GE VERNOVA

DIGITAL

PROFICY OPERATIONS HUB

Secure Deployment Guide

GE VERNOVA

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.

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

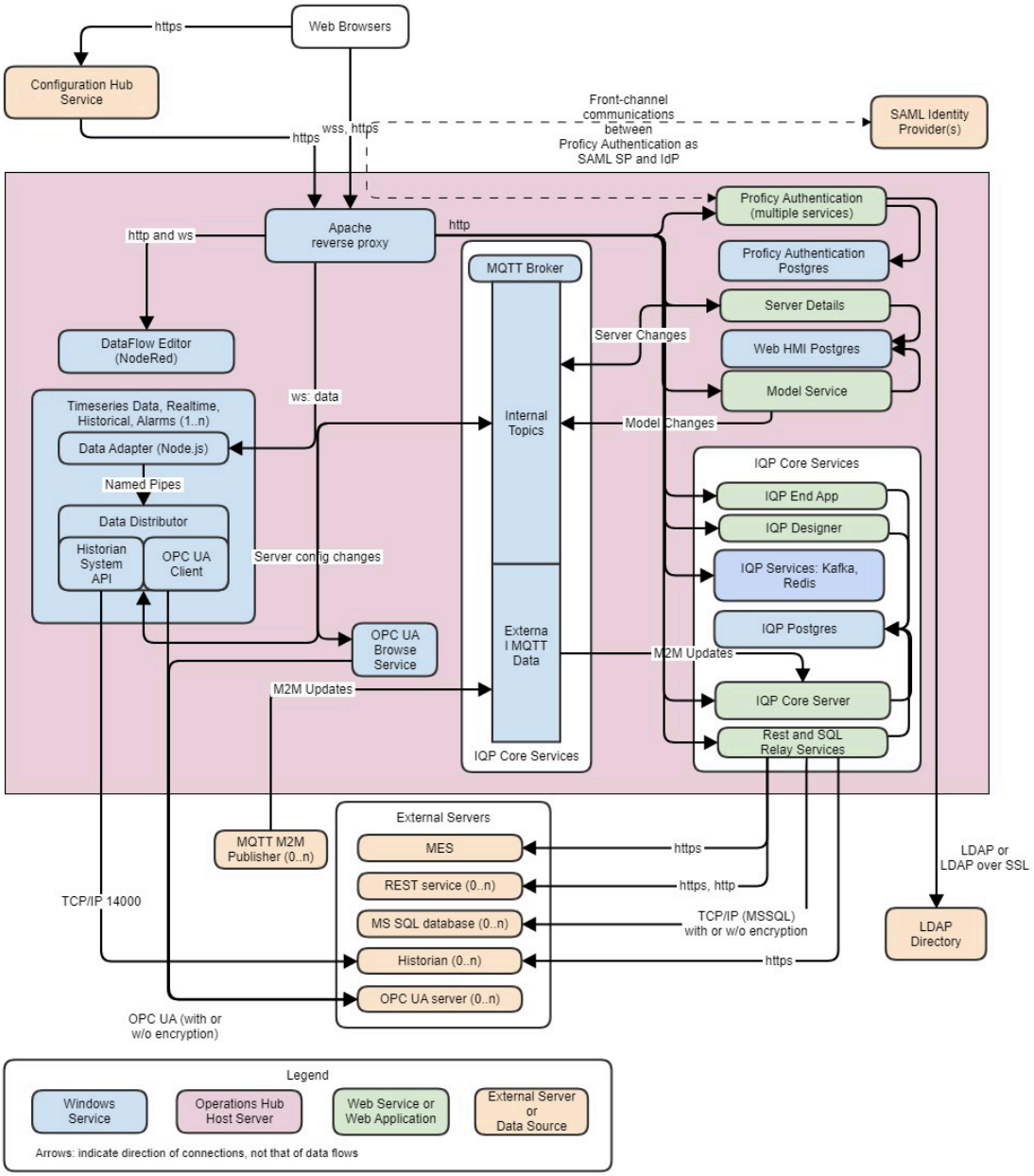
Table of Contents

1. Introduction

GE Operations Hub provides a platform to quickly develop web applications to visualize, monitor, and control your plant operations. GE Operations Hub was designed following best security practices to protect customers' digital assets. This document covers security related topics when deploying Operations Hub, as well as steps and measures customers should take in order to maximize the security when deploying and maintaining GE Operations Hub.

