OpenBlue
Central Utility Plant

OpenBlue Plant Optimizer Security and IT Guide

Building Technologies & Solutions
www.johnsoncontrols.com

LIT-12013045
Release v2023.Q3
2023-09-22

Contents

Introduction

Johnson Controls® OpenBlue Plant Optimizer is a software solution that uses data from the plant automation system and from external web services to advise operators in making the optimal operating decisions. OpenBlue Plant Optimizer can also operate the central plant automatically, while it informs operators of each change in advance.

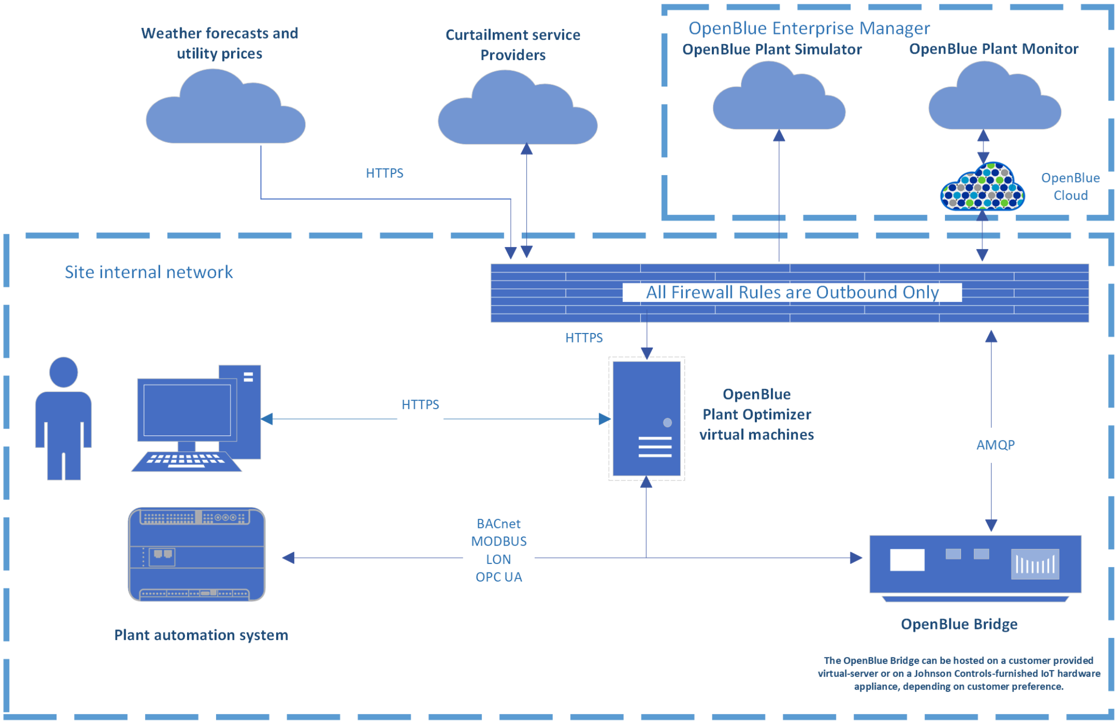
Plant Optimizer supplies predictive optimization algorithms and provides a user interface for real-time monitoring and supervisory control of the central plant. With a HTTPS connection, you can access the Plant Optimizer user interface from any browser.

There are three different system architecture options for the OpenBlue Central Utility Plant (CUP) software applications, which are flexible to customer-specific requirements:

1. The Plant Optimizer application runs on virtual servers on premise, while the Plant Simulator and Plant Monitor applications run in Johnson Controls' cloud environment.
2. All applications run in the cloud with a connection through OpenBlue Bridge, which can run on a local virtual machine or a Johnson Controls furnished appliance.
3. Plant Optimizer runs on virtual servers on premise with no external connections to the internet. However, in some cases there is a connection to a weather forecast service.

Under the architecture options 2 and 3, there can be outbound connections to collect weather forecasts, utility pricing data, demand response data, or to export Plant Optimizer data or application troubleshooting logs to the cloud. Outbound connections can be made through the internet (HTTPS) or a cellular modem within the OpenBlue Bridge appliance.

