



Proficiency Historian 2022

Quick Installation Guide –
Configuration Hub Plugin for Historian

Proprietary Notice

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

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

© 2022, General Electric Company. All rights reserved.

Trademark Notices

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

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

All other trademarks are the property of their respective owners.

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

doc@ge.com

Install the Historian Server Using the Installer

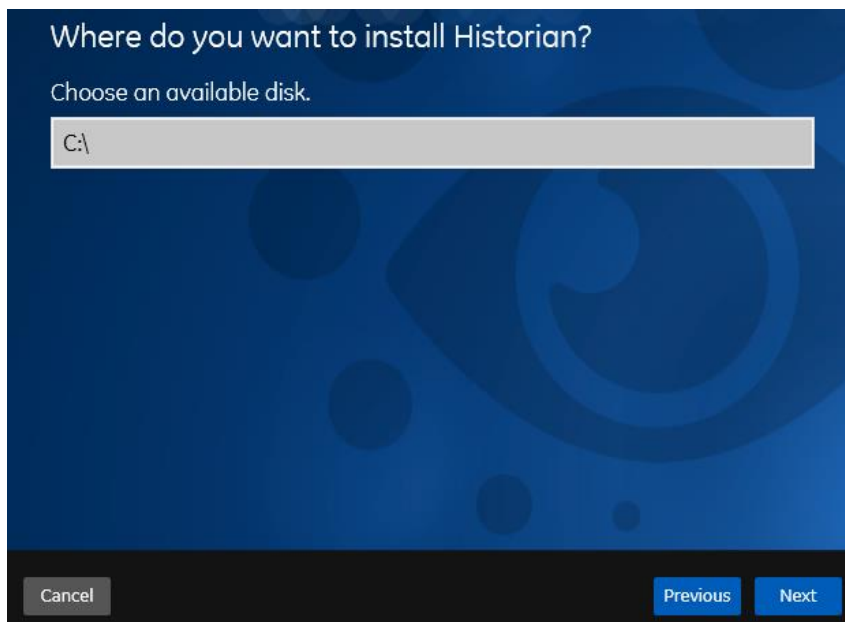
Before You Begin

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

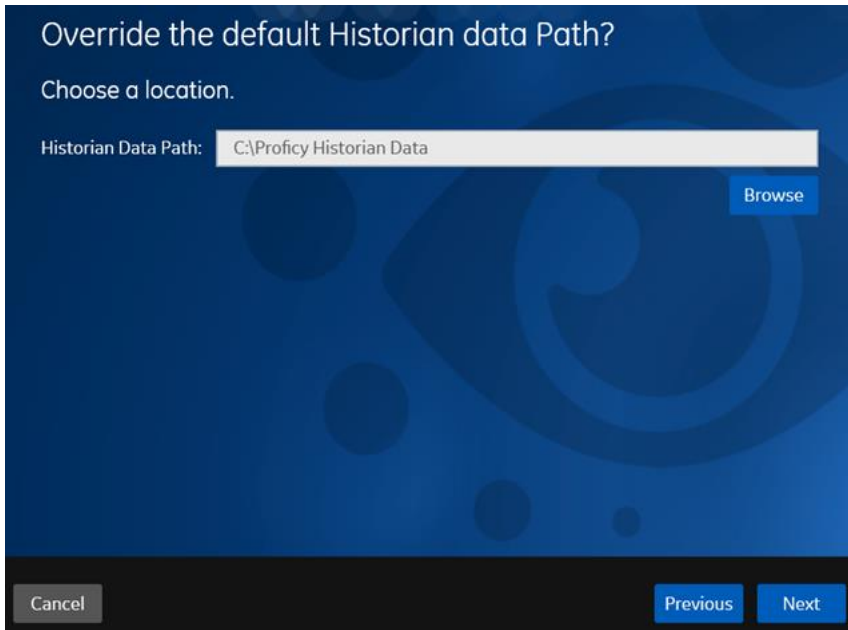
This topic describes how to install the Historian server using the installer.