2. Deployment Overview

The following is a diagram depicting elements of Operations Hub in deployment.



Most notable is the pink-colored box in this diagram, which represents the host where Operations Hub is deployed to – which is the trust boundary from security's point of view.

In the diagram, the arrows represent connections along which data flows. Arrows points to the direction of connection (that is, which party initiates the connection), which can be different from the direction of logical data flow. The peach-colored boxes are either (a) external data sources, where data flow into Operations Hub, regardless of the direction of arrows, or (b) an external server or service that Operations Hub interoperate with to provide rich user experiences It should be noted that while the Proficy Authentication services (previously referred to as UAA) can be deployed as a standalone product on a different host, in which case the communications with it should be considered a potential vector for attacks and thus be protected accordingly.

The browser box at the top represents clients that access the data flowing into and managed by Operations Hub. Together with external data sources, these external connections could potentially be attack vectors and therefore must be secured.

3. Firewall Configuration and Securing the Ports

As illustrated in the diagram, one common attack vector is the TCP ports exposed by servers, and it is the best to limit them as much as reasonably and practically possible, as long as normal operations are not hindered.

GE Operations Hub opens multiple ports, which fall under two categories.

Under one category are the ports intended to be accessible externally. They are a secure http port for web server to allow user access and a port for external MQTT data in-flow. For Operations Hub v1.6, the https port is 443, and the MQTT data port is 1883. For Operations Hub v1.7 onward, the https port is configurable and selected by the user at install time. While in-bound rules should be created to allow access, you should evaluate the range of remote IP addresses, and restrict the access by scope (i.e., to the identified range of IP addresses permitted to access).

The other category includes the ports used for internal communications between different components of Operations Hub, and there is no need for them to be accessed remotely. For such ports, they should be blocked. This is in line with generally how TCP ports should be treated by a Firewall – block until there is a specific need.

The following table lists the ports used by Operations Hub that are not configurable. They must be made available and free of conflict on the host before installing Operations Hub:

TCP Port Number	Purpose	Remarks
1883	Inbound M2M MQTT data	Should be remotely accessible to MQTT clients that send M2M data to Operations Hub.
6379	Redis	No remote access
9002	Data Distributor	No remote access

4. Certificates

Public Key Infrastructure and at its core digital certificates are the foundation of how modern network communications are protected from being eavesdropped or compromised. GE Operations Hub as a web application follows industrial standards when it comes to using certificates to ensure data communication between web clients and web servers is secure.

In general, communications to each server are protected by a server certificate. Given that there are multiple data flows to various servers, user should have a good understanding of how each data flow is protected and how the associated certificate is managed.

4.1 Operations Hub Server Certificate

Operations Hub acts as an https/wss server when communicating with web browsers. For this purpose, a server certificate is needed to authenticate the server to clients. At install time, a certificate is generated locally, based on the provided list of host names. In addition, a certificate management tool is provided to allow an externally issued server certificate to be imported and put in use.

4.1.1 Using Local Certificate

This is the out-of-box option provided by Operations Hub. For customers who do not need to support a large number of clients or cannot get a server certificate from an external issuer, they can continue to use this certificate after deployment.

While this option does not require additional work up-front, Operations Hub's installer needs to create a certificate authority (CA) to issue the server certificate. This certificate authority is not trusted by any clients, and therefore its certificate needs to be added to the trusted issuers list on every client machine/device.

This local certificate expires in two years, so the certificate management tool should be used to renew it when it's approaching expiration. This should be a part of the maintenance routine.

For Operations Hub v1.6 onwards, the CA certificate is valid for five years. When it is approaching expiration, you should run Operations Hub's certificate management tool to renew the local certificate. As a part of local certificate renewal, the issuer certificate will be renewed if it is expiring.

