Proficy Plant Applications 8.1

Secure Deployment Guide

Disclaimer of Warranties and Liability

The information contained in this manual is believed to be accurate and reliable. However, GE assumes no responsibilities for any errors, omissions or inaccuracies whatsoever. Without limiting the foregoing, GE disclaims any and all warranties, expressed or implied, including the warranty of merchantability and fitness for a particular purpose, with respect to the information contained in this manual and the equipment or software described herein. The entire risk as to the quality and performance of such information, equipment and software, is upon the buyer or user. GE shall not be liable for any damages, including special or consequential damages, arising out of the user of such information, equipment and software, even if GE has been advised in advance of the possibility of such damages. The user of the information contained in the manual and the software described herein is subject to the GE standard license agreement, which must be executed by the buyer or user before the use of such information, equipment or software.

Trademark Notices

* Indicates a trademark of General Electric Company and/or its subsidiaries.

All other brands or names are property of their respective owners.

All other product names and marks identified throughout this book are trademarks or registered trademarks of their respective companies. They are used throughout this book in editorial fashion only. No such use or the use of any trade name is intended to convey endorsement or affiliation.

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

doc@ge.com

Contents

About this Guide

The Proficy Plant Applications Secure Deployment Guide is intended for process control engineers, integrators, IT professionals, and developers responsible for deploying and configuring GE Digital's Proficy Plant Applications.

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 Proficy Plant Applications

Proficy Plant Applications is a unique software solution that digitizes the collective information being generated throughout your production facilities into a "virtual plant" for access where, when, and how you need it.

Proficy Plant Applications provides clear insight into your production to greatly improve operational effectiveness.

Restricting Access to Internet Protocols

Proficy Plant Applications 8.1 leverages a Microsoft SQL database and relies on communication with Proficy Workflow 2.6 SP1. Access to an end-user interface is provided through the Google Chrome browser. The Plant Applications Report (Web) Server is not supported as part of the solution.

This document gives recommendations to mitigate potential security threats associated with underlying applications leveraged by Plant Applications. 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.

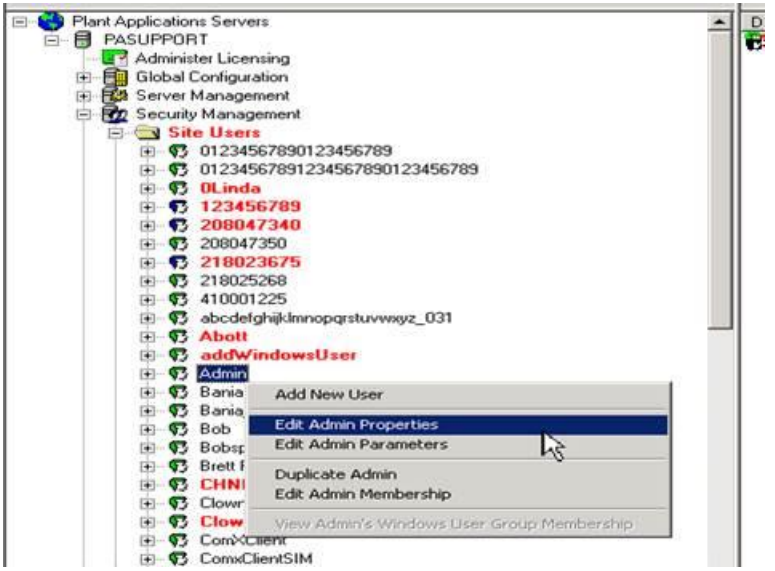
Passwords

Setting passwords for accessing user accounts for Proficy Plant Applications and SQL Server is critical to a security strategy.