Procedure

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

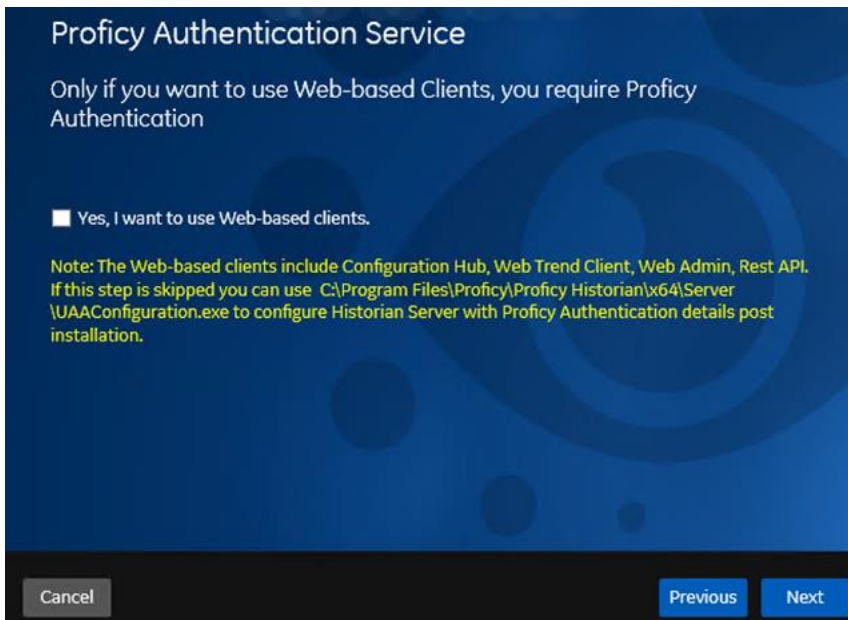


6. If needed, change the default installation drive of the Historian server, and then select **Next**.
The **Override the default Historian data Path?** page appears.



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

Only if you want to use Web-based Clients (such as Configuration Hub, Trend Client, the Web Admin console, and REST APIs), you need Proficy Authentication. Otherwise, you can skip this step. If you use Web-based Clients, Proficy Authentication is required for user authentication. It provides identity-based security for applications and APIs. It supports open standards for authentication and authorization, including OAuth2.



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

Field	Description
Proficy Authentication server name	Enter the name of the machine on which the Proficy Authentication server is installed. If the machine uses a fully qualified domain name (FQDN), provide the FQDN. By default, the local hostname is considered.

Field	Description
Public https port	Enter the port number used by the Proficy Authentication service. The default value is 443. Ensure that this port number matches the one on the TCP Port Assignments page during Web-based Clients installation.

NOTE:

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

9. Select **Next**.

The **Historian Security Groups** page appears.

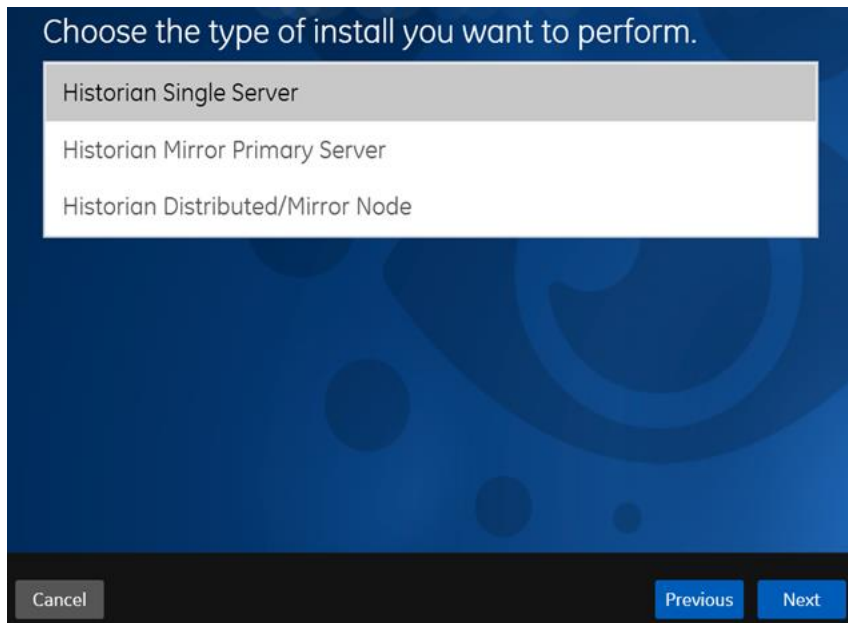
Using Historian security groups provides an added layer of control over access to your Historian system.

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



10. If you want the installer to create Historian security groups, select the corresponding check box, and then select **Next**.

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



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

The **Ready to Install** page appears.