Figure 1: OpenBlue CUP expert package with Plant Optimizer on premise



Weather forecasts and utility prices
Curtailment service Providers
OpenBlue Enterprise Manager
OpenBlue Plant Simulator
OpenBlue Plant Monitor
HTTPS
OpenBlue Cloud
Site internal network
All Firewall Rules are Outbound Only
HTTPS
HTTPS
OpenBlue Plant Optimizer virtual machines
AMQP
BACnet
MODBUS
LON
OPC UA
Plant automation system
OpenBlue Bridge

The OpenBlue Bridge can be hosted on a customer provided virtual-server or on a Johnson Controls-furnished IoT hardware appliance, depending on customer preference.

Figure 2: OpenBlue CUP expert package with Plant Optimizer in the cloud

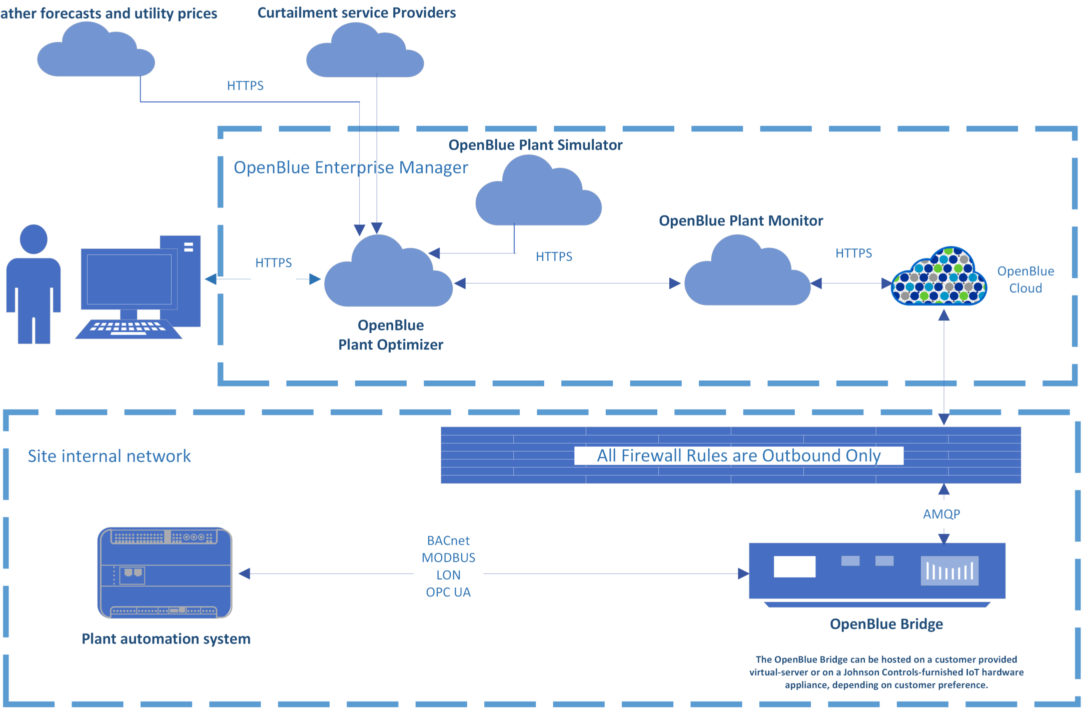
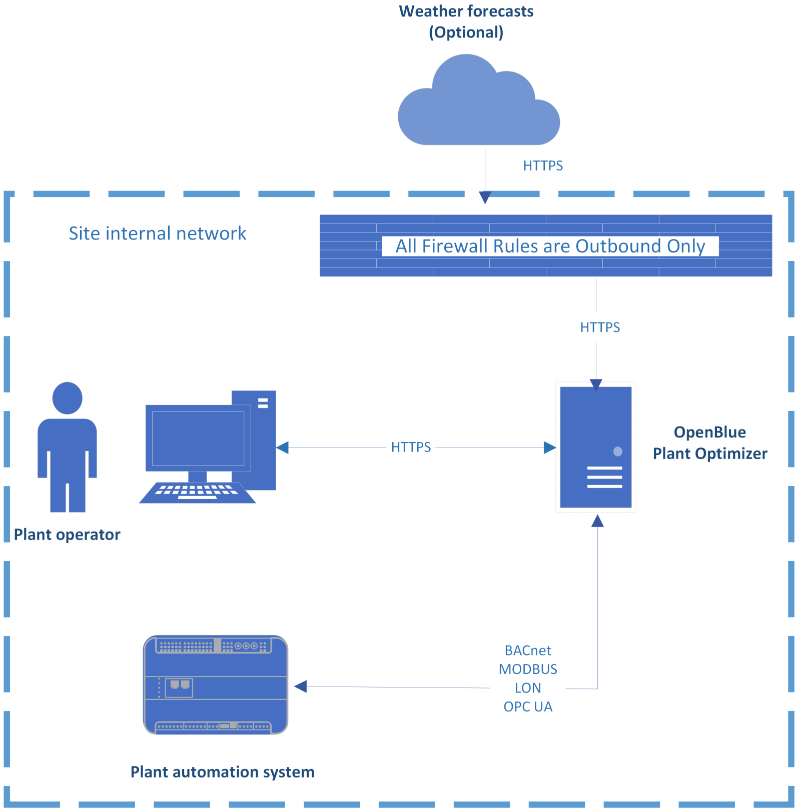