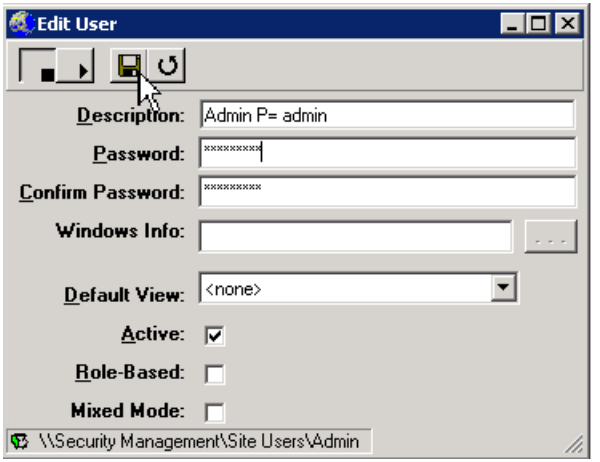
Setting Strong Passwords for Plant Applications User Accounts

When Plant Applications Server is installed, the users *ComXClient* and *Admin* are created with a default password. After installation, it is recommended to change the password to protect access to Plant Applications information. Proceed as follows:

1. Generate a strong password as dictated, for example, by your IT department.
2. Drill down to the **Admin User** under Security Management in the Plant Applications Administrator.
3. Right-click the Admin User, and select **Edit Admin Properties**.



4 Enter the new password and the confirmation, and then click the Disk icon to save the changes.



5 Repeat steps 1 to 4 to create a strong password for the *ComXClient* user account.

Setting Strong Passwords for Plant Applications SQL Users

When the Plant Applications Server is installed, three SQL user accounts are created to perform various tasks in Plant Applications ranging from software installations to data processing. Be aware that the table storing user names and passwords for accessing the SQL database is not encrypted.

- The SQL database user **ComXClient** is used by Plant Applications to execute procedures and add, update, or delete data from the database.
- The SQL database user **ProficyDBO** is used by Plant Applications to create, alter, or modify tables, stored procedures, functions, or views and install updates distributed in Software Improvement Modules (SIMS).
- The SQL account **ProficyConnect** is used by the Plant Applications LicenseMgr service. ProficyConnect has "execute" permissions for the spServer_CmnGetLicenseMgrInfo stored procedure. ProficyConnect provides no

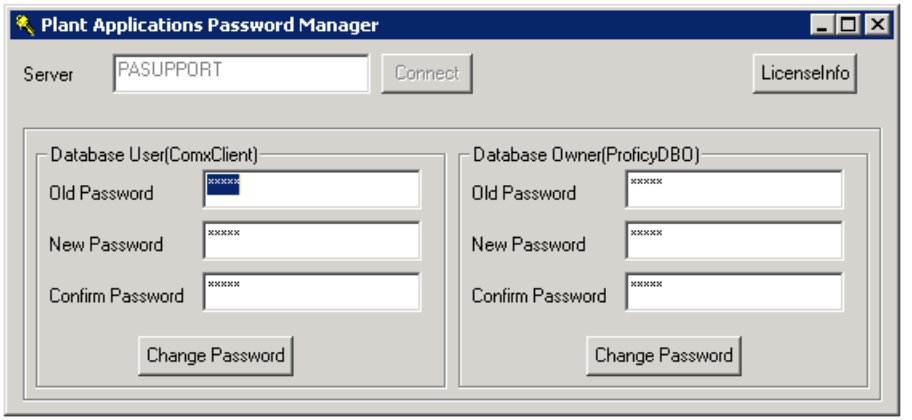
access to any critical information, nor should the password be changed using SQL Manager as this will break the Plant Applications installation.