12. Select **Install**.

The installation begins.

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

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

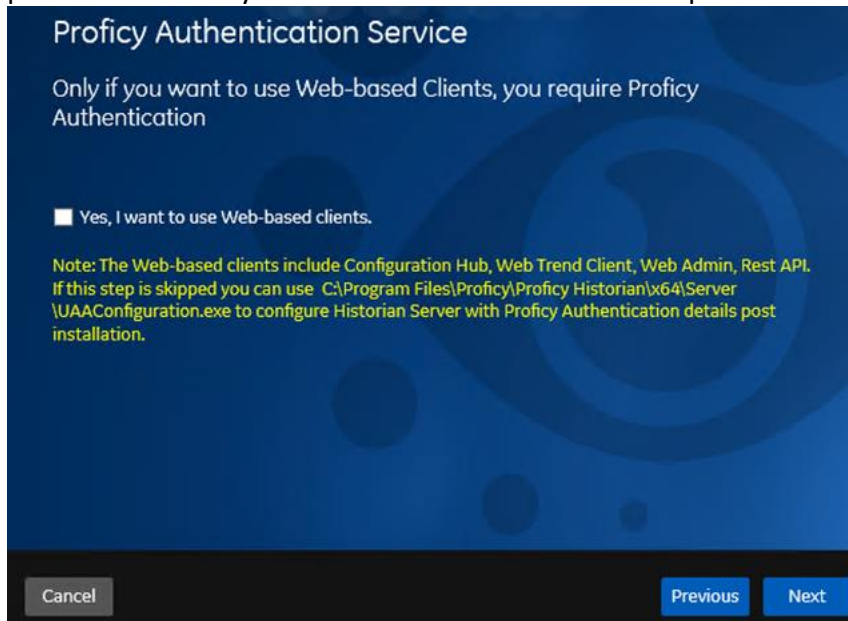
In addition, the following components are installed:

- **The RemoteCollectorConfigurator utility:** A command-line tool, which allows you to manage collectors remotely. By default, it is located in the C:\Program Files\GE Digital\NonWebCollectorInstantiationTool folder.
- **The Proficy Authentication Configuration tool:** A utility that allows you to specify the Proficy Authentication server details to match with the Proficy Authentication server used by Web-based Clients. By default, it is located in the C:\Program Files\Proficy\Proficy Historian\x64\Server folder.

Install Web-Based Clients Using the Installer

Before You Begin

1. Install the Historian Server Using the Installer. During the installation, in the Proficy Authentication page, select the Yes, I want to use Web-based Clients check box, and provide the Proficy Authentication server name and port number.

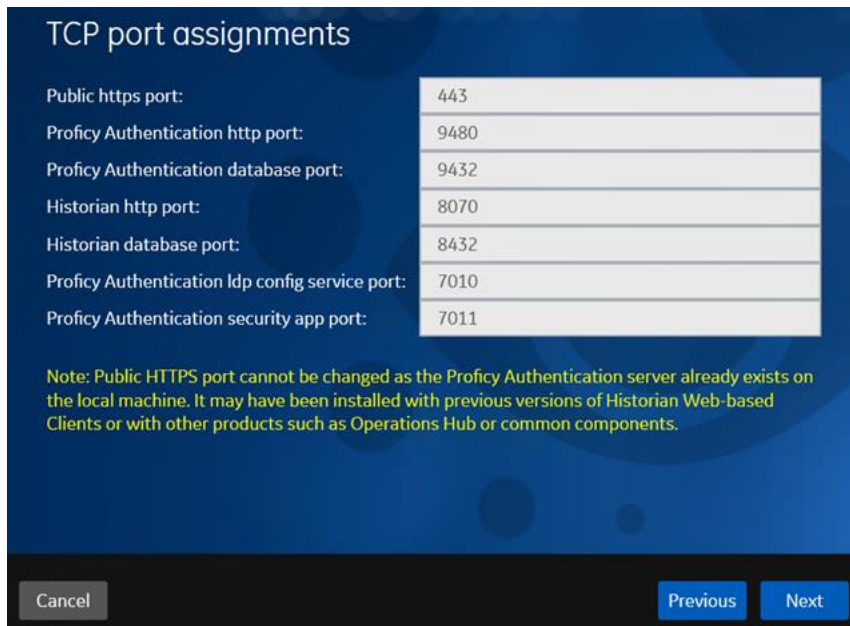


2. If you want to use Web-based Clients in a cluster environment, ensure that your network is enabled for multicast traffic, and set up high availability on each node in the cluster.