4.1.2 Using Externally Issued Certificate

Optimally, a server certificate issued by an external certificate authority should be used. Whether it is issued by an enterprise-wide certificate authority (to be used on the intranet) or a commercial one, the root CA is usually trusted by client machines and devices

In order to use such a certificate, user should use the Operations Hub certificate management tool to import it and its private key into Operations Hub. Note that it is strongly recommended to import the certificate chain, including the server certificate, all intermediate CA certificates, and the root CA certificate. It is optional to include the root CA certificate only

if the server certificate is purchased from a commercial certificate vendor. If you have received certificate files in PEM format, you can copy and paste all of them into one PEM file to be imported.

An imported server certificate must list the primary host name as one of the Subject Alternative Names (including wildcard names). If not, the certificate management tool will give a warning, since using such a certificate not intended for a host will cause runtime errors.

Importing merely loads the certificate into Operations Hub. User needs to specifically elect to use the imported certificate, also in the certificate management tool. During testing phase, user may switch between the local certificate and the imported certificate to help troubleshoot any suspected certificate problems.

As with the local certificate, the imported certificate expires after a period and a new certificate needs to be imported to replace it once it approaches expiration time.

4.2 Operations Hub Server as Client

Operations Hub can also act as a client when interacting with external hosts. In such cases, Operations Hub relies on certificates provided by external hosts to authenticate them. This is done by verifying that the server certificate was issued by a trusted certificate authority. For a commercially issued server certificate, the root issuer is usually already trusted. For self-signed certificates or certificates issued by an unrecognized certificate authority, explicit steps need to be taken to ensure Operations Hub accepts such certificates. Such activities are also referred to as “trust management”.

Usually a root issuer’s certificate has a long validity period. However, self-signed certificates can vary and therefore you still should pay attention to how long a certificate you are trusting remains valid and be sure to update them when it is close to expire.

4.2.1 REST Data Sources

Operations Hub supports accessing external REST data sources. For each https-based REST data source, you can configure an issuer certificate to trust. This only applies to one data source and doesn’t apply to any other data sources or any other operations.

4.2.2 Relational Database (SQL) Data Sources

Similar to a REST data source, you can configure an issuer certificate to trust for each SQL data source. This only applies to one data source and doesn’t apply to any other data sources or any other operations.

4.2.3 LDAP server

The Proficy Authentication server installed as a part of Operations Hub can use an LDAP server as an external identity provider. Usually, LDAPS (LDAP over SSL) rather than unencrypted LDAP should be used as the protocol to access the LDAP directory. Therefore, when Proficy Authentication server establishes connections to the LDAP server, it needs to trust the issuer of the server certificate presented by the latter. If the issuer of the certificate is not a well-recognized certificate authority, the Proficy Authentication Identity Provider Configuration tool should be used to load such its certificate to be trusted.

4.2.4 External Proficy Authentication Server

Similar to how an LDAP server is incorporated, user may choose an external Proficy Authentication server as the authorization server Operations Hub uses.

In case the selected Proficy Authentication server uses a server certificate that wasn't issued by a recognized certificate authority, you need to provide Operations Hub the issuer's certificate to be trusted. This is typically done by providing the certificate to the Operations Hub installer at install time, but can also be done after install by using the Certificate Management Tool, where a tab "External Trust" is dedicated to managing the trust of an external Proficy Authentication server. For example, when the root CA certificate changes for the Proficy Authentication server.

4.3 Trust Operations Hub Certificate on Client Machines

If you opt to use the locally generated server certificate for Operations Hub server, then you will need to ensure the issuer is trusted on the client machines, in order to avoid the certificate warning messages given by browsers.

The exact process differs based on the operation system and the browser. Operations Hub does send the entire certificate chain in the TLS negotiation with the browser, so the browser should allow you to view the certificate path and export individual certificates. You should export the root issuer's certificate (the one at the top of the certificate path or chain) and then use the operation system's certificate management tool to import it into a trusted root certificate store.

If you are developing custom client applications based on the API of Operations Hub, then you should import the root issuer certificate into the language runtime's trust store.