IMPORTANT NOTE: *IT should distribute the* SQL ComXClient *and* ProficyDBO *accounts credentials. They are not intended for users.*

After installation, change the passwords for the other two users to protect access to SQL information. Use the Password Changer utility to modify the SQL passwords for the *ComXClient* and *ProficyDBO* users after installing Plant Applications, version 8.0 or later. Proceed as follows:

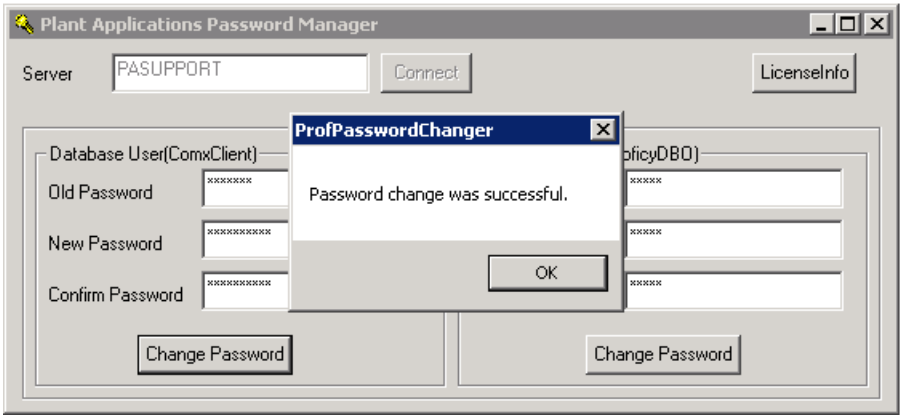
1. Generate strong passwords as dictated, for example, by your IT department.
2. Stop the following services:
   - Plant Applications ProficyMgr
   - Plant Applications LicenseMgr
   - Proficyserver, Proficysts, Proficypublisher (SOA services)
   - Common Licensing
3. Start the Password Changer utility at the Plant Applications Server under the **Support** folder. (The default location is: `<Drive>:\Program Files (x86)\Proficy\Proficy Server\Support`)

4 Enter the SQL server name for Plant Applications, and then click **Connect**.



5 Enter the old *ComXClient* password. Next, enter the desired password. Confirm the password, and click **Update**.

6 Enter the old *ProficyDBO* password. Next, enter the desired password. Confirm the password, and click **Update**.



7 Restart the Common Licensing service and other services that were stopped in step 2 for the changes to take effect.

Default Passwords for Third Party Components in Web Client

While upgrading the Plant Applications from Universal Client 7.0 SP5 to Web Client 8.1, you will be prompted for various usernames and passwords. Some of these accounts were created automatically during the Plant Applications Universal Client 7.0 SP5 install. For reference, those account credentials are as follows:

- Application Assembler / Operations Hub
  - Username: Administrator
  - Password: admin
- PostgreSQL
  - Username: postgres
  - Password: password

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

Reducing Permissions for SQL Server Accounts

Microsoft SQL Server is the database server used by Plant Applications and Proficy Connect. The SQL Server account that is used to install the Proficy Application Server is used to connect to the database after installation. Although you can install using the system administrator (*sa)* default account, it is recommended that you create a separate SQL account to perform the installation. After the installation, reduce the permissions to db_owner.

Reduce the permissions after installation for all SQL Server accounts including an SQL Server account for the Proficy Application Server:

- Reduce the SQL permission for an SQL Server account used to install Connect Workflow with SOADB access and no system-level rights as follows (for more information, refer to the KB16642 article posted at the GE Digital Support site):

  NOTE: *Creating a new SQL account to use for the installation instead of sa is recommended, and is a better approach than waiting until after the installation to create a user account. Naming the new account DBOwner is convenient for post-installation use. When you create a new account and use it for the installation, you will not need to use the Configure Database utility through Proficy Connect to reconfigure the database for a new user in order to assign DB Owner privileges.*

  1. Shut down the Proficy Server, ProficySTS, and ProficyPublisher services.
  2. Launch the ConfigureDatabase.exe utility from Workflow.
  3. Reduce the permissions for the SQL Server account.
  4. Restart the Proficy Server, ProficySTS, and ProficyPublisher services.