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

Procedure

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.

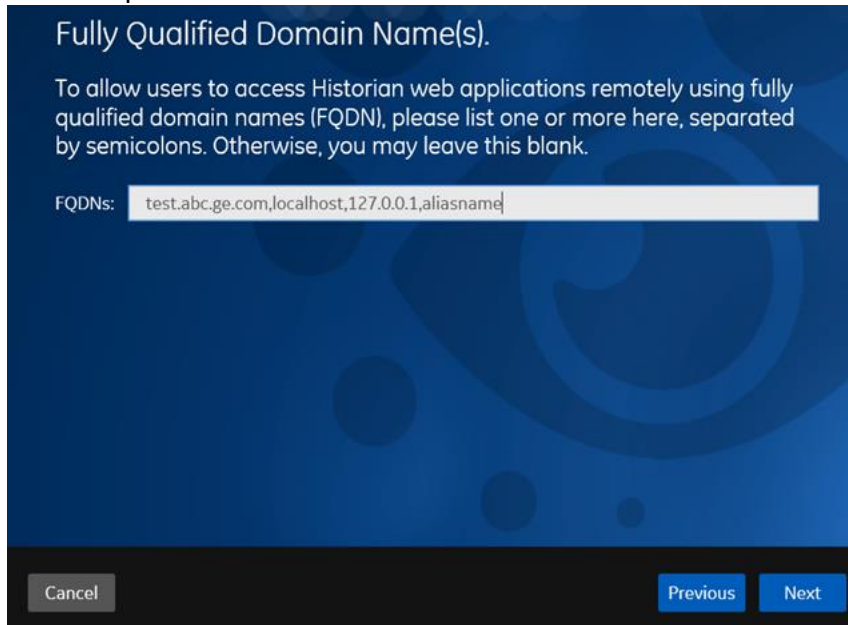


5. As needed, change the values for TCP port assignments as described in the following table, and then select **Next**.

Field	Description
Public https port	Port for https protocol communication used by Web-based Clients (through a firewall). The default value is 443. Ensure that this port number matches the one you specify while installing the Historian server. In addition: <ul style="list-style-type: none"> If you will install Operations Hub later on the same machine, the value that you provide in this field is populated while installing Operations Hub. If you have already installed Operations Hub on the same machine, this field is disabled and populated with the value you have provided while installing Operations Hub.
Proficy Authentication http port	Port for http protocol communication used by the Proficy Authentication service. The default value is 9480.
Proficy Authentication database port	Port for the Proficy Authentication database. The default value is 9432.
Historian http port	Port for the http protocol communication used by Web-based Clients. The default value is 8070.
Historian database port	Port for the PostgreSQL Historian database. The default value is 8432.
Proficy Authentication Idp config service port	Port for the Configuration Hub identity provider service. The default value is 7010.
Proficy Authentication security app port	Port for the Proficy Authentication Configuration tool. The default value is 7011.

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

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



6. In the **FQDNs** field, enter the fully qualified domain names, and then select **Next**. This enables you to access Historian web applications remotely. You can use it to access the Web Admin console using alias names. Enter the values separated by commas.

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

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

- `https:// Test.abc.ge.com /historian-visualization/hwa`
- `https:// 127.0.0.1 /historian-visualization/hwa`
- `https:// aliasName /historian-visualization/hwa`
- `https:// localhost /historian-visualization/hwa`

IMPORTANT:

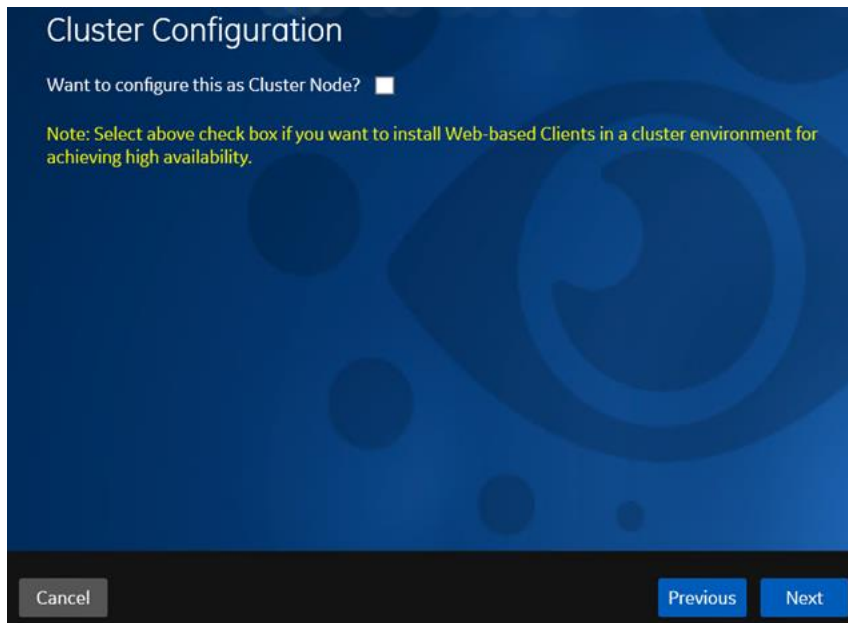
- Do not enter a space between the values.
- You must add the IP address and alias name in the hosts file located at `C:\Windows\System32\drivers\etc`. The IP address that you add must be a static or fixed IP address.

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

Example: `1.2.3.4 myservername`

- FQDN is not supported for Configuration Hub.

The **Cluster Configuration** page appears.



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

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

Field	Description
Historian Database Folder	Provide the database folder in the shared drive that you have created. The default value is <i>C:\ProgramData\GE\OperationsHub</i> . You must change this value.
Cluster FQDN	Enter the client access point of the role for which you have added the resources while setting up high availability.
Multicast Address	If needed, modify the common IP address that all the nodes in the cluster can use. Enter a value between 224.0.0.0 and 239.255.255.255 (or a hostname whose IP address falls in this range). The default value is 228.0.0.4.
Historian Cluster Membership Port	If needed, modify the common port number that all the nodes in the cluster can use. The default value is 45564. This port number, in conjunction with the multicast address, is used to create the cluster.
Historian Cluster Receiver Port	If needed, modify the multicast port number that you want to use for incoming Historian data. The default value is 4000.

8. Select **Next**.

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

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

The admin client secret must satisfy the following conditions:

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

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

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

10. Alternatively, if you want to use an external Proficy Authentication service (that is, a Proficy Authentication instance already installed by an external application such as Operations Hub):
- a. Select the **Use External Proficy Authentication** check box.
The fields for the external Proficy Authentication service appear.

b. Enter values as described in the following table.

Field	Description
Proficy Authentication Base URL	Enter the URL of the external Proficy Authentication server in the following format: https://<Proficy Authentication server name>:<port number>, where <Proficy Authentication server name> is the FQDN or hostname of the machine on which Proficy Authentication 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 Proficy Authentication. The default value is admin.
Admin Client Secret	Enter the client secret that you provided while installing the external Proficy Authentication.

c. Select **Test Connection**.

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

11. Select **Next**.

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

Configuration Hub allows you to add and manage a collector instance remotely.

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

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

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

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

Field	Description
Install Location	If needed, modify the installation folder for Configuration Hub. IMPORTANT: You can install Configuration Hub only in the C drive.
Plugin Name	If needed, modify the name of the Configuration Hub plugin for Historian. The default value is in the following format: Historian_<host name>. If, however, you are installing Web-based Clients in a cluster environment, the default value is Historian_<cluster name>. You can modify this value, but provide the same value for all the nodes in the cluster.
Server Port	If needed, modify the port number that you want to use for the web server (NGINX). The default value is 5000. If you want to install Web-based Clients in a cluster environment, provide the same value for all the nodes in the cluster.
Container Port	If needed, modify the port number for the Configuration Hub container. The default value is 4890.

Field	Description
Client ID	Enter the username to connect to Configuration Hub. The default value is admin. The value that you enter can contain: <ul style="list-style-type: none"> All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_0123456789) The following special characters: ><:~!@#%&^&*?
Client Secret	Enter the password to connect to Configuration Hub. The value that you enter can contain: <ul style="list-style-type: none"> Must contain at least eight characters. All English alphanumeric characters (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_0123456789) The following special characters: ><:~!@#%&^&*?
Re-enter Secret	Re-enter the password to connect to Configuration Hub.

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

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

The fields for external Configuration Hub appear.

