GE VERNOVA

PROFICY® SOFTWARE & SERVICES

ORCHESTRATION HUB

Secure Deployment Guide

GE VERNOVA

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

Trademark Notices
"VERNOVA" is a registered trademark of GE Vernova. "GE VERNOVA" is a registered trademark of GE Aerospace exclusively licensed to GE Vernova. The terms "GE" and the GE Monogram are trademarks of GE Aerospace and are used with permission.

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

All other trademarks are the property of their respective owners.

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

Contents

About this Guide

The Orchestration Hub Secure Deployment Guide is intended for process control engineers, integrators, IT professionals, and developers responsible for deploying and configuring Proficy Orchestration Hub.

What Is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- Confidentiality: Ensure only the people you want to see information can see it.
- Integrity: Ensure the data is what it is supposed to be.
- Availability: Ensure the system or data is available for use.

GE recognizes the importance of building and deploying software with these concepts in mind and encourages customers to take appropriate care in securing their GE products and solutions.

Defense in Depth

Defense in Depth is the concept of using multiple layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability but would need to exploit vulnerabilities in each layer of defense that protects an asset.

If a system is on a network protected by a firewall, for example, an attacker needs to circumvent only the firewall to gain unauthorized access. However, if there is an additional layer of defense such as a username/password authentication requirement, an attacker now needs to find a way to circumvent the firewall and the username/password authentication.

More Information About Security

For more information on security, including GE security advisories and security patch notifications, please visit our website at
https://digitalsupport.ge.com/communities/CC_Home

About Orchestration Hub

Proficy Orchestration Hub enables manufacturing customers to stay in synch with the constant updates to product manufacturing information. The solution provides out-of-the-box tools to unify product manufacturing information from disparate data systems like ERP and PLM, transforms and organizes this raw business-oriented information into production-ready formats like recipes and specifications, and orchestrates the information across the customer's factory floor systems at a single site or multiple facilities.

Orchestration Hub software is for a platform that allows you to integrate L4 systems like ERP and PLM, with L2 software like Plant Applications, iFIX, CIMPLICITY, and Batch Execution, so that you can synchronize the latest / updated manufacturing data (classified as master data) available in L4 systems with that in L2 systems. The approval process / workflow is seen as the key tenant in the data synchronization process.

Restricting Access to Internet Protocols

Orchestration Hub leverages a Microsoft SQL database. Access to an end-user interface is provided through the Google Chrome browser.

This document gives recommendations to mitigate potential security threats associated with underlying applications leveraged by Orchestration Hub . Recommendations on securing user accounts, password, and ports are identified to mitigate potential security threats and restrict access to Internet Protocol (IPs).

For additional recommendations on restricting IPs and firewall configuration, consult with your local IT department and explore the best practices published by Microsoft.

Passwords

Setting passwords for accessing user accounts for Orchestration Hub and SQL Server is critical to a security strategy.

Setting Strong Passwords for Orchestration Hub User Accounts

Passwords should meet the standard password requirements.

Setting Strong Passwords for Orchestration Hub SQL Users

Passwords should meet the standard password requirements as mentioned in the Plant Applications documentation.

Default Passwords for Third Party Components in Web Client

While upgrading Plant Applications from the older version to the newer Web Client, you will be prompted for various user names and passwords. Some of these accounts were created automatically during the previous installation. For reference, those account credentials are as follows:

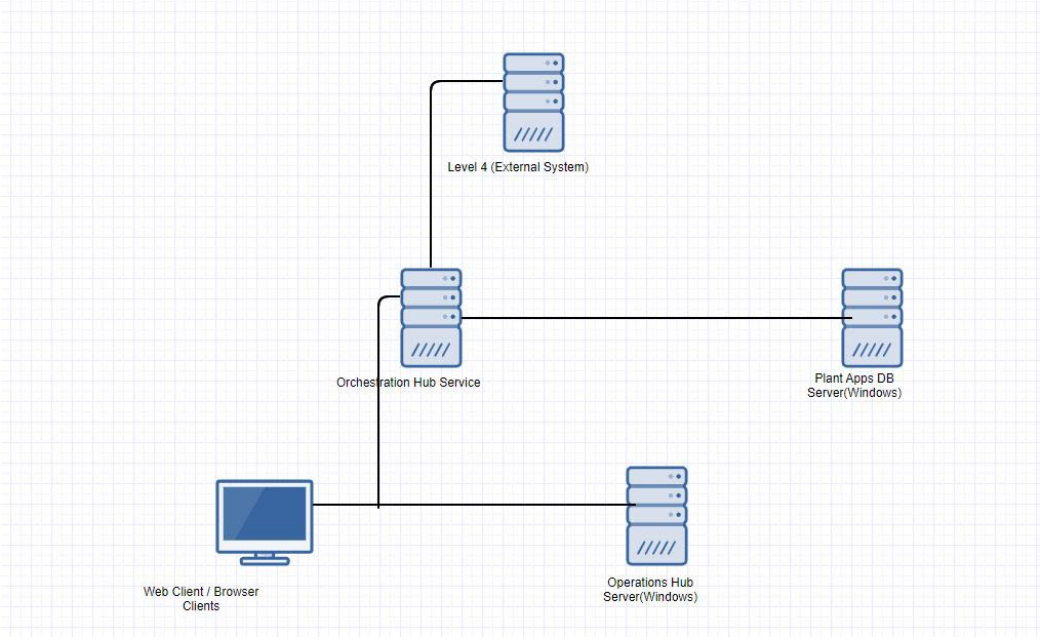
- Application Assembler / Operations Hub
    - Username: Administrator
    - Password: admin
- Denodo Credentials
    - Username: admin
    - Password: admin

