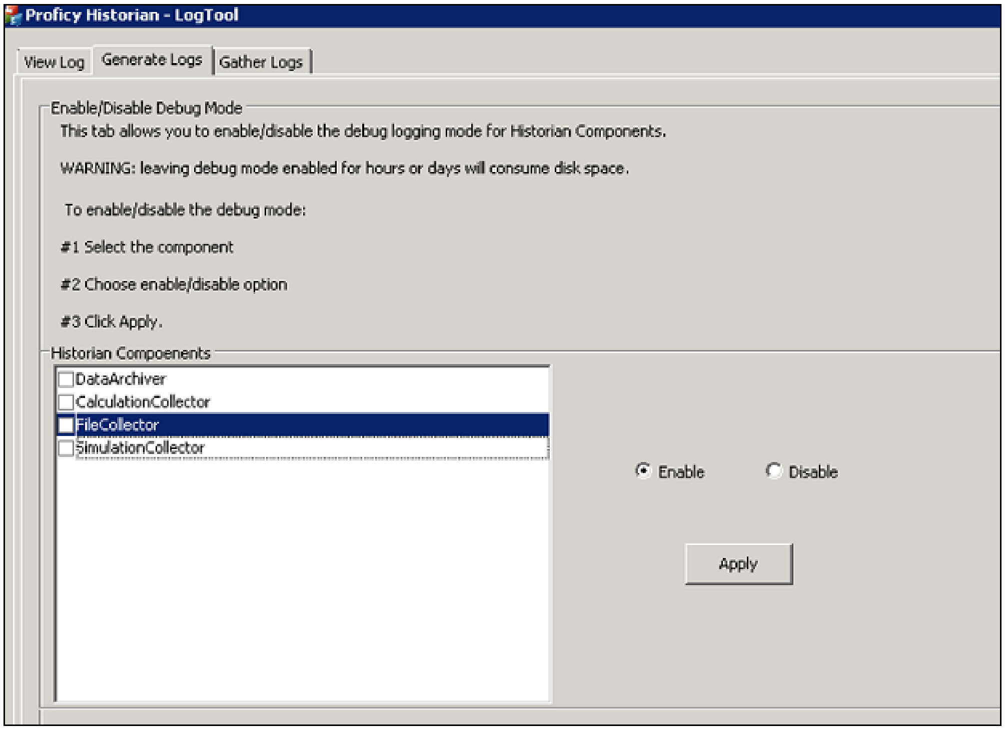
2. Select a component from the left panel to see the available log files, and select **View Log**.
3. Select **Generate Logs** to enable or disable the debug logging mode for Historian components:

   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



Enable/Disable Debug Mode

This tab allows you to enable/disable the debug logging mode for Historian Components.

WARNING: leaving debug mode enabled for hours or days will consume disk space.

To enable/disable the debug mode:

#1 Select the component

#2 Choose enable/disable option

#3 Click Apply.

Historian Compoenents

☐ DataArchiver
☐ CalculationCollector
☐ FileCollector
☐ SimulationCollector

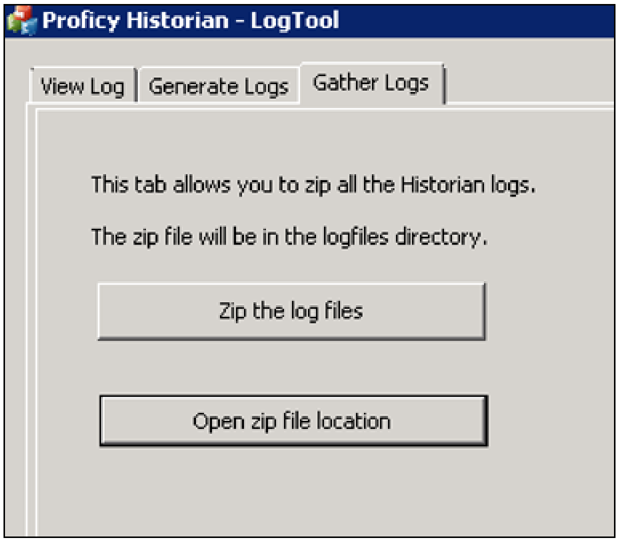
● Enable ○ Disable

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.



This tab allows you to zip all the Historian logs.

The zip file will be in the logfiles directory.

Troubleshooting Historian

Before troubleshooting any performance-related issue, make sure the computer meets the recommended hardware requirements *(page 30)*.

Troubleshooting Strict Authentication Issues

If the Historian Server rejects valid collector or client user credentials while connecting, consider the following condition:

Time Sync between the Server Time and Domain Controller Time

If a client or collector is attempting to connect to the Historian server with Strict Authentication enabled on a Kerberos configuration, ensure that the Server time and Domain Controller time match with each other. Otherwise, the server rejects valid credentials and does not allow the connection.