Weather forecasts and utility prices
Curtailment service Providers
HTTPS
OpenBlue Plant Simulator
OpenBlue Enterprise Manager
OpenBlue Plant Monitor
HTTPS
HTTPS
HTTPS
OpenBlue Cloud
OpenBlue Plant Optimizer
Site internal network
All Firewall Rules are Outbound Only
AMQP
BACnet
MODBUS
LON
OPC UA
Plant automation system
OpenBlue Bridge
The OpenBlue Bridge can be hosted on a customer provided virtual-server or on a Johnson Controls-furnished IoT hardware appliance, depending on customer preference.

Figure 3: OpenBlue CUP 'no cloud' package with Plant Optimizer on premise



OpenBlue Plant Optimizer security and network configuration considerations

Plant Optimizer uses industry-standard system security and encoding protocols to protect against unauthorized access to data and control systems, and includes the following security features:

- TLS 1.2/HTTPS and security certificates provide secure encrypted communication, which prevents unauthorized access.
- The Plant Optimizer web application uses an automatically generated, self-signed CA Root certificate. If you want to use your own trusted security certificate, apply the customer certificate on your web server.

The Plant Optimizer server and client are located inside the site internal network, to ensure that the security considerations are the same as for the whole site.

Plant Optimizer client security and network configuration

An end user's browser connects to the Plant Optimizer client through the HTTPS protocol. The HTTPS protocol encrypts password data in transit using TLS 1.2. Passwords at rest are not stored in Plant Optimizer. User accounts and their passwords are stored either in the Metasys Extended Application and Data Server with or without Active Directory (AD) integration, or in the CUP Network Automation Engine at plants that use an alternative automation system. Each user has their own unique logon credentials and identifiers. An administrator adds Plant Optimizer users and each individual user is assigned roles based on their needs.

Two authentication services are available for Plant Optimizer software that runs on an on-premise server:

- Use the existing Metasys local system authentication database for a Metasys building automation system network. All Plant Optimizer users must first be set up as users in the Metasys system. Use the same local system credentials to log on to Metasys and Plant Optimizer.
- Integrate with AD through Metasys components. This option is only available if Metasys is part of the AD domain. AD users are configured on the Metasys system before they access Plant Optimizer. Plant Optimizer does not currently support sites that use AD alternate UPN authentication for single sign on. To confirm that the authentication works, enter your credentials in the Metasys Launcher dialog box when you log on or log off.

ⓘ **Note:** The system administrator for the system authentication database issues logon credentials to users.

Use a strong password to minimize the chances of unauthorized access. Ensure your password meets the following standards:

- The password must include a minimum of 8 characters and a maximum of 50 characters.
- The password cannot include spaces or a word or phrase that is in the Blocked Words list.
- The password and the username cannot share the same three consecutive characters.
- The password must meet the four following conditions:
    - Include at least one number.
    - Include at least one special character (-, ., @, #, !, ?, $, %)

        ⓘ **Note:** Only the special characters in the above list can be used; all other special characters are invalid.

    - Include at least one uppercase character.
    - Include at least one lowercase character.

In Metasys ADX or CPO-NAE, the password for all user accounts is set to expire in 60 days by default. The maximum password age, password uniqueness, and account lockout properties are not configurable for systems where the ADX is integrated with AD and RADIUS users. You can configure the account policy parameters in either the ADX for Metasys sites, or in the CPO-NAE for plants that use other automation systems.

