



**Use the OpenEdge Command Center**



# Copyright

---

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: <https://www.progress.com/legal/documentation-copyright>.

**September 2025**

**Product version:** Progress OpenEdge Command Center 2.0

**Updated:** 2025/09/04



# Table of Contents

<b>Preface.....</b>	<b>9</b>
<b>Learn about OpenEdge Command Center.....</b>	<b>11</b>
OpenEdge Command Center components.....	12
OpenEdge Command Center console dashboard.....	13
Authorization server.....	15
Roles in Authorization server.....	16
<b>Install and configure the OpenEdge Command Center server.....</b>	<b>19</b>
Launch the OpenEdge Command Center server installer.....	21
Install OpenEdge Command Center server in high availability setup.....	24
Install OpenEdge Command Center server in console mode.....	26
Silent installation of OpenEdge Command Center server.....	28
Start OpenEdge Command Center server.....	31
Uninstall OpenEdge Command Center server.....	33
Provide MongoDB package for offline installation.....	34
<b>OpenEdge Command Center server configuration.....</b>	<b>37</b>
Data store configuration file.....	38
System configuration file.....	39
Server configuration file.....	40
<b>Install and configure OpenEdge Command Center agent.....</b>	<b>43</b>
Launch the OpenEdge Command Center agent installer.....	44
Install OpenEdge Command Center agent in console mode.....	46
Silent installation of OpenEdge Command Center agent.....	47
Bootstrap policy file.....	51
Start the OpenEdge Command Center agent.....	51
Uninstall OpenEdge Command Center agents.....	52
<b>OpenEdge Command Center agent configuration.....</b>	<b>55</b>
OpenEdge Installation configuration file.....	56
Java properties file.....	56
Server information file.....	56
Agent configuration file.....	57

<b>Configure mutual TLS authentication.....</b>	<b>59</b>
---	-----------

<b>View installation log files for OpenEdge Command Center server and agent.....</b>	<b>63</b>
--	-----------

<b>Troubleshoot installation and configuration issues for OpenEdge Command Center server and agent.....</b>	<b>65</b>
---	-----------

MongoDB installation fails during OpenEdge Command Center server installation.....	66
OpenEdge Command Center server fails to start after installation.....	68
OpenEdge Command Center server or agent uninstallation fails.....	70
OpenEdge Command Center server or agent reinstallation fails after uninstallation.....	72
OpenEdge Command Center server startup failure in high availability setup.....	73

<b>How to.....</b>	<b>75</b>
--------------------	-----------

Manage services for OpenEdge Command Center server.....	77
Manage services for OpenEdge Command Center agent.....	78
Change logging level.....	79
Log in to OpenEdge Command Center.....	80
Change or reset passwords.....	82
Configure email settings.....	82
Create a new user.....	83
Edit user details.....	84
Manage OpenEdge Command Center agents.....	85
Add agent label.....	86
Update agent name and label.....	86
Search for and filter agents.....	86
Unregister an agent.....	87
Manage OpenEdge databases.....	87
Add a new OpenEdge database connection .....	88
Start or stop OpenEdge databases.....	90
Edit OpenEdge database connections.....	90
Remove OpenEdge database connections.....	91
View schema, users, and roles of a selected database.....	92
Configure and manage PAS for OpenEdge instances.....	93
Configure PAS for OpenEdge instances.....	93
Manage PAS for OpenEdge instances.....	106
Manage ABL applications, web applications, and REST services.....	110
View ABL applications across multiple PAS for OpenEdge instances.....	111
Manage ABL applications.....	112
Manage web applications.....	114

Manage REST services.....	116
Edit ABL application.....	117
Create users and manage roles using Authorization server.....	122
Log in to Authorization server.....	122
Create a user.....	123
Assign roles to a user.....	124
Remove roles from a user.....	127
Frequently Asked Questions.....	129
Set up TLS for OpenEdge Command Center and MongoDB communication.....	130
Monitor OpenEdge resources using the OpenEdge Command Center agent.....	132
Set up OpenTelemetry Collector.....	133
OpenTelemetry metrics for OpenEdge database.....	134
Enable OpenEdge Command Center agent to collect performance metrics of OpenEdge database.....	136
Sample performance metrics data for OpenEdge database.....	138
OpenTelemetry metrics for PAS for OpenEdge.....	140
Enable OpenEdge Command Center agent to collect performance metrics of PAS for OpenEdge.....	144
Sample performance metrics data for PAS for OpenEdge.....	146
Performance impact and resilience of collecting performance metrics.....	149
Reset super admin user details.....	150
<b>OpenEdge Command Center utilities.....</b>	<b>151</b>
OECCAGENT utility.....	151
OECCSERVER utility.....	152
RESETSUPERADMIN utility.....	153
<b>OpenEdge Command Center performance results.....</b>	<b>155</b>





# Preface

---

## Purpose

This manual is an introduction to the OpenEdge Command Center. It describes the installation and configuration procedures of the OpenEdge Command Center. It also describes the tasks performed by an administrator to monitor and manage OpenEdge environments using the OpenEdge Command Center.

## Audience

This manual is designed as a guide and reference for OpenEdge Administrator and technical personnel responsible for installing and configuring OpenEdge Command Center.

## Organization

- [Learn about OpenEdge Command Center](#) on page 11  
This section provides an introduction to OpenEdge Command Center and its benefits to an OpenEdge administrator.
- [Install and configure the OpenEdge Command Center server](#) on page 19  
This section provides information about the various tasks required for installing and configuring OpenEdge Command Center server.
- [OpenEdge Command Center server configuration](#) on page 37  
This section provides information about the configuration files located in the server installation directory.
- [Install and configure OpenEdge Command Center agent](#) on page 43  
This section provides information about the various tasks required for installing and configuring OpenEdge Command Center agent.
- [OpenEdge Command Center agent configuration](#) on page 55  
This section provides information about the configuration files located in the agent installation directory.
- [Configure mutual TLS authentication](#) on page 59  
This section provides information about the log files that the server and agent generate for installation or uninstallation scenarios.
- [View installation log files for OpenEdge Command Center server and agent](#) on page 63  
This section provides information about the log files that the server and agent generate for installation and uninstallation scenarios.
- [Troubleshoot installation and configuration issues for OpenEdge Command Center server and agent](#) on page 65  
This section provides information about identifying and resolving common issues that may occur during the installation of OpenEdge Command Center server and agent.
- [How to](#) on page 75  
This section provides information about the various tasks that are required to operate the OpenEdge Command Center.

- [OpenEdge Command Center utilities](#) on page 151

This section provides information about the OpenEdge Command Center utilities in alphabetical order.

- [OpenEdge Command Center performance results](#) on page 155

This section provides information about the performance results of OpenEdge Command Center under various scenarios

### **Documentation conventions**

See [Documentation Conventions](#) for an explanation of the terminology, format, and typographical conventions used throughout the OpenEdge content library.

---

# Learn about OpenEdge Command Center

---

Progress® OpenEdge® Command Center is a cloud-ready OpenEdge management console capable of managing multiple OpenEdge resources and versions across local and remote systems. The vision of OpenEdge Command Center is to offer substantial productivity gains for the day-to-day administration and management of the OpenEdge platform while providing flexibility for today's environment where system resources are volatile.

OpenEdge Command Center is a complimentary tool that supports customers using OpenEdge 12.2 or later releases. For more information about tool life cycle policy, see "OpenEdge Tool Life Cycle" in the [OpenEdge Life Cycle Guide](#). You can install OpenEdge Command Center by using separate installers available on Progress Software Download Center. To know more about installing OpenEdge Command Center, see [Install and configure the OpenEdge Command Center server](#) on page 19 and [Install and configure OpenEdge Command Center agent](#) on page 43.

OpenEdge Command Center features the latest UI and UX technologies. Currently, OpenEdge Command Center is built to effectively manage PAS for OpenEdge instances and OpenEdge databases. It aims to incrementally support everything you need to manage PAS for OpenEdge instances and databases. It simplifies the administrative overhead for system administrators by introducing lightweight agents and a centralized server, and it is designed to be highly available and extremely reliable.

OpenEdge Command Center uses open standard APIs to rapidly serve your integration use cases and provide timely information in a modern and easy-to-use interface. Intuitively designed, OpenEdge Command Center can be accessed with modern desktop or tablet-based web browsers. All the connections to the OpenEdge Command Center are secured using HTTPS, regardless of your platform.