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

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

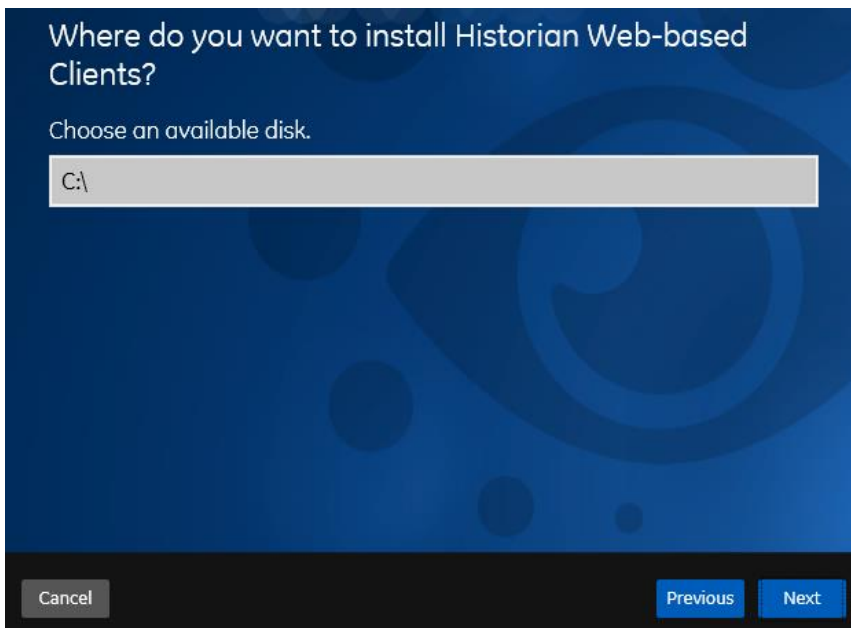
Field	Description
Client ID	If needed, modify the username to connect to Configuration Hub. The default value is admin.
Client Secret	Enter the password to connect to Configuration Hub.

- c. Select **Test Connection**.

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

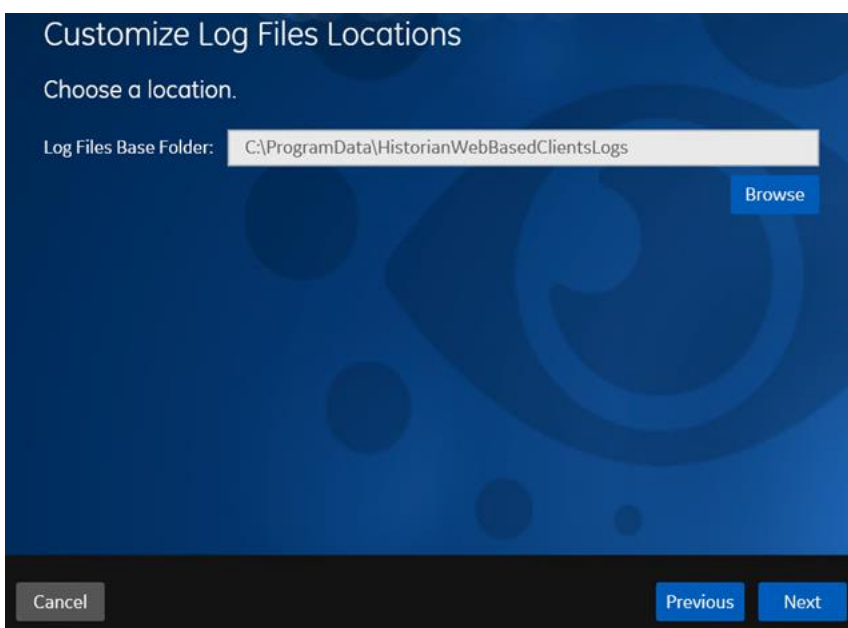
14. Select **Next**.

The default installation drive appears.