Table 1: Password configuration

Field	Description	Default Value
Password never expires	The password never expires.	Unselected
Expires in days	You must enter the number of days until the password expires.	60 days for users selected
Do not keep password history	The system does not remember the password history.	Unselected
Remember passwords	The system remembers the number of passwords indicated. The system does not allow the user to repeat the same password.	10 previous passwords selected
Never terminate	The session does not terminate as long as the operating system that hosts the Metasys system is not suspended or terminated to shut down, sleep, or hibernate. Make sure the options to suspend the operating system are disabled.	Unselected
Terminate in minutes	The amount of time the system allows the user to remain in active before the session terminates and automatically logs the user off from the Metasys system.	30 minutes selected
No account lockout	The account does not lock out.	Unselected
Lockout after bad attempts	The account locks out after the designated number of sequential failed logon attempts.	3 failed login attempts for users selected
Lockout in minutes	The account locks out after the designated number of sequential failed logon attempts within the designated time frame. Users are presented with the opportunity to re-enter their password once every five minutes thereafter.	15 minutes selected
Do not check user account for dormancy	The account never becomes dormant. The user has access to the account regardless of the number of days after the last logon.	Unselected
Dormant after days	The account becomes dormant after the designated number of days after the last logon.	365 days selected

Table 1: Password configuration

Field	Description	Default Value
Create dormant user account event	An event message displays to alert the administrator that the dormant user account has not been accessed in the designated number of Dormant After (Days). ⓘ **Note:** For a report of all accounts, dormancy settings, and status, click **Query** and select **Dormant User Account Report** in SMP. Dormant user account events are also included in the **Audit Viewer** and the **Event Viewer**.	Selected
Lock out user account when dormant	The account is locked out after the designated number of dormant days.	Unselected

Plant Optimizer server security and network configuration

DevOps remote access

If it does not violate the customer's IT security policy, you can give DevOps users remote access to VMs to install software. Remote DevOps users do not need elevated server rights. Open port 10933 on the VPN to facilitate remote software deployment to the VMs.

Updates and patch management

Updates to the virtualization system, hosts, or guests including operating system, anti-virus' and other base image software are the responsibility of the customer as defined by their security and service standards. Johnson Controls is responsible for security patches and updates to the Plant Optimizer software.

Plant Optimizer server requirements

You can run Plant Optimizer on non-dedicated server hardware. The minimum VM allocation requirements depend on the following variables:

- The number of plants included in the instance
- The size and complexity of the plants
- Whether a physical or virtual CPO-NAE is used to integrate the plant automation system.

Plant Optimizer requires up to three VMs:

- A web application server
- A database server
- A CPO-NAE server

After Plant Optimizer is stable and operational, Johnson Controls works with the customer’s IT team to measure resource utilization and adjust the VMs to match the requirements of the site in the most cost-effective way.

Table 2: Hardware and software requirements

Type of Deployment	VM use	VM OS	No. of VMs	Cores	CPU (GHz)	RAM (GB)	C: Drive (GB)	D: Drive (GB)
All on-premises sites	CUP Web Application VM (UI + Web Service APIs)	Windows Server® 2016 or later	1	8	>2.5	32	100	100
	SQL database VM	SQL Server 2016, SQL Server 2017, SQL Server 2019 Enterprise (preferred) or Standard	1	4	>2.5	64	100	1000
Virtual CPO-NAE (NAE85) only	CPO VM	Windows Server 2016 or later	1	4	>2.5	16	100	100
Metasys ADX	Metasys ADX	Windows Server 2016 or later MS SQL Server 2016 Standard or MS SQL Server 2016 Enterprise	1	4	>2.5	32	100	1000

ⓘ **Note:**

- For the CUP Web Application VM, the number of cores and RAM size may vary based on number and size of plants.
- For SQL database VM and Metasys ADX, D: Drive size may vary based on the number and size of plants.
- ADX virtual server requirements only apply for new construction or brand new Metasys installation.