Additionally, you should have a record of client machines where this CA certificate is trusted. As a part of scheduled maintenance, Operation Hub's CA certificate's expiration should be monitored and once it is renewed, all the client machines shall re-establish the trust to the renewed CA. In the event this CA certificate is ever compromised, you should remove it from the trusted root certificate store on all the client machines and replace it with a new one.

5. User and Security Principal Management

5.1 Proficy Authentication server

In Operations Hub, the Proficy Authentication server is an integral part used for managing user accounts and access control. It supports user accounts created and managed locally, as well as ones originating from another Identity Provider. With v1.7, LDAP is the protocol for integrating external Identity Providers. Starting with v2.0, SAML Identity Providers are supported. Thru Proficy Authentication server and its support of external Identity Providers, Operations Hub can delegate management of users and their access control to an existing directory service, such as Active Directory. User accounts in an external directory are mapped into Proficy Authentication server, as well as their access control information.

To further simplify administration, Operations Hub can use an existing Proficy Authentication instance, for example, one installed with another GE Digital Products, such as Historian.

However, as of Operations Hub 2023.1, it is not supported to share an instance of Proficy Authentication server with another Operations Hub deployment.

5.2 Different User Types

At the highest level, there are four types of user accounts (or roles, in general terms) in Operations Hub:

- Site Administrator

  A site administrator is someone who can perform certain maintenance tasks for an instance of Operations Hub. While considered a privileged account, such a user doesn't have access to most application data. It is IMPORTANT, when using any external tools such as Proficy Authentication configuration UI, to not grant the corresponding group membership (named "iqp.studioAdmin") to user accounts of other three types.

  For Operations 2023.1 or any prior versions, a site administrator should only use Chrome or Edge to access the Site Administration Console (/site/adminconsole/SiteAdminConsole.do), and consult GE Digital Technical Support if there is a need to use another browser to access it.

- Operations Hub Administrator

  An Operations Hub Administrator is the "superuser" of an Operations Hub deployment. Such an account is responsible for creating or maintaining other user accounts and managing their access to application data.

- Application Developer

  An application developer is a user who can create and maintain applications using Operations Hub's Designer environment.

  It is important to note that while application developers are not administrators, they are still considered highly privileged as they author applications that run in other users' security context. It is therefore vital to safeguard the privileges to develop, import, and deploy applications and only grant them to trusted individuals, and import applications only from trusted sources.

  An alternative (also as an additional measure) is to separate the application design environment and production environment by running multiple Operations Hub instances, and only deploy to production instances those applications that have been vetted by administrators or trusted application developers. Such a vetting process should in particular scrutinize Javascript code for anything potentially malicious.

- Application User

  An application user is authorized to view and interact with a specific set of running applications, but not authorized to develop (make changes to) applications.

5.3 Proficy Authentication Clients

Other than users, Proficy Authentication as an OAuth2 authorization server also supports and in fact relies on *clients* (as defined in OAuth2 standard). For a newly deployed Proficy Authentication instance, there is no user account, and a built-in "admin" *client* is used for bootstrapping and provisioning. Similarly, if you are using an external instance of Proficy Authentication server, the admin *client* credentials should be provided to you by its administrator, so its provisioning related to Operations Hub can be performed.

During this phase of provisioning, Operations Hub's UAA provisioner service will create additional *clients* for different functional needs. Usually this process and this set of *clients* do not need human user's attention. However, if there are login failures after install, then UAA provisioner service's log files may provide useful troubleshooting information.

5.4 Relations to Security Realms in the Host

Operations Hub's security is related to the host operating system's in a few ways.

Foremost, Operations Hub's security relies on the operating system to ensure access to sensitive data is restricted. On Windows, it means that many files are only read-only to non-administrators and files containing sensitive data are only readable by administrators. Therefore, it is critically important to ensure administrators' access is closely guarded and not compromised.

Most services in Operations Hub run in the security context of a dedicated OS service user account during normal operations. The service isolation reduces the chance that compromise of one service by a remote attacker leads to system-wide security breakdowns.

There is no special consideration for a host in Active Directory. However, it is highly recommended that in this case Active Directory be used as an LDAP server and external Identity Provider to the Proficy Authentication server.