Troubleshooting Historian Server Components

Changing Service Port Numbers: To change the port number of any of the Configuration Manager, Data Archiver or Diagnostics Manager:

1. From Historian Admin Console, change the **Port Number** from the **Services** page.

   Note: You cannot update the port number of a service which is already in use in the same machine.

2. Ensure that the changed port numbers are updated in the registry which is located at `HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\Services`.

   If the port number is not updated, you must update it manually.
3. Restart the corresponding service.

   For example, if you change the port number of the Data Archiver, then you must restart the Data Archiver service.

Connecting a Historian Server to a Historian Client through a Firewall: To connect a Historian server to a Historian Client through a firewall from a remote machine, you must enable the public HTTPS port number that you have specified while installing Web-based Clients.

Receiving a Collector Configuration Error: If you receive a single `ihConfigurationGetProperties[-2]` error in the `collector.LOG` file, the error most likely occurred as a result of the collector connecting and querying for changes in the tag database immediately, getting a timeout, and then immediately querying again and succeeding.

User API Programs Not Freeing Up Memory: User API Programs built with anything other than Visual Studio .NET should be modified to call `ihuFreePtr()` to free any memory pointers returned by the User API. Do not free these pointers using `free()` in your application or you can risk memory corruption. User API does not support Unicode programming.

Maximum Buffer Memory Size: You can specify the maximum memory buffer size that an archiver queue can take. By default, memory buffer size is 100MB.

Troubleshooting Remote Collector Management Issues

Remote Collector Management does not work

Issue: 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. This is applicable to the iFIX Alarms and Events collector as well.

Workaround: 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.

The ServiceName Registry Key is not Updated

Issue: When you attempt to manage collectors, sometimes, an error message appears in the `CollectorManager.shw` file.

Error message: Below are collectors in the registry without a service name. The String Registry value 'ServiceName' exists, but is blank. Collector Manager will not try to determine what the service name is. This will need to be manually configured.

Cause: When Remote Collector Management is started for the first time, the collector that you want to manage is not running. When this happens, the ServiceName registry key is not updated.

Workaround:

1. Stop the Remote Collector Management service.
2. Start the collector.
3. Start the Remote Collector Management service.

The ServiceName Registry key is Updated Incorrectly

Workaround:

1. Stop the Remote Collector Management service.
2. Access the registry folder of the collector.
3. Delete the ServiceName key.
4. Start the collector.

5. Start the Remote Collector Management service.
6. Access the .shw file to verify that the ServiceName key has been updated.

Troubleshooting a Historian Cluster

You may find these issues with clusters:

- If a Historian resource does not go online initially, make sure you have cluster feature included in your license.
- If a Historian resource runs for a long period of time and then has an unexpected failover, debug the log messages of the Data Archiver and the Clusters before taking appropriate actions.

Troubleshooting iFIX and Historian

Running iFIX as a Service with iFIX Workspace Listed in the SCU Task List: Prior to iFIX 5.1, if you have configured iFIX to run as a service, you should not have WORKSPACE.EXE listed as a configured task in the Task Configuration window of the SCU. If WORKSPACE.EXE is listed as a configured task, it may lead to unpredictable results. For example, if you are also running Historian, no servers will appear in the Server Name field of the Configure the Historian Server window and you will not be able to browse Historian tags in the iFIX Expression Editor.

To rectify this, remove WORKSPACE.EXE from the list of configured tasks in the SCU.

iFIX WorkSpace delay when remote session is lost: If the connection between iFIX and a remote Historian session is lost, you may experience a 90 second delay in the iFIX Workspace Configuration environment, chart, or Expression Builder when accessing a pen associated with that Historian session.

In the Run Time Environment, all pens in a chart disappear for 90 seconds when the session to a remote Historian session is lost, even if they are associated with a local Historian server.

Starting iFIX when a remote Historian session is unavailable: If you are using Historian with iFIX, the iFIX Workspace attempts to connect to the Historian Server when it starts up. If a remote Historian server is unavailable, it may take one minute or longer for iFIX Workspace to display for each unavailable server.

Accessing Mission Control when a remote Historian session is lost: If a remote Historian session is lost while you are accessing the **HTC** section of Mission Control in the iFIX Workspace, the **HTC** section may become unresponsive for a minute or longer.

Accessing tags in the iFIX chart after setting OPC "Collector to Made After Restart": If you add tags in Historian Administrator to a Server from an OPC Collector that has Configuration Changes set to Made After Collector Restart, you will be able to see those tags in the iFIX Expression Builder. You can add them to a chart, for example, but they have no collected data until you manually stop and restart the OPC Collector.