Windows server features and role requirements

Table 3: Windows server features and role requirements

Windows server features	Windows server roles
.NET Framework 3.5 features • NET Framework 3.5 (includes .NET 2.0 and 3.0) • HTTP activation	File and storage services • Storage services
.NET Framework 4.6 features • NET Framework 4.6 • ASP.NET 4.6 • WCF services	Web server (IIS) • Common HTTP features - Default document - Directory browsing - HTTP errors - Static content

Table 3: Windows server features and role requirements

Windows server features	Windows server roles
Message queuing • Message Queuing Server	Health and diagnostics • HTTP logging • Request monitoring
• SMTP Server Tools • SNMP Tools	Performance • Static content compression
SMB 1.0/CIFS File Sharing Support	Security • Request filtering • Windows authentication
SNMP service • SNMP WMI provider	Application development • .NET Extensibility 3.5 • .NET Extensibility 4.6 • ASP.NET 3.5 • ASP.NET 4.6 • ISAPI extensions • ISAPI filters
Windows Defender features • Windows Defender • GUI for Windows Defender	Management tools • IIS Management Console • IIS 6 Management Compatibility - IIS 6 Metabase Compatibility - IIS 6 Management Console - IIS 6 Scripting tools - IIS 6 WMI compatibility • IIS management scripts and tools
Windows Powershell • Windows Powershell 5.1 • Windows Powershell 2.0 Engine • Windows Powershell ISE	
Windows Process Activation Service • Process model • .NET Environment 3.5 • Configuration APIs	
WoW64 support	

Table 4: Additional Windows component requirements

Additional Windows component requirements
.Net 6.0.19 or later is recommended

Table 5: SQL Server requirements

SQL Server requirement	Additional detail
Ensure the most current SQL Server pack is installed.	Requires the latest service pack to be installed.
Ensure **SQL Server Always-On** is applied.	Select the Availability Groups (AG) database option. Ensure the instance is named.
Give database owner (DBO) rights to Johnson Controls engineers.	Johnson Controls engineers require DBO rights in application databases to configure the application schema.
Set **SQL Server collation** to `sql_latin1_general_cp1_ci_as`.	sql_latin1_general_cp1_ci_as is the default American install setting for **SQL Server collation**. This enables the deployment of the database.
Turn on **Filestream enabled** and **broker enabled** settings.	These settings are not turned on by default.
Enable the **Transactional File Stream** setting.	Enable this setting to ensure that the SQL server functions correctly.
Configure the SQL Server to require mixed-mode authentication.	Mixed-mode authentication is a security requirement.
Apply elevated SQL rights to DevOps administrators during installation.	You can remove or reduce elevated rights after installation.
SQL Server uses default port 1433.	Contact technical support (BTS-CPO-TechSupport@jci.com) if a different port is required.

ⓘ **Note:** You can implement SQL data encryption but it is not required.

ⓘ **Note:** Plant Optimizer can use either a dedicated SQL server, VM, or a shared server instance such as an existing SQL farm. The network must be configured to allow access from Plant Optimizer Web Application VM to the SQL Server instance. Johnson Controls requires elevated rights on the SQL Server instance during the installation process.

Network requirements

Internal communication

Important: Set up all virtual servers on the same VLAN subnet as the plant automation system to avoid the need for routing rules and tables between subnets.

Plant Optimizer uses industry-standard protocols to connect to the NAE, such as HTTP, HTTPS, and BACnet®. The NAE uses MODBUS, LON, and BACnet to connect to the plant automation system.

ⓘ **Note:** If the NAE is on a different subnet to the Plant Optimizer server, open port 47808 on Plant Optimizer for NAE BACnet/IP Broadcast Management Device (BBMD) communication traffic. If the NAE is on the same network subnet as the Plant Optimizer server, the BACnet communication does not require a BBMD.

Johnson Controls works with your plant automation system maintenance services provider to set up the network connections.

External communication

The Plant Optimizer server connects to the Internet using HTTP or HTTPS to access data from external web services, such as weather forecast data or utility prices. Configure the site firewall or proxy server to allow the outgoing connection from the CUP server.

- For a HTTP connection, access firewall port 80.
- For a HTTPS connection, access firewall port 443.