To support your custom business needs for application integration and access, OpenEdge Command Center uses OpenAPI v3.0 REST APIs accompanied by interactive swagger documentation to help you add your own resources along the way and automate your tasks.

With the OpenEdge Command Center labeling feature, you easily manage all touch points of your PAS for OpenEdge components development pipeline from development to testing, staging, and production.

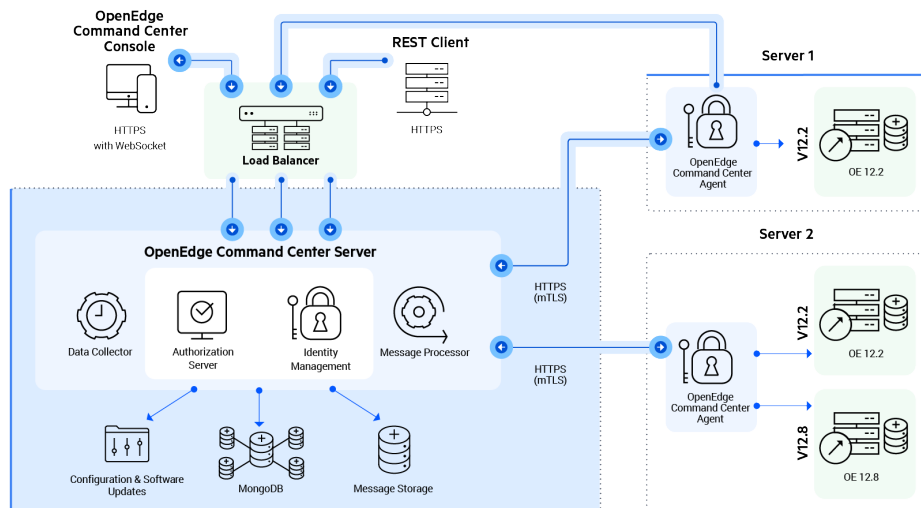
OpenEdge Command Center is composed of the OpenEdge Command Center console, the OpenEdge Command Center servers, and the OpenEdge Command Center agents.

For details, see the following topics:

- [OpenEdge Command Center components](#)
- [OpenEdge Command Center console dashboard](#)
- [Authorization server](#)

# OpenEdge Command Center components

Built for high availability, the OpenEdge Command Center server can be deployed on multiple servers, with the traffic distributed by a load balancer. Its built-in user management provides System Administrators and Application Administrators secure control of OpenEdge Command Center user permissions across all server instances. For complete resource visibility, OpenEdge Command Center offers automated component discovery for the OpenEdge version 12.2 and later releases, for all the PAS for OpenEdge deployments and OpenEdge databases.



The key components of OpenEdge Command Center are:

## OpenEdge Command Center server

The OpenEdge Command Center server powers the OpenEdge Command Center console and APIs. You can deploy the OpenEdge Command Center server as a single node or, if configured for high availability, as a multi-node cluster of OpenEdge Command Center servers. For high availability, the server works with all load balancers that support HTTPS and WebSocket (WSS) protocols, such as Nginx, AWS, ELB/ALB, and more.

## Authorization server

The Authorization server manages user access to the components of the OpenEdge Command Center, such as the OpenEdge Command Center server, OpenEdge Command Center agent, Authorization server, and their resources. It provides a framework for defining and enforcing authorization policies. For more information, see [Authorization server](#) on page 15.

## OpenEdge Command Center data store

The OpenEdge Command Center uses MongoDB as its internal configuration database that stores all the OpenEdge Command Center configurations and details of discovered OpenEdge components. When the OpenEdge Command Center server is configured for high availability, multiple server instances of OpenEdge Command Center can be linked to the same database. In event of a planned or unplanned outage of an OpenEdge Command Center server, other OpenEdge Command Center servers can balance the load without impacting the end user.

To use high availability mode, MongoDB is installed on your first node system on which you install OpenEdge Command Center server. For the subsequent nodes, you point to the data folder of the first node, meaning the MongoDB configuration is shared across all the OpenEdge Command Center servers.

---

**Note:** The terms *OpenEdge Command Center data store*, *OpenEdge Command Center database* and *MongoDB* are used interchangeably in this guide and refer to the same database component.

---

## OpenEdge Command Center agent

An OpenEdge Command Center agent is a lightweight process is co-located with your OpenEdge installation of the resources to manage. The agent has a one-to-many relationship with all your OpenEdge resources across (OpenEdge release 12.2 and later) installations on that system. Regardless of whether you have one or more OpenEdge installations on a server or host machine, you need only one installation of the OpenEdge Command Center agent. The agent is always backward compatible and can manage all versions of the OpenEdge release 12.2 and later. You can also use the OpenEdge Command Center agent to collect performance metrics of OpenEdge resources, such as OpenEdge database and PAS for OpenEdge using OpenTelemetry.

The agent initiates all the communications to an OpenEdge Command Center server, to ensure secure and protected access to the OpenEdge resources. The communication between them is through a secure, mutual TLS connection.

During the installation of the agent, you can configure the agent with the connection details of the server. The OpenEdge Command Center agent runs autonomously, monitoring OpenEdge components on its system. You need to ensure that the agent is up and running to manage OpenEdge resources on the remote system.

## Browser clients

The OpenEdge Command Center server supports the HTTPS transport protocol to facilitate a secure and reliable connection for modern desktop, tablet, or iPad web browsers. Through your web browser, you can configure and manage OpenEdge resources using the OpenEdge Command Center console.

## OpenEdge Command Center console dashboard

The OpenEdge Command Center console dashboard helps you to monitor and manage OpenEdge resources, including PAS for OpenEdge instances and OpenEdge databases. It provides an intuitive interface that includes a Getting Started video, banner notifications, and navigation bar to access the console pages. It also provides a list of newly auto-discovered OpenEdge Command Center agents, PAS for OpenEdge instances, and OpenEdge databases, and links to REST API documentation and user help resources. For more information, see [OpenEdge Command Center console dashboard](#) on page 13.

# OpenEdge Command Center console dashboard

After you log in to OpenEdge Command Center, the console **dashboard** is displayed. The dashboard is the home page and consists of the following components to help you manage the PAS for OpenEdge instances and the OpenEdge databases:

## Getting Started video

Watch the [Get started with the OpenEdge Command Center](#) video to get a high-level view of the product, to learn about the interface and its PAS for OpenEdge and OpenEdge database management features, and to learn where and how to perform the set of first-time tasks you need to complete to start using it.

## Banner notification

The top right area of the console dashboard displays banner notification, alerting you to configure email settings. As a super administrator, the first task to complete is configuring your email settings. After that is done, you can create new users, manage your OpenEdge Command Center deployments, and receive email notifications sent by OpenEdge Command Center. After you configure your email settings, this banner notification is no longer displayed.

## Discovered Resources

After you connect one or more OpenEdge Command Center agents, you can view these agents in the **Discovered Resources** panel. These agents list OpenEdge resources, such as PAS for OpenEdge instances and running OpenEdge databases, on their respective systems. As these resources are made discoverable by the agent, you can view these resources in the **Discovered Resources** panel.

If you click an agent in this panel, the **OECC Agents** page appears. For information about managing the agent from this page, see [Manage services for OpenEdge Command Center agent](#) on page 78.

Similarly, if you click an OpenEdge database or PAS for OpenEdge instance resource in this panel, the corresponding resource page appears. For information about managing the OpenEdge database, see [Manage OpenEdge databases](#) on page 87. For information about managing the PAS for OpenEdge instance, see [Configure and manage PAS for OpenEdge instances](#) on page 93.