Collecting data in an iFIX chart with Time Assigned By Source: If you are retrieving data in an iFIX Chart from a Historian Server, have set the Time Assigned by field to Source, and have collectors running behind the Server time, the chart will display a flatline up to the current time of the local machine.

Note: You must set Time Assigned by field to Source if you have unsolicited tags getting data from an OPC Collector.

Synchronizing the time on iFIX SCADA Servers and View Clients: To ensure that acknowledgements are not lost or attributed to the wrong alarm, synchronize the clocks on SCADA servers and iFIX View Client machines. If the clocks are not synchronized, alarms generated on the SCADA nodes and acknowledged on the iFIX View Client nodes could have significantly different timestamps. You can synchronize the clocks using the NET TIME command. Refer to the Windows Help system for more information.

The *Historian REST API Reference* manual specifies port 8443 in examples and sample code. If you copy and paste the sample code from this Help manual, you must change this port number to your installed port.

If you have a previous install of Historian, and you have installed PHA/PKC 6.0/6.1, you will need to uninstall and then reinstall Historian.

Troubleshooting Collectors

Proxy Timeout Error While Adding a Collector Instance

When you attempt to add a collector, sometimes, a proxy error appears even if the error occurs because of an API timeout. To view the actual cause of the error:

1. Access the `historian-httpd.conf` file located at `C:\Program Files\GE \Operations Hub\httpd\conf\app-specific.d`.
2. Increase the timeout value (for example, 250).
3. Restart the GE Historian Tomcat Server and the GE Operations Hub Httpd Reverse Proxy services.

Troubleshooting the OPC UA Data Access (DA) Collector

The OPC UA Data Access (DA) collector gathers and collects data from any OPC UA 1.0-compliant OPC UA DA server. The OPC UA DA collector automatically determines the capability of the OPC UA DA server to which it is connected, and supports the appropriate features based on this information.

Troubleshooting the OPC Classic HDA collector

The OPC Classic HDA collector collects data from any OPC HDA 1.2 -compliant OPC Classic HDA server. The OPC Classic HDA server automatically determines the capability of the OPC HDA Server to which it is connected, and supports the appropriate features based on this information.

Note: GE assumes no responsibility for the ability for the OPC Classic HDA collector to connect to specific HDA servers.

Troubleshooting Historian 7.2 with PHA/PKC 6.0

Installing PHA/PKC on a machine that has Historian 7.0 or greater will fail due to a port conflict issue. Both applications use the same default port 8443. You must follow the recommended order of install below to avoid this error. Installing Historian after PHA/PKC on the same machine will not fail as Historian has the ability to detect used port and will configure an unused port.

The recommended order of install is:

1. Install PHA/PKC 6.0/6.1.
2. Install Historian 7.2.

Note: If you are performing an install on a system with no prior install of PHA/PKC or Historian, you must first install the Historian Alarms and Eventss Archiver and the Historian Client Tools from the Historian install media, and then you can install PHA or PKC, and then finally the rest of Historian.

Troubleshooting Steps for Web-based Clients

Issue	Workaround
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.	Try one of the following options: • 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.
Even after installing Web-based Clients, you cannot access Configuration Hub.	Start the GE Operations Hub Httpd Reverse Proxy and the Data Archiver services.

Issue	Workaround
When you upgrade to Historian 9.1, 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.	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 UAA PostgreSQL Database • GE Operations Hub UAA Tomcat Web Server • GE UAA External IdP Configuration Service • GE Security App Service
The **WhereTo** page is displayed when you logout and login to the Web Admin console without closing tab or browser.	Logout and close the tab or browser and reopen it.
Internet Explorer is not supported for the latest Web-based Clients. There may be some formatting issues in the text.	Use Google Chrome for better viewing experience.
This Site Can't be reached issue is encountered.	User should start the **GE Operations Hub Httpd Reverse Proxy** Service
Unable to login due to some certificate issues.	Follow the steps provided under Connecting to External UAA section.
After logging in to Web-based Clients, the Web-based Clients are not connected successfully to the Historian server.	• Ensure that the **Enforce Strict Client Authentication** and **Enforce Strict Collector Authentication** options are disabled in the **Data Stores Security** section in Historian Administrator. • Make sure you have given a valid UAA URL while installing the Historian Server.
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 Historian UAA, a message appears, stating that the credentials are incorrect.	Use the Web based configuration tool to point to a different Configuration Hub and UAA instance. By default, this tool is located in the following folder: `C:\Program Files\GE Digital\Historian Config`
If you install iFIX on a machine that has Historian Web-based Clients, the reverse proxy service stops working.	Restart the reverse proxy service - GE Operations Hub Httpd Reverse Proxy.