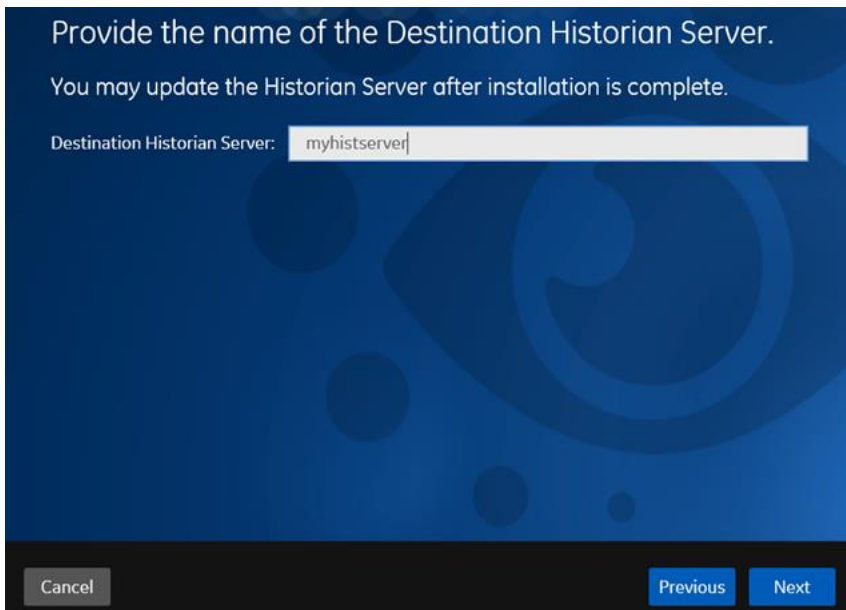
15. If needed, change the installation drive for Web-based Clients, and then select **Next**.

The log files location page appears.



16. If needed, change the location for log files, and then select **Next**.

The destination Historian server page appears.



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

NOTE:

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

18. Select **Next**.

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

19. Select **Install**.

The Web-based Clients installation begins.

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

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

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

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

Install Collectors Using the Installer

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

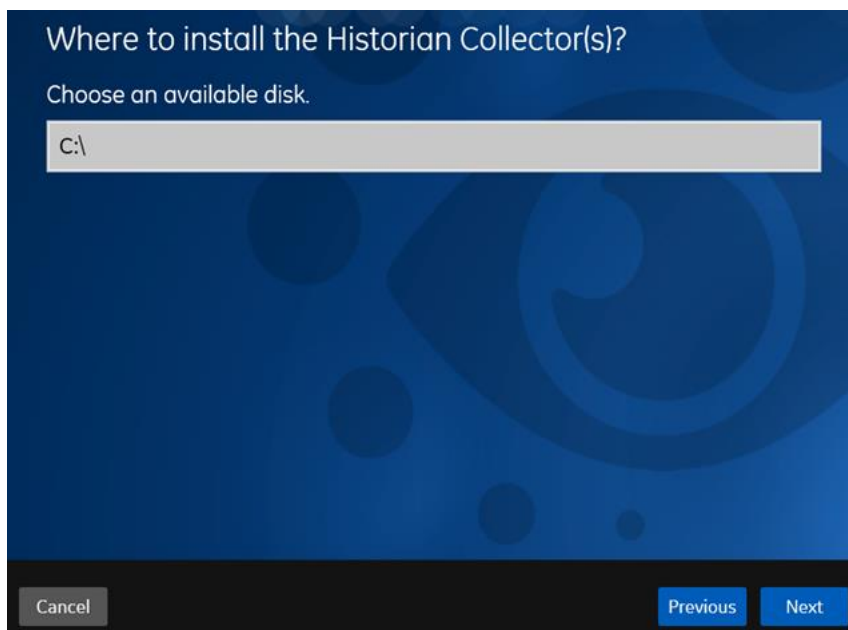
- **Executable files:** These files are required to add a collector instance.
- **Instances of the following collectors:**
 - The iFIX collector
 - The iFIX Alarms & Events collector
 - The OPC Classic Data Access collector for CIMPLICITY
 - The OPC Classic Alarms and Events collector for CIMPLICITY