## Quick links







The **Quick Links** panel provides instant access to:

- OpenEdge Command Center online help, which is posted on the Progress Content Portal
- Progress community help
- Public REST APIs for business application use cases
- Version and build number of OpenEdge Command Center

## Navigation bar

Running down the left side of the console is the **navigation bar**, which you can use for quick access to the following console pages:

Click . . .	. . . to display
	The OpenEdge Command Center console dashboard.
	<p>The OECC Agents page, from which you can manage agents across all of your OpenEdge deployments. Additionally, you can monitor the status of your agents (running or stopped), as well as manage the labels associated with specific agents.</p> <p>For more information about agents, see <a href="#">OpenEdge Command Center agent configuration</a> on page 55 and <a href="#">Manage services for OpenEdge Command Center agent</a> on page 78.</p>

Click . . .	. . . to display
	<p>The OpenEdge Databases page, which lists all the connected OpenEdge databases, including the automatically discovered running databases and manually added database connections. You can view the OpenEdge database details, such as name, labels, and status.</p> <p>From this page, you can add a new OpenEdge database connection, edit or remove existing OpenEdge database connections, and start or stop OpenEdge databases. For more information, see <a href="#">Manage OpenEdge databases</a> on page 87.</p>
	<p>The PAS for OpenEdge page, which lists all instances that are available from an agent. You can view the instance details, such as its name, labels, and status.</p> <p>From this page, you can create, view, start, stop, clone, and delete PAS for OpenEdge instances. You can also modify the configuration instances, monitor CPU and memory consumption by PAS for OpenEdge instance, deploy and undeploy ABL and web applications for a selected PAS for OpenEdge instance. For more information, see <a href="#">Configure and manage PAS for OpenEdge instances</a> on page 93.</p>
	<p>The ABL Applications page, from which you can view and manage ABL applications, web applications, and REST services. For more information, see <a href="#">Manage ABL applications, web applications, and REST services</a> on page 110.</p>
	<p>The users page, from which you can create and manage users and user information, such as name, email, and role for OpenEdge Command Center servers.</p> <p>For more information, see <a href="#">Create a new user</a> on page 83.</p>
	<p>The OECC system settings page, from which you can manage general settings for OpenEdge Command Center server. From this tab, you can manage OpenEdge Command Center database settings, update settings, OpenEdge Command Center agent settings, general settings, and repository settings.</p>
	<p>The email settings page, from which you can manage email notification and configuration settings. You can set the mail server host name, port, and authentication credentials.</p> <p>For more information, see <a href="#">Configure email settings</a> on page 82.</p>

## Authorization server

The Authorization server is a component within the OpenEdge Command Center server. It is responsible for managing user access to systems such as the OpenEdge Command Center server, the OpenEdge Command Center agent, and the Authorization server and their resources. It provides a framework for defining and enforcing authorization policies using Role-Based Access Control (RBAC). With RBAC, your access to the systems and their resources is determined by your assigned role. Each role comes with a predefined set of permissions that define the actions you are authorized to perform. For information about roles, see [Roles in Authorization server](#) on page 16.

The Authorization server starts automatically upon the initial startup of the OpenEdge Command Center server. Upon the startup, a set of predefined roles is provisioned within the Authorization server. These roles enforce access control for the OpenEdge Command Center server and Authorization server.

In addition, the Authorization server enforces access control for the OpenEdge Command Center agent based on its bootstrap policy. For information about the bootstrap policy, see [Bootstrap policy file](#) on page 51. Currently, the access control is applicable at the agent level. This means the users assigned with appropriate roles can access all the PAS for OpenEdge instances and OpenEdge databases that the agent manages.

The Authorization server provides user and role management capabilities. You can create users, assign roles, and remove roles in the Authorization server through Authorization server REST APIs. For more information, see [Create users and manage roles using Authorization server](#) on page 122.

## Roles in Authorization server

The Authorization server manages access control using predefined roles and policy-based roles. Each role is associated with a specific set of permissions that define the actions that a user can perform within a system.

The following table provides a brief description of predefined roles and policy-based roles in the Authorization server:

Role	Type	Description
OECC_ADMIN	Predefined	Grants access to the OpenEdge Command Center server.
AUTHZ_ADMIN	Predefined	Grants access to create users and manage roles.
AGENT_ADMIN	Predefined	Grants access to manage the AGENT_ADMIN and AGENT_RESOURCE_USER roles in the Authorization server for the OpenEdge Command Center agent.
AGENT_RESOURCE_USER	Policy-based	Grants access to all the OpenEdge resources that the OpenEdge Command Center agent manages.

### Role URN

A role Universal Resource Name (URN) identifies the roles within the Authorization server, indicating what a specific role has access to and where it is used. The Role URN format includes the resource name it represents, role name, and agent partition IDs (only when assigning roles to a user for an agent).

The following table lists roles and their corresponding URNs:

Role	Role URN
OECC_ADMIN	role:oecc/oecc_admin
AUTHZ_ADMIN	role:authz/authz_admin
AGENT_ADMIN	role:agent/<partitionid>/agent_admin
AGENT_RESOURCE_USER	role:agent/<partitionid>/agent_resource_user



---

**Note:** The agent partition ID is a unique identifier assigned to each agent. You can obtain the agent partition ID using the `Retrieve specific agent details` API on the OpenEdge Command Center server. For more information, see "Retrieve specific agent details" in *OpenEdge Command Center REST API Reference*.

---



---

# Install and configure the OpenEdge Command Center server

---

Before you install OpenEdge Command Center server, Progress recommends that you perform a set of planning tasks. These tasks include understanding the system requirements for the environment in which you plan to install OpenEdge Command Center server and determining the installation method to use.

## Supported platforms

The OpenEdge Command Center server is compatible with multiple operating system platforms. For information on supported operating system platforms, see *OpenEdge 12 Platform Compatibility Guide*.

## Installation modes

You can install the OpenEdge Command Center server in one of the following ways:

- [Launch the OpenEdge Command Center server installer](#) on page 21—Installs OpenEdge Command Center server and MongoDB in graphical user interface (GUI) mode.
- [Install OpenEdge Command Center server in high availability setup](#) on page 24—Installs additional server instances to ensure an agreed level of operational performance, usually uptime, for a higher than normal period. The additional servers use the MongoDB configuration of the first server.
- [Install OpenEdge Command Center server in console mode](#) on page 26—Installs the OpenEdge Command Center server and MongoDB in the console mode, which requires manual entry of configuration settings.
- [Silent installation of OpenEdge Command Center server](#) on page 28—Installs OpenEdge Command Center from a script, which requires a two-step process. In the first step, you run the interactive installer and record your installation choices in a response file. In the second step, you use the response file to perform non-interactive, batch-mode installations on other systems.

You can specify the mode in which you want to install OpenEdge Command Center server using `-i` option in the installation command:

- GUI or interactive mode—The installer prompts you for responses before installing.
- Console or terminal mode—The installer prompts are displayed on the console.
- Silent—The installer runs in the background without any interference with other processes. You can also record the response properties file and use it to install OpenEdge Command Center server in silent mode.

---

**Note:** If you do not specify a mode, then the installer is launched in GUI mode.

---

### Prerequisite

- Ensure that you have administrator privileges on the system where you are installing the OpenEdge Command Center server.
- Ensure that the Java Development Kit (JDK) version 17.0.3 or later is installed on your system.
- Ensure that you manually provide the MongoDB package if you are installing the server on a system where the firewall restricts the internet access. The installer cannot automatically download the package in restricted environments. For more information, see [Provide MongoDB package for offline installation](#) on page 34.

---

### Note:

- Progress recommends that you uninstall earlier versions of the OpenEdge Command Center server before installing version 2.0. Migration from OpenEdge Command Center 1.3 to 2.0 is not supported.
- The terms *OpenEdge Command Center data store*, *OpenEdge Command Center database* and *MongoDB* are used interchangeably in this chapter and refer to the same database component.
- When you are providing an installation path during the installation and configuration of the server, make sure that it does not include any of the following characters:

`* ? < > | ^ & ; ! $ ``

Also, if the path contains percent-encoded characters (such as `%20`), verify that they are valid. The installer rejects paths with prohibited characters or invalid encoding.

- When running the installer (`.bin`) from a directory other than its location, use the absolute path to the file instead of a relative path to avoid any installation errors.
  - If you encounter any issues during installation or configuration, see [Troubleshoot installation and configuration issues for OpenEdge Command Center server and agent](#) on page 65.
- 

For details, see the following topics:

- [Launch the OpenEdge Command Center server installer](#)
- [Install OpenEdge Command Center server in high availability setup](#)
- [Install OpenEdge Command Center server in console mode](#)
- [Silent installation of OpenEdge Command Center server](#)
- [Start OpenEdge Command Center server](#)

- [Uninstall OpenEdge Command Center server](#)
- [Provide MongoDB package for offline installation](#)

## Launch the OpenEdge Command Center server installer

To install the OpenEdge Command Center server, either as a standalone deployment or as a primary server in a high-availability setup, download the software image from the Progress Software Download Center and launch the installation program. The installation program installs the OpenEdge Command Center server and downloads and installs MongoDB.