Troubleshooting UAA Issues

Issue	Workaround
You cannot access the UAA LDAP tool in a browser.	Enter http://localhost:3010/ in the browser, and then access the UAA LDAP tool.
If the PFX file that you want to use with Historian does not contain a full-chained certificate, a while label error message appears.	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 Configuration Hub Issues

Unable to Access External Configuration Hub if Public Https Port is Different

Issue: During Web-based Clients installation, if you provide an external UAA and Configuration Hub, and if the public https port numbers of these two machines do not match, you cannot access the external Configuration Hub from the current machine.

For example, suppose you have installed Web-based Clients on machine A, which points to the UAA and Configuration Hub installed on machine B. If the public https port numbers of machines A and B do not match, you cannot access Configuration Hub of machine B from machine A (although you can access it locally from machine B).

Workaround: Perform the following steps on the machine on which you have installed Configuration Hub (machine B):

1. Access the following folder: `C:\Program Files (x86)\GE\ConfigurationHub\Web\conf\confighub`
2. Access the file that contains the details of the machine from which you want to access external Configuration Hub (machine A). The file name begins with the host name of machine A.
3. In the line that contains the details of the UAA server (for example, proxy_pass https://machine_B.Domain.com:Port/uaa/), change the port number to match the public https port number of machine B.
4. Save and close the file.
5. Restart the following services:
   - ConfigHubContainerService
   - ConfigHubNGINXService

- ConfigHubStorageService

Issue: You can install Configuration Hub only in the C drive

Workaround:

1. Create Configuration Hub server certificates.
2. Start the ConfigHubNGINXService service.
3. Using the Web Based Clients Configuration tool *(page 103)*, provide the UAA and Configuration Hub details, test the connection, and select **Resgister** to re-register the Historian plugin with Configuration Hub.

Issue: Error Occurs When Historian Plugin is Registered with an External Configuration Hub

Description: If you install Configuration Hub using iFIX, then install Web-based Clients on another machine with local UAA, and then register the Historian plugin with Configuration Hub, testing the connection to Configuration Hub fails. Even after you add the IP addresses of both the machines to the hosts file, the issue is not resolved.

Error Message: Error while getting token in ConfigAuth App

Workaround: Register the Historian plugin *(page 103)* on the machine on which you have installed Web-based Clients, install the UAA certificate *(page 42)*, and then restart the browser.

Issue: Cannot Access the Collectors Section or Add a Collector Instance

Possible cause - user credentials not provided while installing collectors or Remote Collector Manager: While installing collectors and the Historian server on the same machine, if strict collector authentication is enabled, providing the user credentials is mandatory. Otherwise, an error occurs when you access the list of collectors or add a collector instance using Configuration Hub or the RemoteCollectorConfigurator utility.

To fix this issue, disable the strict collector authentication using Historian Administrator, and then restart the Historian Remote Collector Management Agent service.

Issue: Cannot Access or Add a System in Configuration Hub

Possible Causes:

- **User does not have security privileges:** During installation of the Historian server, if you have allowed the installer to create security groups, you must create a user with the name in the following format: <UAA host name>.admin. Verify that this user has been created and added to the ihSecurityAdmins group.

If the UAA 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 UAA user, and then create the corresponding Windows user, using the uaa_config_tool utility:

1. Access the `uaa_config_tool` utility. By default, it is located at `C:\Program Files\GE Digital\Historian Config`.
2. Run the following command: `uaa_config_tool add_user -u <username> -p <password> -s <the client secret you provided while installing the Historian server> -c`

   Example: `uaa_config_tool add_user -u adminuser -p Password123 -s pwd@123 -c`

- **Incorrect UAA details:** You must provide the host name of the UAA server while installing the Historian server. In the `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\iHistorian\SecurityProviders\OAuth2` registry path, verify that the URI value is in the following format: `https://<UAA host name>:<port number>/uaa/check_token`.

  If needed, modify the value, and then restart the Data Archiver service.

Issue: Error Appears When Creating a Collector Instance

Description: When you add a collector instance, the following error message appears: `The server encountered an error processing the request. Please try again.` The collector instance is added successfully, but it does not appear in the **Collectors** section.

Possible causes: When you add a collector instance, the collector service is started and stopped so that it is connected to the Historian server. The collector then appears in the table in the **Collectors** section. Sometimes, however, the collector service does not respond to these commands on time, resulting in the error message. If you attempt to add the same collector instance again, a message appears, stating that it exists.

Workaround: Select **Cancel**, and refresh the **Collectors** section. If the collector instance still does not appear, access the collector machine, and start the collector manually.