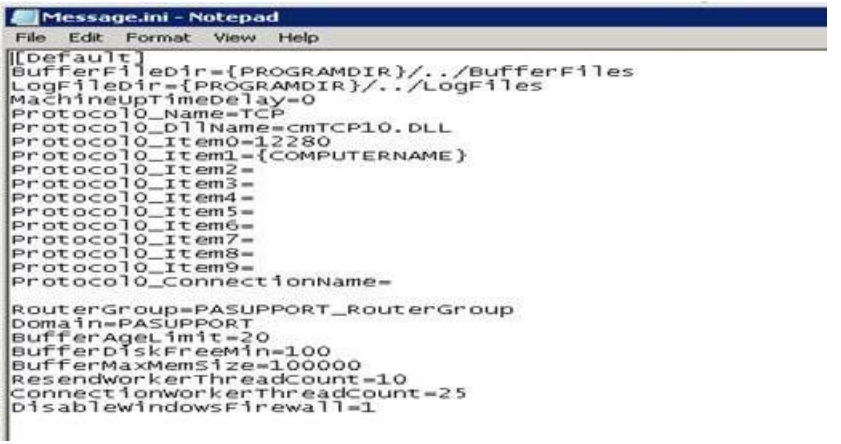
Changing Default Ports

Changing default communication ports may be advisable after installation to a port that is less commonly used or a known default, thus "hiding" the port.

Ports Specified in INI Files

Entries in associated INI configuration files are used by the Plant Applications services to facilitate communications. Four of the INI files reside in `\Program Files\GE Fanuc\Plant Applications\Messaging`. They include cmConfigMgr.ini, cmRtr.ini, Message.ini, and PlantAppsMessaging.ini. A fifth INI file resides in `\Program Files\GE Fanuc\Plant Applications\Server`. To modify the default ports in the INI files, make these changes:

1. Stop the PRProficyMgr and ProficyLicense services, as well as three SOA services: Proficyserver, Proficysts, and Proficypublisher.
2. If the site has remote RDS instances on historian boxes, stop them.
3. In each of the five INI files, modify the port number by changing the value for Protocol0_Item0.



4. Restart the services.

Ports Defined in the CXS_Service Table

"Listener" ports for PRGateway, PRProficyMgr, and PRRDS services are recorded in the CXS_service table. Follow these steps to change the ports:

1. Stop the PRGateway, PRProficyMgr, and PRRDS services.

2 From the SQL Manager, access the CXS_Service table as shown below.

	Service_Id	ApplicationName	Auto_Start	Auto_Stop	Domain	Is_Active	Listener_Address	Listener_Port	Monitor_Interval	Monitor_Service	Node_Name	Non_Responding_Kill_Script	NTService_Name	Proficy_Service_Name
1	14	NULL	1	1	NULL	1	PASUPPORT	12294	NULL	1	PASUPPORT	NULL	NULL	PRGateway
2	15	NULL	0	0	NULL	1	PASUPPORT	12293	NULL	0	PASUPPORT	NULL	NULL	PRProficyMgr
3	21	NULL	1	1	NULL	1	NULL	12299	NULL	1	PASUPPORT	NULL	NULL	PRRDS

3 Restart the services.

SQL Server Communication Port

By default, SQL server communicates on port 1433. Additionally, you can modify the port that SQL Server uses for communications after installation. For more information, refer to the Microsoft article KB823938, which outlines how to modify SQL TCP ports and how to troubleshoot communication issues after modifications. If the default port is modified, make a note of the change because the updated port information is needed when installing the Proficy Application Server and Plant Applications.

IMPORTANT NOTE: *Dynamic SQL Ports are not supported with Plant Applications Workflow.*

After installation, change the configuration files by following the steps in KB16620 at the GE Digital Support site.

NOTE: *The Knowledge Base article applies to Proficy Connect 2.5, as well as earlier versions of Workflow. If the user account is added after installation, use the Configure Database utility. Refer to the section, Reducing Permissions for SQL Server Accounts.*

User Management

Who are the Users in the System?

Users in the system can be created from Operations Hub as a UAA user, or imported from LDAP into the system as UAA user with a domain as origin. User can access application based on the group membership. User can be mapped to multiple groups. This mapping is done by assignment. Assignment includes roles, groups, and resources (Site, Department Line, Unit).