---

**Note:** If the firewall on your system restricts the internet access, the installer cannot download the MongoDB package. In this case, you must manually provide the MongoDB package for installation. For more information, see [Provide MongoDB package for offline installation](#) on page 34.

---

The installation program is available for the Linux and Windows platforms, with the following installation files:

Platform	Installer file name
Windows	PROGRESS_OECC_SERVER_2.x.x_WIN_64.exe
Linux	PROGRESS_OECC_SERVER_2.x.x_LNX_64.bin

To launch the installer, you must have administrator privileges on the system where you are installing the OpenEdge Command Center server.

To install the OpenEdge Command Center server as a standalone deployment or as a primary server in a high-availability setup, complete the following steps:

1. Navigate to the directory that contains the installer file.
2. Run the installer file to launch the installation procedure. For example, on the Windows platform:

```
prompt> ./PROGRESS_OECC_SERVER_2.0.0_WIN_64.exe -r <response-filename>
```

If you use the `-r <response-filename>` startup parameter, the installer prompts you to make installation choices and records them in the specified response file after the installation completes. You can use the response file for silent installations. The inputs are recorded in the location specified by the `-r` option. If you do not provide a full path, the file is created in the same location as the executable or binary (`exe/bin`). If the `-r <response-filename>` startup parameter is not specified, the response file is not generated.

---

**Note:** By default, the installer runs in graphical mode. However, if you are running the installation on a system that does not support graphical mode, then the installation runs in console mode. The installer prompts you to make installation choices and records them after the installation is complete.

---

3. On the **Introduction** page, read the information and click **Next**.
4. On the **Host Configurations** page, enter the values in the following fields and click **Next**:
  - a. In the **Port** field, enter the port number on which the OpenEdge Command Center server runs. Its default value is 8000.
  - b. In the **Management Port** field, enter the port number on which OpenEdge Command Center agent connects to the OpenEdge Command Center server. Its default value is 8001.
  - c. The **Do not validate hostname in TLS connection (nohostverify)** checkbox is selected by default, to skip the validation of host name when establishing a connection between the OpenEdge Command Center server and the Authorization server.

---

**Note:** OpenEdge Command Center ships with default certificates for the server that do not contain valid hostname entries. As a result, if you clear this checkbox, the `nohostverify` property performs host validation, which fails with default certificates, causing:

- Failure to connect the OpenEdge Command Center server with the Authorization server.
  - Failure to start the OpenEdge Command Center server.
- 

- d. In the **Java Home Directory** field, enter the location where you installed the Java Development Kit (JDK) on your system.

---

**Note:** If the `JAVA_HOME` environment variable is already set, this field is populated by default.

---

5. On the **Install Configurations** page, enter the values in the following fields and then click **Next**:
  - a. In the **Install Directory** field, enter the installation directory path. The default installation location for the Linux platform is `/usr/oecc/server`, and that for the Windows platform is `C:\Progress\OECC\Server`.
  - b. The **Install Server as a Service** checkbox is selected by default, to install the OpenEdge Command Center server as a service, enabling you to launch OpenEdge Command Center as a service on Windows or Linux platform.

- c. The **Primary Server** checkbox is selected by default, to set the server that you are installing as either a standalone deployment or the primary server in the high-availability configuration. If you clear this checkbox, MongoDB will not be installed.
- d. In the **Data Directory** field, enter the path where the server stores its data, including the configuration files and email templates. The default data directory location for the Linux platform is `/usr/oecc/data`, and that for the Windows platform is `C:\Progress\OECC\data`.

---

**Note:** For a High Availability (HA) setup, you must enter a path on a shared file system that all servers in the HA cluster can access. This way, every server uses the same configuration and resources, which is critical for maintaining consistency and preventing failures.

---

6. Review the following information before you complete the installation, to ensure that it is correct, and then click **Install**:
  - **Product Name**—Progress OpenEdge Command Center Server.
  - **Install Directory**—Path where the OpenEdge Command Center server will be installed.
  - **Data Directory**—Path where the OpenEdge Command Center server will store the configuration files and email templates.
  - **Port**—Port where the OpenEdge Command Center server runs.
  - **Management Port**—Port where agent connects to the OpenEdge Command Center server.
  - **Java Home Directory**—Path where JDK is installed on your system.
  - **MongoDB Directory**—Path where the MongoDB database will be installed.
  - **Disk Space Information (for Installation Target)**—Amount of space required or occupied by OpenEdge Command Center server.

7. In the **Finish Installation** section, confirm the successful installation of OpenEdge Command Center server.

The OpenEdge Command Center server starts automatically if it is installed as a service. Otherwise, you must start it manually. For information on starting the server as a process, see [Start OpenEdge Command Center server](#) on page 31.

## Post-installation recommendations

After a successful installation, the following accounts are created:

- Default super admin user account to log in to the OpenEdge Command Center server.
- Built-in database user account to log in to the MongoDB.

Change the password of the default super admin user after your first login to enhance security. Also, change the default email address for creating new users. For more information, see [Log in to OpenEdge Command Center](#).

# Install OpenEdge Command Center server in high availability setup

If a system that runs the OpenEdge Command Center server becomes unavailable, installing OpenEdge Command Center in high availability setup provides failover capabilities. When OpenEdge Command Center is configured for high availability, multiple installations of the OpenEdge Command Center server can be linked by the OpenEdge Command Center database. In the event of a planned or unplanned outage of an OpenEdge Command Center server system, other OpenEdge Command Center server systems balance the load without negatively impacting on the end user as long as the OpenEdge Command Center database remains reachable.

To configure additional systems with the OpenEdge Command Center server, install the OpenEdge Command Center server on each additional system in the same way as you did for the first system. However, during installation, ensure the server is not configured as the primary server, and specify the same data directory used on the first system. The installer validates the database connection from the specified data directory and displays a warning if any errors are detected. After the validation is successful, the database connection details are retrieved automatically, simplifying the installation on the secondary systems.

---

**Note:** For a successful connection between the additional server and MongoDB, Progress recommends that you set the `dbHostNameAndPort` value in the `db-config` file to *<IP of the system hosting the primary server>:<MongoDB port>*. This file is located in the `data\conf` directory within the primary server installation directory on the system. For information on how to edit configurations, see [OpenEdge Command Center server configuration](#) on page 37.

---

## Install additional OpenEdge Command Center servers

You can install one or more additional OpenEdge Command Center servers to an existing High Availability (HA) deployment.

### Prerequisites

Before you install an additional OpenEdge Command Center server in high availability setup, ensure that the following requirements are met:

- A primary server is already installed and configured on another system.
- The data directory from the primary server is available on a shared drive that the additional servers can access with read/write permissions.
- You have the OpenEdge Command Center server installer file that was used for the earlier OpenEdge Command Center installation. For example, `PROGRESS_OECC_SERVER_2.x.x_LNX_64.bin` or `PROGRESS_OECC_SERVER_2.x.x_WIN_64.exe` for the Linux and Windows platforms, respectively.
- The Java Development Kit (JDK) version 17.0.3 or later is installed on your system.
- You have administrator privileges on the system where you are installing the OpenEdge Command Center server.

On each additional system that you want in your high-availability deployment of the OpenEdge Command Center server, perform the following steps:

1. Open a command line as a user with administrator privileges and navigate to the directory that contains the installer file. The installer files available for the platforms are as follows:



Platform	Installer file name
Windows	PROGRESS_OECC_SERVER_2.x.x_WIN_64.exe
Linux	PROGRESS_OECC_SERVER_2.x.x_LNX_64.bin

2. Run the installer file to launch the installation procedure.

The installer prompts you to make installation choices and records them after the installation is complete.