Firewall rules

Table 6: Firewall rules for Plant Optimizer

Source	Destination	Port	Protocol	Connection details
Application VM	Database VM	1433	Raw socket	Standard SQL server port
End user network	Application VM	443	HTTPS	User interaction with web front end
CPO-NAE VM	Application VM	47808	BACnet/ IP over UDP	Bidirectional communication for BAS data
Application VM	CPO-NAE	47808	BACnet/ IP over UDP	Bidirectional communication for BAS data
Application VM	CPO-NAE	443	HTTPS	Additional user/point data pulled from web API
Application VM	CPO-NAE	80	HTTP	Additional user/point data pulled from web API
Application VM	*.noaa.gov (internet)	443	HTTPS	Weather forecast – https://graphical.weather.gov
Application VM	*.accuweather (internet)	443	HTTPS	Weather forecast – https://xml.efas.aes.accuweather.com/
Application VM	*.logdna.com (internet)	443	HTTPS	Outbound-only port for log shipping for technical support to LogDna Dashboard
Application VM	*.planningtoolapi.mysmartcentralplant.com (internet)	443	HTTPS	Optional outbound-only port to CUP Plant Simulator API
Application VM	*.jemprod.myenterprisemanagement.com (internet)	80	HTTPS	Optional outbound only port to JCI EIMS for authentication to CUP Plant Simulator
JCI VPN	All CPO VMs	3389	RDP	Allows remote admin for JCI

Table 6: Firewall rules for Plant Optimizer

Source	Destination	Port	Protocol	Connection details
JCI VPN	All CPO VMs	10933	Raw socket	Allows automated deployments from Octopus
OpenBlue Bridge	OpenBlue Cloud	443	HTTPS, AMPQ, MQTT	OpenBlue Cloud authentication, telemetry data, command and control
OpenBlue Bridge	OpenBlue Cloud	443	HTTPS	OpenBlue Bridge device updates
OpenBlue Bridge	OpenBlue Cloud	53	DNS	Public DNS servers, if none are available on the customer network
OpenBlue Bridge	OpenBlue Cloud	123	NTP	Public NTP server, if none is available on the customer network
Application VM	*.jemprod.myenterprisemanagement.com/authorization/ *.jemprod.myenterprisemanagement.com/validation/ *.jemprod.myenterprisemanagement.com/security/	443	HTTPS	Access to the OpenBlue Enterprise Manager EIMS API
Application VM	*.jemprod.myenterprisemanagement.com/entity/	443	HTTPS	Access to the OpenBlue Enterprise Manager Entity API
Application VM	*.jemprod.myenterprisemanagement.com/timeseries/ *.jemprod.myenterprisemanagement.com/java/	443	HTTPS	Access to the Time Series API
Application VM	*jemprod.myenterprisemanagement.com/license/	443	HTTPS	Access to OpenBlue Enterprise License Management API
Application VM	*.jemprod-publisher.myenterprisemanagement.com/ *.jemprod-websocket.myenterprisemanagement.co	443	HTTPS	Access to OpenBlue Enterprise Message Broker API
Application VM	*.jemprod.myenterprisemanagement.com/heartbeatapi/	443	HTTPS	Access to OpenBlue Enterprise Heartbeat API
Application VM	*.jemp-autoconfiguration-ui.azurewebsites.net	443	HTTPS	OpenBlue Auto Configurator UI (OBAC)

Table 6: Firewall rules for Plant Optimizer

Source	Destination	Port	Protocol	Connection details
Application VM	*.jemp-autoconfigurationtool.azurewebsites.net	443	HTTPS	OpenBlue Auto Configurator API (OBAC)
Application VM	*.jcids.jfrog.io	443	HTTPS	OpenBlue Bridge installation and maintenance

ⓘ **Note:** Apply open firewall rules to use weather services. You only need to enable one weather-forecast service destination. Use Accuweather outside North America. Fully air-gaped sites that operate based on load prediction do not need weather forecast services.

Table 7: Local/Intranet Connectivity

Direction	Port number	Transport protocol	Protocol	Required	Endpoint	Purpose
Bidirectional	47808 Port can be what is applicable by BMS settings	UDP	BACnet/IP	Yes	OpenBlue Bridge and all engines IP addresses	To collect BACnet data and push it to OpenBlue Cloud

Network latency requirements

The application requires manual intervention if Plant Optimizer takes more than one minute to push operational instructions back to the plant automation system.