User Roles, Purpose and Privileges

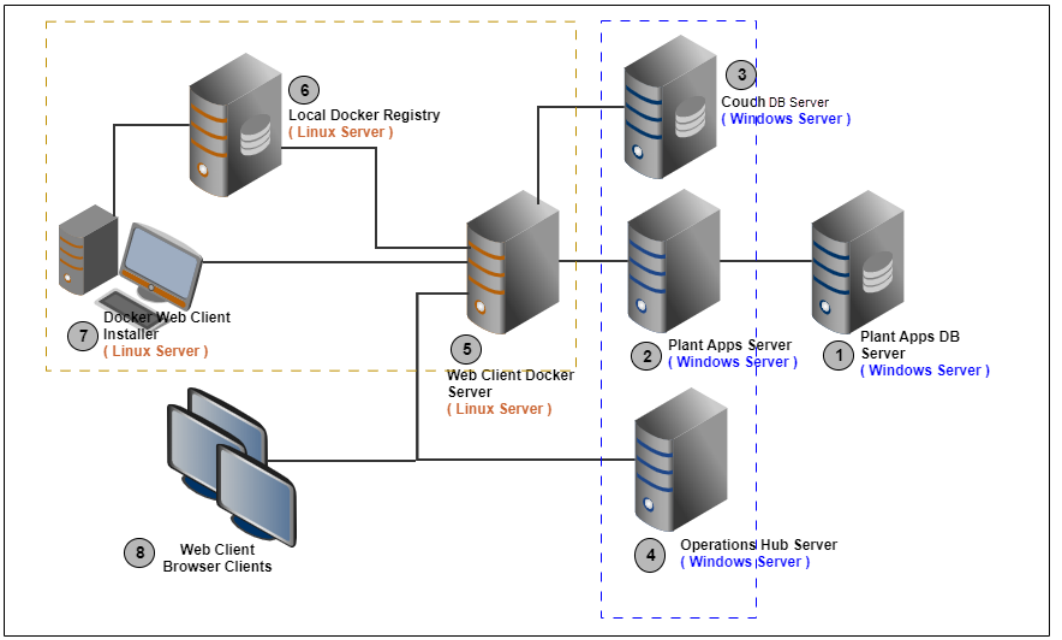
A role contains a set of permissions (privileges) required to perform various tasks. For example, Role1 may include permission to create a work order, update a work order, and so on.

A role should include in an assignment along with user group and resources.

An assignment enables you to assign a role and resources to groups. An assignment defines the tasks and the resources to which a group of users have access.

Deployment Architecture (Docker-based Plant Applications Web Client)

The recommended deployment architecture is as shown below:



NOTE: *Depending upon your project data storage and no. of concurrent clients requirements, you can choose to have servers (2), (3) and (4) as one Windows Server, and servers (5), (6) and (7) as one Linux Server, and have the required software packages installed. However, if you choose the minimum number of servers' configuration for the deployment, please take care of the below port conflicts.*

- ***Operations Hub port vs. Plant Applications Web Reports server port***
  Operations Hub services use port '443' for https binding. Therefore, if you are running Plant Applications' Web Reports on the same node, please choose a different port, other than 443, for the Web Reports server.
- ***Operations Hub IQP ports vs. CouchDB server port***
  If you are installing CouchDB and Operations Hub on the same node, there is one port conflict that should be taken care – in this scenario please edit the CouchDB's default.ini file to select '5987' instead of the default value of '5986' for the port under 'httpd' section.

Please be informed that in the above diagram the numbering of the servers was chosen to suggest the order of installation of different software packages on their respective servers. It is recommended to follow the same order.

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**: Windows 2016 operating system SQL Server 2016 **Hardware**: As recommended in the *Plant Applications Installation Guide*.