3. On the **Introduction** page, read the information and then click **Next**.
4. On the **Host Configurations** page, enter the values in the following fields and click **Next**:
  - a. In the **Port** field, enter the port number on which the OpenEdge Command Center server runs. Its default value is 8000.
  - b. In the **Management Port** field, enter the port number on which OpenEdge Command Center agent connects to the OpenEdge Command Center server. Its default value is 8001.
  - c. The **Do not validate hostname in TLS connection (nohostverify)** checkbox is selected by default, to skip the validation of host name when establishing a connection between the OpenEdge Command Center server and the Authorization server. If you clear this checkbox, the `nohostverify` property performs host validation, which fails with default certificates, causing failure in:
    - a. Connecting the OpenEdge Command Center server with the Authorization server.
    - b. Starting the OpenEdge Command Center server.
  - d. In the **Java Home Directory** field, enter the location where you installed the JDK on your system.

---

**Note:** If the `JAVA_HOME` environment variable is already set, this field is populated automatically.

---

5. On the **Install Configurations** page, enter the values in the following fields:
  - a. In the **Install Directory**, enter the installation directory path. The default installation location for the Linux platform is `/usr/oecc/server`, and that for the Windows platform is `C:\Progress\OECC\Server`.
  - b. The **Install Server as a Service** checkbox is selected by default, to install the OpenEdge Command Center server as a service, enabling you to launch OpenEdge Command Center as a service on Windows or Linux platform.
  - c. Clear the **Primary Server** checkbox that is selected by default, to set the OpenEdge Command Center server that you are currently installing as an additional server.
  - d. In the **Data Directory**, enter the path where the primary server stores its data, including the configuration files and email templates.
6. Review the following information before you complete the installation to ensure that it is correct, and then click **Install**:

- **Product Name**—Progress OpenEdge Command Center Server.
  - **Install Directory**—Path where the OpenEdge Command Center server will be installed.
  - **Data Directory**—Path where the OpenEdge Command Center server will store the configuration files and email templates.
  - **Port**—Port where the OpenEdge Command Center server runs.
  - **Management Port**—Port where OpenEdge Command Center agent connects to the OpenEdge Command Center server.
  - **Java Home Directory**—Path where JDK is installed on your system.
  - **Disk Space Information (for Installation Target)**—Amount of space required or occupied by the OpenEdge Command Center server.
7. In the **Finish Installation** section, confirm the successful installation of OpenEdge Command Center server. The OpenEdge Command Center server starts automatically if it is installed as a service. Otherwise, you must start it manually. For information on starting the server as a process, see [Start OpenEdge Command Center server](#) on page 31.

If you are using a load balancer, add the newly installed server to it so the server can handle traffic and support failover. Before proceeding, ensure that the primary server is already included in the load balancer configuration. The instructions for adding the server vary depending on the load balancer you are using. See your load balancer's documentation for detailed instructions.

## Post-installation recommendations

After a successful installation, the default super admin user account is created to log in to the OpenEdge Command Center server.

Change the password of the default super admin user after your first login to enhance security. Also, change the default email address for creating new users. For more information, see [Log in to OpenEdge Command Center](#).

# Install OpenEdge Command Center server in console mode

To install the OpenEdge Command Center server in console mode, you use the `-i console` option. The console mode provides a text-based installation process, which is suitable for systems that do not support GUI. The installation program downloads and installs both the OpenEdge Command Center server and MongoDB. Before you begin, ensure that you have administrator privileges on the target system.

---

**Note:** If the firewall on your system restricts the internet access, the installer cannot download the MongoDB package. In this case, you must manually provide the MongoDB package for installation. For more information, see [Provide MongoDB package for offline installation](#) on page 34.

---

To install the OpenEdge Command Center server in console mode on Linux, complete the following steps:

1. Open the terminal as a `root` user and navigate to the directory containing the installer file.
2. Launch the installer in console mode by running the following command:

```
prompt> ./PROGRESS_OECC_SERVER_2.0.0_LNX_64.bin -i console
```

3. In the **Introduction** section, read the information and press `ENTER`.
4. In the **Host Configurations - Port** section, either press `ENTER` to accept the default port number 8000, or type a preferred port number and press `ENTER`.
5. In the **Host Configurations - Management Port** section, either press `ENTER` to accept the default port number 8001 or type a preferred port number, and then press `ENTER`.
6. In the **NoHostVerify Configurations** section, either press `ENTER` to accept the default option 1 to skip the host name verification or type 2 to verify the host name and press `ENTER`.
7. In the **Host Configurations - Java Home Directory** section, type the path to the directory where JDK is installed and press `ENTER`.

---

**Note:** If the `JAVA_HOME` environment variable is already set, this field is populated by default.

---

8. In the **Install Configurations - Install Directory** section, either press `ENTER` to accept the default installation directory path, `/usr/oecc/server`, or type the preferred directory path and press `ENTER`.
9. In the **Install Configurations—Data Directory** section, type the data directory path and press `ENTER`.
  - If this server is the primary server, type the directory where you want to store the configuration files.
  - If this server is not the primary one, type the shared data directory path of the primary server.
10. In the **Install Configurations - Install Server as a Service** section, either press `ENTER` to accept the default option 1 to install the server as a service or type 2 to skip installing as a service and press `ENTER`.
11. In the **Install Configurations - Primary Server** section, either press `ENTER` to accept the default option 1 to install the server as a primary server or type 2 to install it as a non-primary server and press `ENTER`.
12. In the **Preview** section, review the configuration details and press `ENTER`.

After the server and MongoDB are installed, the **Installation Complete** section displays the message `Progress OpenEdge Command Center Server has been successfully installed`.

13. To exit the installer, press `ENTER`.

If the OpenEdge Command Center is installed as a service, it starts automatically. Otherwise, you must start it manually. For information on starting the server as a process, see [Start OpenEdge Command Center server](#) on page 31.

### Post-installation recommendations

After a successful installation, the following accounts are created:

- Default super admin user account to log in to the OpenEdge Command Center server.
- Built-in database user account to log in to the MongoDB.

---

**Note:** For an additional server configured for high availability, only the default super admin user account is created.

---

Change the password of the default super admin user after your first login to enhance security. Also, change the default email address for creating new users. For more information, see [Log in to OpenEdge Command Center](#).

## Silent installation of OpenEdge Command Center server

A silent installation runs the installer executable using the `-i silent -f <response-filename>` command line option. The response file is generated during an interactive installation using the `-r <response-filename>` option:

1. When you start an interactive installation using the `-r <response-filename>` option as an administrator, the data that you enter is automatically recorded in a response file. You can use this file for silent installations in the future. The inputs are recorded in the location specified by the `-r` option. If you do not provide a full path, the file is created in the same location as the executable or binary (`exe/bin`).

---

**Note:** You can generate the response file only in the GUI mode of the installer. The installer does not support recording in console mode (`-i console`).

---

2. The installation data captured in the response file is available for playback to perform a silent installation through a batch mechanism.

### Response file contents

The data captured in the `<response-filename>` file provides a detailed snapshot of the installation choices made during an interactive installation and can be used for silent installations after an interactive installation.

The `<response-filename>` file includes:

- Host configurations
- Install configurations

The following example shows an excerpt from the automatically-generated `<response-filename>` file:

```
# Mon Mar 17 22:56:37 EDT 2025
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Host Configurations
#-----
OECC_PORT=8000
OECC_MANAGEMENT_PORT=8001
OECC_NOHOST_VERIFY=1
OECC_JAVA_HOME=C:\java\jdk-17.0.3+7

#Install Configurations
#-----
USER_INSTALL_DIR=C:\Progress\OECC\server
OECC_INSTALL_AS_SERVICE=1
IS_PRIMARY_SERVER=1
OECC_DATA_DIR=C:\Progress\OECC\data
```

When you create the response file based upon the above template, enter values for the following variables within this template:

For the following variable . . .	. . . specify the following
OECC_PORT	The port number on which the OpenEdge Command Center server runs.
OECC_MANAGEMENT_PORT	The OpenEdge Command Center server management port number on which the agent connects to the server.
OECC_NOHOST_VERIFY	<p>Whether to perform the host validation when connecting the OpenEdge Command Center server with the Authorization server. The supported values are:</p> <ul style="list-style-type: none"> <li>0—The host name is validated during the mutual TLS handshake and after the installation is complete, the connection is not established automatically.</li> <li>1—The host name is not validated during the mutual TLS handshake and after the installation is complete, the connection is established automatically.</li> </ul>
OECC_JAVA_HOME	The directory that contains JDK, version 17.0.3 or later.
USER_INSTALL_DIR	<p>The directory in which you want to install the server.</p> <hr/> <p><b>Note:</b> The directory must be empty, otherwise, the installation will be terminated.</p> <hr/>
OECC_INSTALL_AS_SERVICE	<p>Whether to install the server as a service. The supported values are:</p> <ul style="list-style-type: none"> <li>0—The server is not installed as a service and not started automatically after installation is complete.</li> <li>1—The server is installed as a service and started automatically after the installation is complete.</li> </ul>

For the following variable . . .	. . . specify the following
IS_PRIMARY_SERVER	<p>Whether to install the server as an additional server. The possible values are:</p> <ul style="list-style-type: none"> <li>0—The server is installed as an additional server and MongoDB is not installed.</li> <li>1—The server is installed as a primary server and MongoDB is installed during the server installation.</li> </ul>
OECC_DATA_DIR	<p>A directory that contains the configuration information of server.</p> <hr/> <p><b>Note:</b> This directory must be empty for the primary server.</p> <hr/>

## Create the response file

You can generate a response file in two ways:

- Automatically by running the installer with the `-r <response-filename>` option during an interactive installation.
- Manually by creating or modifying a response file based on the sample template provided above.