6. Access Control and Authorization

Operations Hub uses two complementary authorization mechanisms to control access to program features, user-developed applications and data, as described below.

6.1 Proficy Authentication Groups

Proficy Authentication groups are used to control accesses to application features, such as:

- logon
- access to the site admin console
- access to the designer user interface
- access to the runtime application environment, and
- access to individual applications, queries and pages (new in v1.7)

Access is granted based on user's membership in a set of pre-defined groups or customer-defined groups. The following table describes the pre-defined groups and their access to features, corresponding to what's described in Section 5.2 Different User Types:

Group Name	Description
Iqp.studioAdmin	User with privileges to access the site admin console, which is primarily used for configuration the built-in MQTT broker for inbound MQTT data. IMPORTANT: any users of another type shall not also be a member of this group. Also see 5.2 Different User Types.
iqp.tenantAdmin	User with administrative privileges.
iqp.developer	User that can create and update applications and have access to Entities and Queries.
iqp.user	User can access applications developed with Operations Hub.

Starting from v1.7, it is possible to control access to applications and pages with user's Proficy Authentication group memberships. Refer to the product documentation on how to set permissions for them.

Other than built-in user accounts, it is recommended that you not add user accounts to these groups directly. Instead, organize users into groups based on their roles and then assign these groups as members of the built-in groups above ("nesting"). This additional layer of indirection provides flexibility and minimizes the administrative work when user's role changes in the organization. Group nesting can be done using the Proficy Authentication Identity Provider Configuration tool (even if you are not using an LDAP directory).

If your organization has a larger number of users and already has an LDAP directory, it is strongly recommended that the LDAP server be used as the identity provider. You need to use Proficy Authentication's Identity Provider Configuration tool to configure its to access the LDAP directory. In particular, you should map LDAP groups to the built-in Proficy Authentication groups above, and then manage group membership and permissions in the LDAP directory.

6.2 Role Trees

Operations Hub also supports a fine-grained access control to data. For more details, refer to the following link:

https://www.ge.com/digital/documentation/opshub/windows/c_about_roles.html

7. Logging

Operations Hub maintains a centralized directory where log files generated by various services in Operations Hub are stored. Unless you have chosen to customize it at install time, it is typically under:

%*ProgramData*%\OphubLogs, and
%*ProgramData*%\ProficyAuthenticationLogs

(where *ProgramData* is the system-designated directory for storing application runtime data, typically \ProgramData directory of the system drive).

Underneath either of these directories each service or process has its own subdirectory to store its log files, such as uaa-tomcat, DataDistributor, etc. Each service maintains its own logging configuration, which determines what is logged and how detailed the logging is. Usually, it is informational entries and audit events. When error occurs, log files contain richer contextual information that can be useful for troubleshooting. However, there are times where apparent errors or exceptions in log files are not true indication of server-side failures. For example, if a user entered a bad password, this error is benign and any corresponding entries in the Proficy Authentication log file can be safely disregarded.

GE Technical Support may instruct customers to tune logging levels and request log files from this directory when providing support.

8. Mosquitto MQTT Broker and External Device Communication

Operations Hub is installed with Mosquitto, a message broker that implements the MQTT protocol. The external port used by the MQTT broker, port 1883, is secured by an initial user and password post installation (mqttuser/mqttpasword).

When not using MQTT it is important to ensure that the machine firewall does not allow external communication to this port (as defined in the Firewall chapter of this document).

It is important to note that the Mosquitto broker is also used for inter-process communication within the internal processes (on port 1884).

For optimal security you should change the default password post installation if and when port 1883 is not blocked for external access. Follow this procedure to change Mosquitto password:

1. Create a new Password file:

    - From the Windows cmd.exe, switch to following folder: C:\Program Files\GE\Operations Hub\mosquitto. (Note the exact location of the folder may vary, if you chose to customize the install location.)
    - Run the following command:

      `mosquitto_passwd -c passwordfile` mqttuser

      You will be prompted to supply the password for the user.

2. Replace existing password file with the new one you just created.

3. Restart GE Operations Hub Mosquitto service.