As always, it is strongly recommended that default passwords be updated and managed according to the local IT best practices.

Deployment Architecture (Tomcat-based Plant Applications Web Client)

The recommended deployment architecture is as shown in the following figure.

Be aware that the numbers next to the server names suggest the order of installation of different software packages on their respective servers. It is recommended to follow the same order.



- ***Operations Hub port vs. Denodo Server Port***
  Operations Hub services use port '443' for https binding. Therefore, if you are running Denodo Server on the same node, please choose a different port – other than 443 – for the Denodo Server

The details of each of the servers in the above diagram and the pre-requisites on each of them are given below:

Server	Node Description	Pre-requisites
1	**Plant Apps DB Server** This is the Plant Applications' database server.	Microsoft SQL Server, as recommended by the Plant Applications core. **System Requirements**: As recommended in the *Plant Applications Installation Guide*. **Hardware**: As recommended in the *Plant Applications Installation Guide*.
2	**Operations Hub Server** This is the Operations Hub container running server. Starting with Plant Applications v8.1, the Web Client applications are hosted in the Operations Hub container.	**Operating System**: Windows Server 2016
3	**Orchestration Hub server** This is the server node you will choose to run the Tomcat-based installer.	**System Requirements**: Windows 2016 operating system and SQL Server 2016 **Hardware**:

		As recommended in the *Orchestration Hub Installation Guide*.
4	**Web Client Browser Clients** These are the browser-based clients for accessing the Web Client application.	Any node in the same network in which all the above servers are connected, with Google Chrome browser installed.
5	**External System**	Client Specific

Secure Certificate Management

Consider these recommendations to protect remote access certificates:

- **Tomcat Based Version of Plant Applications Web Client:**

  The Tomcat version of Orchestration Hub has multiple microservices. These services are available through a reverse proxy.

- **Operations Hub Server:**

  The Operations Hub Server's installer also installs self-signed certificate by default. Refer to the topic *Install the Certificate on your Clients* in the Operations Hub *Getting Started Guide*.

- **Denodo Server:** Is the third-party Data Virtualization platform.
- **Required Open TCP/IP Ports:**

  In the distributed system shown the deployment architecture, the TCP/IP communication is between:

  a) Orchestration Hub application is available at HTTPS port 9443.
  b) Orchestration Hub components (both UI and back-end services) use the below listed TCP/IP ports which should be blocked for the external traffic:

- '9999', '7777' and '8090'.
- The ports can be blocked from external traffic by manually setting the Windows firewall rules . Or, the same can be achieved by running the following command from the command prompt with Administrator privileges:

  C:\your\path\>*netsh advfirewall firewall add rule name="POInternalPorts" protocol=TCP dir=in localport=9999,7777,8090 action=block*

Backup and Maintenance

Many companies have local IT policies that are driven at least in part by regulatory agencies and compliance needs. We do offer the following recommendations in terms of system backup and maintenance if other policies do not apply:

- SQL databases are recommended to be updated weekly, with transaction logs backed up daily.
- If running in a virtual environment, export the virtual image prior to applying updates (GE, Microsoft, or other third party as well) and routinely export them monthly.

Additionally, we recommend remaining current with product SIMs and Service Packs to remain current in terms of security, performance, and functional improvements.

Antivirus Software

Antivirus software does not stop custom malware or new malware that is not yet discovered by antivirus vendors. It does, however, stop mass market malware that is the most common cause of cyber security incidents in control systems. Install antivirus software on every computer in the system, update the antivirus signatures, and run a full scan on the computers.

Getting Assistance

- GE Digital Support and Knowledge Base: https://digitalsupport.ge.com
- GE Digital product offering: https://www.ge.com/digital/products
- Comments about manuals or online help: doc@ge.com