### Note:

- You can generate the response file only in the GUI mode of the installer. The installer does not support recording in console mode (`-i console`).
- Before creating the response file, ensure that the OpenEdge Command Center server is not already installed on your system. If it is installed, uninstall it first and then proceed with creating the response file.

To create a response file:

- Open a command-line interface with administrative privileges. On Windows, run the command prompt as an administrator. On Linux, run the terminal as a root user.
- Navigate to the directory that contains the OpenEdge Command Center installer file, `PROGRESS_OECC_SERVER_2.x.x_LNX_64.bin` or `PROGRESS_OECC_SERVER_2.x.x_WIN_64.exe` for the Linux and Windows platforms, respectively.
- To record installation choices in the `<response-filename>` file:
  - For the Linux platform: `PROGRESS_OECC_SERVER_2.x.x_LNX_64.bin -r <response-filename>`
  - For the Windows platform: `PROGRESS_OECC_SERVER_2.x.x_WIN_64.exe -r <response-filename>`
- Run the OpenEdge Command Center server installer file by performing the steps in [Launch the OpenEdge Command Center server installer](#) on page 21. The `<response-filename>` file is generated, which you can rename, if necessary.

---

**Note:** You can modify the variable values in the `<response-filename>` file, but do not change the variable names.

---

## Run the silent installation

1. Open a command-line interface with administrative privileges. On Windows, run the command prompt as an administrator. On Linux, run the terminal as a root user.
2. Navigate to the directory that contains the `<response-filename>` file.
3. Enter the following command:
  - For the Linux platform: `./PROGRESS_OECC_SERVER_2.x.x_LNX_64.bin -i silent -f <response-filename>`
  - For the Windows platform: `PROGRESS_OECC_SERVER_2.x.x_WIN_64.exe -i silent -f <response-filename>`

After you enter the command, the OpenEdge Command Center server initiates silent installation without your intervention.

A log file of the installation procedure is available in the `install_logs` subdirectory of the server installation directory.

## Post-installation recommendations

After a successful installation, the following accounts are created:

- Default super admin user account to log in to the OpenEdge Command Center server.
- Built-in database user account to log in to the MongoDB.

---

**Note:** For an additional server configured for high availability, only the default super admin user account is created.

---

Change the password of the default super admin user after your first login to enhance security. Also, change the default email address for creating new users. For more information, see [Log in to OpenEdge Command Center](#).

# Start OpenEdge Command Center server

This topic explains how to start the OpenEdge Command Center server on the Windows and Linux platforms. Before starting the server, ensure that all the configurations are completed.

## Start the OpenEdge Command Center server on Windows

You can start the OpenEdge Command Center server on Windows as a service or as a process based on your configuration during the installation.

### Start the server installed as a service

To start the OpenEdge Command Center server:

1. Open the **Task Manager** on your system where the server is installed as a service using an account with administrator privileges.
2. Navigate to the **Services** tab and locate `ProgressOpenEdgeCommandCenterServer2.0` in the list.
3. To start the server that is installed as a service, right-click `ProgressOpenEdgeCommandCenterServer2.0` and click **Start**.

### Start the server installed as a process

To start the OpenEdge Command Center server:

---

**Note:** Progress recommends not to start the server as a process if you selected the **Install Server as a Service** option during installation.

---

1. Open the command shell in the **Run as administrator** mode.
2. Navigate to the directory where the server is installed.
3. To start the server that is installed as a process, type the following command:

```
oeccserver.bat start
```

To know more about the `oeccserver` utility, see [OECCSERVER utility](#).

### Start the OpenEdge Command Center server on Linux

You can start the OpenEdge Command Center server on Linux as a service or as a process based on your configuration during the installation.

---

**Note:** Do not use the `Proenv` environment command shell to start the OpenEdge Command Center server. It can result in errors.

---

### Start the server installed as a service

To start the OpenEdge Command Center server:

1. Open the Linux shell with Super User or `root` privileges.
2. To start the server that is installed as a service, type the following command:

```
systemctl start ProgressOpenEdgeCommandCenterServer2.0.service
```

### Start the server installed as a process



To start the OpenEdge Command Center server:

---

**Note:** Progress recommends not to start the server as a process if you selected the **Install Server as a Service** option during installation.

---

1. Open the Linux shell with Super User or `root` privileges.
2. Navigate to the directory where the server is installed.
3. To start the server that is installed as a process, type the following command:

```
./oeccserver start
```

To know more about the `oeccserver` utility, see [OECCSERVER utility](#).

## Uninstall OpenEdge Command Center server

On the Windows and Linux platforms, the `uninstall` executable file consolidates and formalizes the actions required to remove an OpenEdge Command Center server instance. The `uninstall` file is located in the `uninstall` subdirectory within the OpenEdge Command Center server installation directory. On Linux, a shortcut to the uninstaller is also placed in the user's home directory (`$HOME`). On Windows, the OpenEdge Command Center Server Uninstall shortcut is added to the user's **Start** menu.

### Uninstall OpenEdge Command Center server on Windows

To uninstall the OpenEdge Command Center server on the Windows platform:

1. Navigate to the `uninstall` directory and locate the `Uninstall Progress OpenEdge Command Center Server` executable file.
2. Run the `Uninstall Progress OpenEdge Command Center Server` file as an administrator.
3. Follow the instructions in the **Uninstall OpenEdge Command Center** wizard.

---

**Note:**

- During the uninstallation process, a **Delete Database** dialog appears, prompting you to confirm whether to remove the OpenEdge Command Center database. By default, the option is set to **No**. If you select **Yes**, all data of the OpenEdge Command Center server, including `oecc` collection, is removed from the database. Regardless of your choice, the database user account is deleted. However, in high availability configurations, when uninstalling an additional server that does not host the database, the database user account is not deleted.
  - For the server in high availability mode, click **Yes** only if it is the final remaining active server. If any other servers are still active, deleting the database disrupts their operations.
- 

4. After the uninstallation is complete, the **Uninstall Complete** screen displays the message: All items were successfully uninstalled. Click **Done** to exit.

Alternatively, you can uninstall the server by completing the following steps on the Windows platform:

1. Select **Start**, then choose **Settings > Apps**.
2. Scroll to and select **Progress OpenEdge Command Center Server**, then click **Uninstall**.

## Uninstall OpenEdge Command Center server on Linux

To uninstall the OpenEdge Command Center server on the Linux platform:

1. Open a command line and navigate to the `uninstall` subdirectory of the OpenEdge Command Center installation directory. For example:

```
prompt> cd /usr/oecc/server/uninstall
```

2. Enter the following command:

```
./Uninstall Progress OpenEdge Command Center Server -i mode
```

In the preceding command, *mode* represents one of the following parameters:

- `gui`—Launches the uninstaller in GUI mode and prompts you for responses before uninstalling.
- `console`—Launches the uninstaller in console mode and displays prompts in the console.
- `silent`—Launches the uninstaller in silent mode and proceeds with the uninstall using default settings without prompting for any input. Response files are not supported and will be ignored if provided.