Logging and monitoring

The Audit Log continuously tracks user modifications to Plant Optimizer. Enter an explanation for each modification that you make to the operation. The following modifications appear in the Audit Log:

- Forecast input overrides, for example, loads, weather, dynamic utility rates.
- Manual input entries, for example, occupancy schedules, equipment maintenance schedules, fixed utility rates.
- Changes in the equipment availability schedule.
- Operating mode changes, for example, switching between Auto mode and Advisory mode.

The CUP technical support team can provide logs for a user's last change, add, and delete upon request. You can only access data through Plant Optimizer and you can download, or export, all data sets, including JSON models, and delete data. It is the user's responsibility to implement an appropriate backup strategy in the event of any data corruption. In case of end of agreement, you have access to the application for a transition period to extract or delete any data files or model files. After the transition period, the data is deleted.

Plant Optimizer can be configured to utilize a non-Johnson Controls logging site called LogDna that ships non-sensitive data, outbound only from site to logdna.com, which allows Johnson Controls users to see real time application logs.

Configuring email notifications

Configure email notifications for changes to the operating mode, unavailable utility pricing, and unavailable monitored weather extend periods of adviser mode operation, and equipment being unavailable to Plant Optimizer, for example, due to manual overrides.

About this task:
To set up Plant Optimizer with email notifications, contact CUP technical support and provide the following information:

1. SMTP server name
2. Required SMTP port

   ⓘ **Note:** Indicate to technical support if you are not using a standard 25 SMTP port.
3. Username and password credentials used to send the alert emails

Technical support enter the SMTP server name and credentials in the A3S agent app settings, as well as the email 'from' address in the form cpo-notifications@XXXX.com, where XXXX is the customer domain.

If you do not have SMTP credentials, use a Gmail® account.

To configure who receives each type of email notification, complete the following steps:

1. In the **Administration** interface, select **Configuration** from the menu.
2. In the **Optimization** tab, in the **Email Notifications** section, to enable email notifications, select from the following:
   - Change of Mode Notifications
   - Pricing Unavailable Notifications
   - Weather Unavailable Notifications
   - Advisory Mode Alert Notifications
   - Equipment Unavailable Notifications
3. In the email address field, enter an email address, and click **Add**.
4. From the **Send email notification after** list, select a time.
   Users listed in the **Email Notifications** section are notified that the operating mode has changed, or that utility pricing or weather is unavailable, along with the time and date of the change.

Performing server upgrades or network maintenance

Contact CUP technical support BTS-CPO-TechSupport@jci.com before server updates or patches, SQL server maintenance, or network firewall security changes. You can send a calendar invitation to BTS-CPO-OnPremDevOps@jci.com to alert the CUP Team.

Accessing data elements within Plant Optimizer and Plant Simulator

The types of data elements both CUP applications store include:

- Weather data, historic data, and 7-day forecasts

- Cooling, heating, and electricity hourly load profiles, historic data, and engineering design estimates
- Central plant equipment specifications and energy performance regression models
- Campus occupancy schedules
- Equipment out-of-service-for-maintenance schedules
- Utility rates, historic data, and day-ahead rates
- Central plant data trends for sensor process variable data points, system set points, and command data points
- Central plant energy efficiency metrics
- Central plant utility cost estimates
- Usernames and email addresses

  ⓘ **Note:** Plant Optimizer does not store end user email addresses associated with user accounts. Users configure email alerts, but email addresses on those alerts have no connection to user accounts.

This application does not create, modify, store, or transmit personally identifiable information (PII) or electronic personal health information (ePHI). Johnson Controls has a strong corporate policy dedicated to safeguarding personal information and processing it in a manner consistent with user expectations. Please review the Johnson Controls Privacy Notice http://www.johnsoncontrols.com/legal/privacy for information about how Johnson Controls handles personal information collected through the services.

Role permissions

Plant Optimizer is a local on-premises application that offers the following operational roles and associated role permissions for each role:

- **Guest –** can view all data and reports in the Plant Optimizer local instance.
- **Campus Schedule Editor** - same permissions as Guest, but can also edit campus schedules, and in doing so add Audit Log note.
- **Service Schedule Editor** – same permissions as Campus Schedule Editor but can also edit equipment out-of-service or must-run schedules.
- **Predictions Editor –** same permissions as Service Schedule Editor, but can also override load predictions, utility pricing, and weather predictions.
- **Operating Mode Editor** – same permissions as Predictions Editor, but can also change the Operating Mode, Auto vs Advisory.
- **Economic Demand Response Editor –** same permissions as Operating Mode Editor but can also override demand response program participation.
- **Admin** - can configure the application and provision user accounts.