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

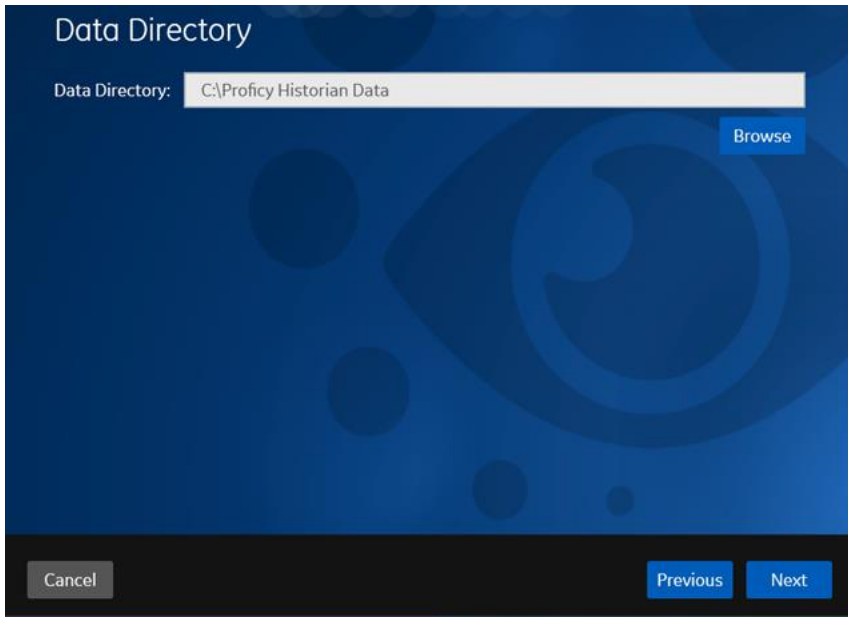
- **The Remote Collector Management agent:** Provides the ability to manage collectors remotely.

Procedure

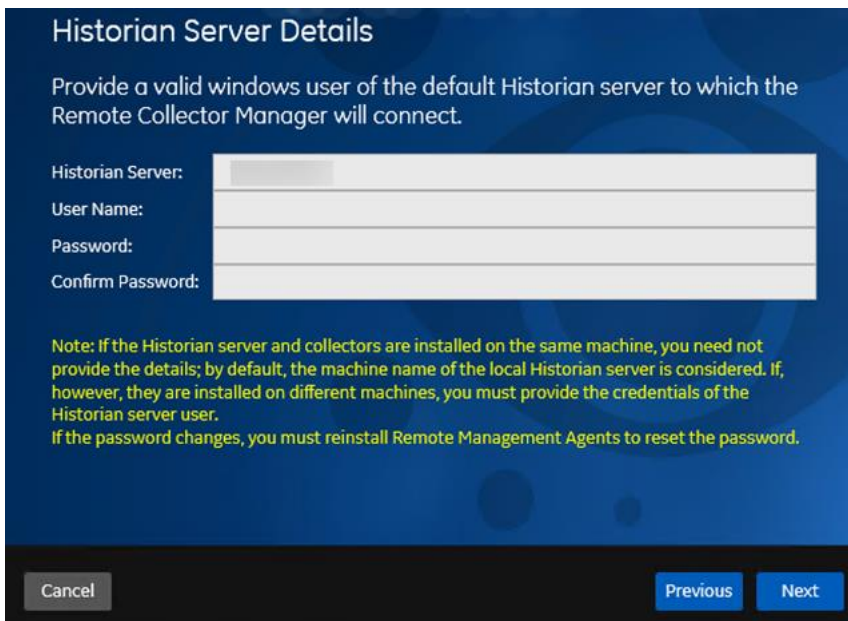
1. Run the *InstallLauncher.exe* file.
2. Select **Install Collectors**.
The welcome page appears.
3. Select **Next**.
The license agreement appears.
4. Select the **Accept** check box, and then select **Next**.
The default installation drive appears.



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



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



7. Provide the credentials of the Windows user account of the destination Historian server to which you want Remote Management Agent to connect. These details are required for Remote Collector Manager to connect to Historian to manage the collectors remotely. If are installing collectors on same machine as the Historian server, and if strict collector authentication is disabled, you need not provide these details; by default, the machine name of the local Historian server is considered. If, however, they are installed on different machines, or if strict collector authentication is enabled, you must provide the credentials of the Historian server user.
8. Select **Next**. A message appears, stating that you are ready to install collectors.
9. Select **Install**. The installation begins.

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

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

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

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

Perform Post-Installation Tasks

1. If you do not want strict authentication, disable the Enforce Strict Client Authentication and Enforce Strict Collector Authentication options under Historian Administrator > Data Stores > Security.
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 ihSecurity Admins group. This user will log in to Web-based Clients.

Alternatively, you can create Proficy Authentication users in an external Proficy Authentication and map their security groups. For information, refer to About Proficy Authentication Groups.

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

3. Ensure that the Windows user that you have specified while installing collectors is added to the iH Security Admins and iH Collector Admins groups.
4. Enable trust for a client certificate for Configuration Hub.
5. Enable trust for a self-signed certificate on Chrome.
6. Import an issuer certificate.

You are now ready to use Configuration Hub.