---

### Note:

- If you do not specify a mode parameter, then the uninstaller is launched in GUI mode.
  - During the uninstallation process, whether in GUI mode or console mode, a **Delete Database** dialog appears, prompting you to confirm whether to remove the OpenEdge Command Center database. By default, the option is set to **No**. If you select **Yes**, all data of the OpenEdge Command Center server, including `oecc` collection, is removed from the database. Regardless of your choice, the database user account is deleted.
  - For the server in a high availability mode, click **Yes** only if it is the final remaining active server. If any other servers are still active, deleting the database disrupts their operations.
- 

A log file of the uninstallation process is created in the `$HOME` directory with the name `$HOME/Progress_OpenEdge_Command_Center_Server_Uninstall_mm_dd_yyyy_hh_mm_ss.log`.

## Provide MongoDB package for offline installation

When installing the OpenEdge Command Center server, the installer attempts to download the MongoDB package from the internet. In environments where the firewall restricts internet access, the installer cannot retrieve the package automatically. In the restricted environments, you must manually provide the MongoDB package for installation.

Before you begin, ensure that you have administrator privileges on the target system.

To provide the MongoDB package for offline installation, perform the following steps:

1. Download the appropriate MongoDB archive for your operating system from the official MongoDB download center.
  - For Windows, download the MongoDB `.zip` archive.
  - For Linux distribution, download the appropriate `.tgz` archive.

---

**Note:** Progress recommends downloading the latest available service pack in the MongoDB 7.x series that is appropriate for your operating system to avoid any compatibility issues during the installation.

---

2. Rename the downloaded MongoDB package, depending on your operating system:

- For Windows, rename it to `mongodb.zip`
- For Linux, rename it to `mongodb.tgz`

3. Place the package in the same directory where the server installer file is located.

When the installer is launched, it detects the MongoDB package and proceeds with server and MongoDB installation without attempting to download MongoDB from the internet. For further details on installing and configuring OpenEdge Command Center server along with MongoDB, see [Install and configure the OpenEdge Command Center server](#) on page 19.



---

# OpenEdge Command Center server configuration

---

After you install the OpenEdge Command Center server, the installer places the following configuration files in the installation directory to support the operations of server.

- Data store configuration file (`db-config.json`)
- System configuration file (`system-config.json`)
- Server configuration file (`server-config.json`)

These configuration files enable the server to manage its connection to MongoDB, control its runtime behavior, and define its operational settings. The data store `db-config.json` and system (`system-config.json`) configuration files are stored in the `data/conf` directory, while the server configuration file (`server-config.json`) is stored in the `server/conf` directory. In a High Availability (HA) setup, the files in the data directory are shared across all servers, whereas the server configuration file remains local to each server. You can modify these files to change the configuration of the OpenEdge Command Center server. However, Progress recommends retaining the default settings unless you have a specific requirement.

Before making any changes to the configuration files, stop the server if it is already running. After making the changes, restart the server to apply the changes.

For details, see the following topics:

- [Data store configuration file](#)
- [System configuration file](#)
- [Server configuration file](#)

## Data store configuration file

The data store configuration file (`db-config.json`) defines the database connection settings that the OpenEdge Command Center server uses to communicate with MongoDB.

The default location for this file on the Windows platform is `C:\Progress\OECC\data\conf`, and that for the Linux platform is `/usr/oecc/data/conf`.

The sample `db-config.json` file is as follows:

```
{
  "dbHostNameAndPort": "<host name>: <port_number>",
  "srvRecord": false,
  "connectOptions": {
    "autoIndex": true,
    "connectTimeoutMS": 10000,
    "socketTimeoutMS": 45000,
  },
  "auth": {
    "user": "username",
    "password": "password"
  },
  "authSource": "admin"
}
```

The following table describes the key attributes in the `db-config.json` file:

Attribute	Description
<code>dbHostNameAndPort</code>	Specifies the host name and port number of the MongoDB that the server connects to. If the system cannot resolve the host name, replace host name with the IP address of the system.
<code>srvRecord</code>	Indicates whether to use DNS SRV records for MongoDB connection. The default value is <code>false</code> .
<code>user</code>	Username for MongoDB authentication.
<code>password</code>	Password for MongoDB authentication. It is encrypted by default. If the MongoDB password changes, update this attribute with the cleartext password. When the server starts, the password is automatically encrypted.
<code>authSource</code>	Specifies the name of the database where the MongoDB user credentials are stored. The default value is <code>admin</code> .

**Note:** Progress recommends that you do not change the default settings in the configuration file unless you have a specific requirement.

# System configuration file

The system configuration file (`system-config.json`) defines the key system-level settings, such as logging level, setup status, and help resource links for the OpenEdge Command Center server.

The default location for this file on the Windows platform is `C:\Progress\OECC\data\conf`, and that for the Linux platform is `/usr/oecc/data/conf`.

The sample `system-config.json` configuration file is as follows:

```
{
  "loglevel": "info",
  "firstTimeSetupDone": true,
  "helpURLs": {
    "documentation":
      "https://docs.progress.com/bundle/openedge-command-center-olh/page/Learn-about-OpenEdge-Command-Center.html",

    "support": "https://www.progress.com/support/openedge",
    "community": "https://community.progress.com/s/",
    "privacy": "https://www.progress.com/legal/privacy-policy",
    "gettingStartedVideo": "https://www.youtube.com/embed/1fwRdti5QhQ",
    "faqs": "https://www.progress.com/faqs",
    "restAPI": {
      "agents":
        "https://documentation.progress.com/output/OpenEdge-Command-Center/#tag/Agent",
      "pasoe":
        "https://documentation.progress.com/output/OpenEdge-Command-Center/#tag/Progress-Application-Server",

      "database":
        "https://documentation.progress.com/output/OpenEdge-Command-Center/#tag/Database",
      "users":
        "https://documentation.progress.com/output/OpenEdge-Command-Center/#tag/Admin/paths/~ladmin~lusers/get",

      "authorizationServer":
        "https://documentation.progress.com/output/OECC/Authorization-Server-APIs/index.html#tag/Users"
    }
  }
}
```

The following table describes the attributes in the `system-config.json` file:

Attribute	Description
<code>loglevel</code>	Specifies the verbosity of server logs. The supported values are: <ul style="list-style-type: none"> <li><code>info</code></li> <li><code>debug</code></li> <li><code>warn</code></li> <li><code>trace</code></li> </ul> The default value is <code>info</code> .
<code>maxFileUploadSize</code>	Indicates the maximum file size (in bytes) that the server allows for uploads. By default, the value is set to 523,239,424 bytes (499 MB). To increase the upload limit, add the <code>maxFileUploadSize</code> attribute to this configuration file and specify the value in bytes. The maximum value you can set is 3,221,225,472 bytes (3 GB). If you set a higher value than this limit, the server automatically reverts to the maximum allowed upload size of 3,221,225,472 bytes.
<code>firstTimeSetupDone</code>	Specifies whether the initial setup is done during installation.
<code>helpURLs</code>	Provides the links to the product documentation.

**Note:** Progress recommends that you do not change the default settings in the configuration file unless you have a specific requirement.

## Server configuration file

The server configuration file (`server-config.json`) defines the configuration settings that control how the OpenEdge Command Center server operates.

The default location for this file on the Windows platform is `C:\Progress\OECC\Server\conf`, and that for the Linux platform is `/usr/oecc/server/conf`.