Plant Simulator is a cloud-based application that offers the following user roles and associated role permissions:

- **Project Reviewer** – view-only access to see all data associated with specific projects including simulation results.
- **Project Modeler –** same permissions as Project Reviewer for specific projects, but can also configure units and campus schedules, edit models, edit data inputs, edit scenarios, run simulations, and can copy, or share, projects with other users to review.
- **Admin (Johnson Controls only)** – can view information for all projects, can create, modify, and delete users, and can delete projects or restore deleted projects. Admins have access to user names, can trigger a password reset, and can reassign project ownership.

Integration points

Johnson Controls interfaces

Plant Optimizer is a local on-premises application that integrates with:

- Johnson Controls Metasys building automation.
- Plant Simulator, which is cloud-based.

Third-party interfaces

Plant Optimizer also integrates with third-party interfaces:

- Log shipping for rapid technical support.
- Accuweather and National Oceanic and Atmospheric Administration (NOAA) Climate Data Online (CDO) web service API's, which are a third-party interfaces, for 7-day weather forecasts.
- **Optional**: Multiple electricity grid Independent System Operator (ISO) third-party APIs, for day ahead or real-time electricity market prices, for example, PJM and CAISO.
- **Optional**: Multiple Curtailment Service Provider (CSP) third-party APIs for participation in economic demand response or capacity-based demand response programs. The types of data that may be transmitted through this integration include:
    - Demand Response Bid submissions, which include bid offer price and MW of curtailment.
    - Receipt of bid award status, to inform the customer of whether bids were accepted.
    - Submission of historic, and day of event, meter data, to measure baselines and confirm that the curtailment did occur.

Plant Simulator is a cloud-based application that integrates with:

- Plant Optimizer, an on-premises application.
- Accuweather, a third-party API, for historic dry bulb and wet bulb temperature data.

Sharing information between Plant Optimizer and Plant Simulator

You can develop scenarios and simulations in the cloud-based Plant Simulator using the latest historical weather, load, utility pricing, and equipment performance data gathered by the on-premises Plant Optimizer. You can compare simulation results to as-run results stored in Plant Optimizer.

You can set Plant Simulator to import data from Plant Optimizer to share information. After a one-time initial large data export, Plant Optimizer exports hourly change of value (COV) data to Plant Simulator once per day.

Plant Optimizer and Plant Simulator use Oauth-based token authentication to secure communication between the tools. The steps for communication between Plant Optimizer and Plant Simulator are as follows:

- A RESTful end point is established, and a common user is created and provided to Plant Optimizer.

- Plant Optimizer connects with an Information Management System (IMS) end point, which is the same end point used by Plant Simulator for authentication, to generate an Oauth token with credentials provided by Plant Simulator.
- The Oauth token is passed with JSON data to Plant Simulator end point.
- Plant Simulator end point then validates the Oauth token and, if successful, receives the JSON data sent from Plant Optimizer.

A token is generated each time Plant Optimizer sends a data request to Plant Simulator end point. For each request from Plant Optimizer, a new Oauth token is generated to authenticate the request.

Product security processes

Johnson Controls performs internal vulnerability scanning of Plant Optimizer for each quarterly software release. We ensure all critical and high vulnerabilities are mitigated before we deploy software to a customer site. We also use a continuous improvement process to address medium and low vulnerabilities identified. Each product at Johnson Controls is required to identify a security champion responsible for compliance with cybersecurity, who has completed the required training and been approved by the Global Product Security team. The vulnerability scanning is performed by a security champion for each product and the Design for Security report is reviewed and approved by the Global Product Security governance team.

Johnson Controls also performs penetration testing on cloud-based software as a service (SaaS) products such as Plant Simulator. The penetration testing is performed by the Global Product Security Engineering and Innovation Services center of excellence, a team of highly experienced product security engineers.

Johnson Controls has a detailed action plan and governance process in place for Product Security Incident Response, including customer notification. The customer IT point of contact and contracting officer is notified immediately if Johnson Controls discovered a security breach while servicing or monitoring the customer’s on-premises software.