2	**Plant Apps Server** This is the server node for installing Plant Applications' server i.e. Plant Applications Core(1024), MessageBridge, RMQ – Plant Applications' core services server node.	As recommended in the *Plant Applications Installation Guide*.
3	**Couch DB Server** This is the back-end database server required for the Route Management application in Plant Applications Web Client. The purpose of this database is to store documents.	As per the official CouchDB Installation documentation: https://docs.couchdb.org/en/stable/install/windows.html
4	**Operations Hub Server** This is the Operations Hub container running server. Starting with Plant Applications v8.1, the Web Client applications will be hosted in the Operations Hub container.	**Operating System**: Windows Server 2016
5	**Web Client Docker Server** This is the server node on which you want to install or upgrade the Docker version of the Web Client.	**Node Hardware Requirements**: RAM – 32GB (minimum) Processor – 8 Core Free Disc Space – 100GB. **Operating System**:

		Linux distribution (Recommended – Ubuntu v20.x, RedHat v8.x) **Tools and Packages**: - Docker CE/EE v18.0 or greater - Docker Compose 1.25.x - Docker Swarm initialized with this node as Swarm Manager **Public Docker Images**: (by using docker pull command) - confluentinc/cp-kafka:5.1.2 - confluentinc/cp-zookeeper:5.1.2 - thomsch98/kafdrop:latest - confluentinc/cp-schema-registry:5.1.2 redis:5.0.7 - eventuateio/eventuate-tram-cdc-mysql-service:0.21.3.RELEASE - haproxy:1.8
6	**Local Docker Registry** This is the server node for storing / maintaining GE supplied docker images, so that the required images can be pulled onto any node in the network onto which you intend to install and run the Web Client Docker containers.	**Operating System**: Linux distribution (Recommended – Ubuntu, RedHat) **Tools and Packages**: - Docker CE/EE v18.0 or greater - Docker Registry is running with volume mounting done, and the registry service's URL is accessible from any node in the network.

7	**Installer** This is the server node you will choose to run the Ansible-based installer.	**Operating System**: Linux distribution (Recommended – Ubuntu 20.x, RedHat.8.x) **Tools and Packages**: - Ansible 2.9.x - Docker CE/EE v18.0 or greater - pip installed - freetds-dev - freetds-bin - pymssql==2.1.4
8	**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.

Secure Certificate Management

Consider these recommendations to protect remote access certificates:

- **Docker Version of Plant Applications Web Client:**

  The Docker version of Plant Applications has two docker service stacks. These two stacks are available through two different reverse proxies with SSL termination. The installer will create a self-signed SSL certificate and make it available to these reverse proxies through Docker secrets.

  Post-installation, if customers want to replace the self-signed certificate with a CA certificate, they can do so with the help of a utility which is part of the installer. The supported file format is ".pem", and the user needs to provide the location path of the .pem file. Once the Docker secret is created, the CA certificate file can be

removed to secure it. Refer to the *Replace the SSL Certificate of Web Client* in the *Web Client Installation Guide*.

- **Operations Hub Server:**

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

- **CouchDB Server:**

  We are shipping a utility to configure HTTPS and SSL certificate configuration for the Couch DB service. The utility places the required certificate file (.pem file) in a particular folder and the Couch DB service, which is a Windows service, reads the certificate and enables HTTPS. Refer to *Configuring Apache CouchDB Settings* in the *Web Client Installation Guide*.

- **Required Open TCP/IP Ports:**

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

  a) Plant Apps Server and Plant Apps DB Server – ODBC communication, generally standard port #1433.
  b) Web Client Server and Plant Apps DB Server – JDBC / JPA communication, generally standard port #3306.
  c) Web Client Server and Plant Apps Server – communication with RMQ on standard port #15672.

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 in the event that other policies do not apply:

- SQL databases are recommended to be updated weekly, with transaction logs backed up daily.

- The Web Client and the PA Core exchange some data over Kafka, it would be recommended to take the backup of Kafka data directory 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 in terms of the SIM's and Service Packs for the product 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 Plant Applications 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