The sample `server-config.json` configuration file is as follows:

```
{
  "_comment": "Provide complete path for key and certificate files",
  "nodeId": "",
  "port": 8000,
  "managementPort": 8001,
  "dataDir": "",
  "security": {
    "nohostverify": true,
    "key": "${OECC_SERVER}/conf/certs/oeccserver.key",
    "keyPassPhrase": "password",
    "certificate": "${OECC_SERVER}/conf/certs/oeccserver.crt",
    "rootCA": ["${OECC_SERVER}/conf/certs/oeccrootca.crt"],
    "intermediateCerts": []
  }
}
```



The following table describes the attributes in the `server-config.json` file:

Attribute	Description
<code>nodeId</code>	Identifier for the server node.
<code>port</code>	Specifies the port number on which the OpenEdge Command Center server runs. The default value is 8000.
<code>managementPort</code>	Specifies the port number on which the OpenEdge Command Center agent connects to the OpenEdge Command Center server. The default value is 8001.
<code>dataDir</code>	Specifies the path to the server data folder. For example, <code>C:\Progress\OECC\data</code> or <code>/usr/oecc/data</code> .
<code>nohostverify</code>	<p>Controls whether the server verifies the host name during mutual TLS handshake. The default value is <code>true</code>. If you want the host name to be validated during the mutual TLS handshake, change its default value from <code>true</code> to <code>false</code>.</p> <hr/> <p><b>Note:</b> When you set <code>nohostverify</code> to <code>false</code>, it performs host validation, which fails with default certificates, resulting in failure of connection between OpenEdge Command Center server and agent. To prevent these failures, you must provide signed certificates to configure mutual TLS authentication with custom certificates, as described in <a href="#">Configure mutual TLS authentication</a> on page 59.</p> <hr/>
<code>key</code>	Specifies the path to the private key file of the server used for encryption and decryption.
<code>keyPassPhrase</code>	Specifies the password to encrypt the private key. This value is stored in an encrypted format. Similar to database password, you must provide the passphrase in cleartext during server startup. The system automatically encrypts and securely stores it upon initialization.
<code>certificate</code>	Specifies the path to the public certificate of the OpenEdge Command Center server that is signed by the root Certificate Authority (CA). For more information, see <a href="#">Configure mutual TLS authentication</a> on page 59.
<code>rootCA</code>	<p>The path to the public certificate of the signing authority. For example, <code>C:\Progress\OECC\Server\conf\certs\oeccrootca.crt</code> or <code>/usr/oecc/server/conf/certs/oeccrootca.crt</code></p> <hr/> <p><b>Note:</b> Make sure that you use a valid set of certificates which are signed by same <code>rootCA</code> at both the agent and the server side.</p> <hr/>
<code>intermediateCerts</code>	The certificate chain or the series of certificates between root CA and the public certificate of the OpenEdge Command Center server.

---

**Note:** Progress recommends that you replace the default certificates with custom certificates in production environments.

---

---

# Install and configure OpenEdge Command Center agent

---

The OpenEdge Command Center agent can be downloaded and installed independently of OpenEdge. After installing OpenEdge, use the OpenEdge Command Center agent installer to install and configure an agent on the local system to manage your OpenEdge system resources.

The OpenEdge Command Center agents are supported only on 64-bit platforms. They are supported on all operating systems that support OpenEdge 12.2 and later releases, including Windows, UNIX, Linux, and AIX, except for Solaris.

## Prerequisites

- Before you install the OpenEdge Command Center agent on a single system or network, make sure that your environment meets the hardware and software requirements described in the [OpenEdge Platform and Product Availability Guide](#) on the Progress Content Portal. You can also refer to this document for information on the compatibility of OpenEdge Command Center with OpenEdge releases.
- Ensure that the Java Development Kit (JDK) version 17.0.3 or later is installed on your system.
- Ensure that you have administrator privileges on the system where you are installing the OpenEdge Command Center agent.

**Note:**

- Progress recommends that you uninstall earlier versions of the OpenEdge Command Center agent before installing version 2.0. Migration from OpenEdge Command Center 1.3 to 2.0 is not supported.
- If you encounter any issues during installation or configuration, see [Troubleshoot installation and configuration issues for OpenEdge Command Center server and agent](#) on page 65.
- When you are providing an installation path during the installation and configuration of the agent, make sure that it does not include any of the following characters:

`* ? < > | ^ & ; ! $ ``

Also, if the path contains percent-encoded characters (such as %20), verify that they are valid. The installer rejects paths with prohibited characters or invalid encoding.

- When running the installer (.bin) from a directory other than its location, use the absolute path to the file instead of a relative path to avoid any installation errors.

For details, see the following topics:

- [Launch the OpenEdge Command Center agent installer](#)
- [Install OpenEdge Command Center agent in console mode](#)
- [Silent installation of OpenEdge Command Center agent](#)
- [Bootstrap policy file](#)
- [Start the OpenEdge Command Center agent](#)
- [Uninstall OpenEdge Command Center agents](#)

# Launch the OpenEdge Command Center agent installer

To install OpenEdge Command Center agent, download the software image from the Progress Software Download Center and launch the installation program. The installation program is available for the Linux, AIX, and Windows platforms.

**Note:** You must have administrator privileges on system to install the OpenEdge Command Center agent.

To install an agent, complete the following steps:

1. From a command window, change to the directory that contains the agent installation file. The name of the installation file is platform-dependent, as follows:

Platform	Installer file name
Windows	PROGRESS_OECC_AGENT_2.x.x_WIN_64.exe

Platform	Installer file name
Linux	PROGRESS_OECC_AGENT_2.x.x_LNX_64.bin
AIX	PROGRESS_OECC_AGENT_2.x.x_AIX_64.bin

2. Close all other applications before beginning the installation process. Other applications or tasks might interfere with the installation or use files that OpenEdge Command Center agent needs to complete the installation.
3. Change to the directory that contains the installer file.
4. Run the installer file. For example:

```
./PROGRESS_OECC_AGENT_2.x.x_WIN_64.exe
```

By default, the installer runs in graphical mode. However, if you are running the installation on a system that does not support graphical mode, then the installation runs in console mode. The installer prompts you to make installation choices and records them after the installation is complete.

5. Read the information on the **Introduction** page, verify that all the other applications are closed, and click **Next**.
6. On the **Install Configurations** page, enter the following information:
  - a) In **Install Directory**, you can optionally specify a non-default directory in which you want to install the agent. The default installation location for the Linux platform is `/usr/oecc/agent`, and that for the Windows platform is `C:\Progress\OECC\Agent`.
  - b) Keep the **Install Agent as a Service** checkbox selected, to install and automatically launch the agent as a service.
  - c) In **Java Home Directory**, specify the directory where you installed the Java Development Kit (JDK) on your system. The directory must match the one that is defined as the `JAVA_HOME` environment variable.
  - d) Click **Next**.
7. On the **Server Connection** page, you can optionally enter the following information:
  - a) In **OECC Server Host Name**, specify the name of the host system on which the OpenEdge Command Center server is running. Its default value is `localhost`.
  - b) In **OECC Server Management Port**, specify the management port value of the server. Its default value is `8001`.

---

**Note:** Optionally, you can specify it after installation by manually updating the `serverInfo.json` file. However, if you leave this field blank, a connection will not be established between the OpenEdge Command Center agent and server.

---

- c) Keep the **Do not validate hostname in TLS connection (nohostverify)** checkbox selected, to skip the validation of host name when establishing a connection between the OpenEdge Command Center server and OpenEdge Command Center agent. If you clear this checkbox, the `nohostverify` property performs host validation, which fails with default certificates, causing failure in connecting the OpenEdge Command Center server with the OpenEdge Command Center agent.
  - d) Click **Next**.

8. On the **OpenEdge Installation** page, you can optionally browse to an OpenEdge installation directory and select the instance you want to map to the agent. If an existing OpenEdge installation is detected, it is automatically populated. After you make your selection or skip this step, click **Next**.

---

**Note:** You can add only one OpenEdge installation from this page. If you want to add multiple installations, then add their respective paths to the `conf/installationsInfo.json` file. For more information about the file, see [OpenEdge Installation configuration file](#) on page 56.

---

9. On the **Preview** page, review the following information you have provided before completing the installation and click **Install**.

- **Product Name**—Progress OpenEdge Command Center Agent.
- **Install Directory**—Path where the OpenEdge Command Center agent will be installed.
- **Java Home Directory**—Location where JDK is installed on your system.
- **OECC Server Host Name**—Name of the host machine on which the OpenEdge Command Center server is running.
- **OECC Server Management Port**—Port where the OpenEdge Command Center agent connect to the OpenEdge Command Center server.
- **OpenEdge Installation Directory**—Location where OpenEdge is installed on your system.
- **Disk Space Information (for Installation Target)**—Amount of space required or occupied by the OpenEdge Command Center agent.

The **Install Complete** section indicates the successful installation of the OpenEdge Command Center agent.

10. To complete the agent installation, click **Done**.

The OpenEdge Command Center agent starts automatically if it is installed as a service. Otherwise, you must start it manually. For information on starting the agent as a process, see [Start the OpenEdge Command Center agent](#) on page 51.

## Install OpenEdge Command Center agent in console mode

To install the OpenEdge Command Center agent in console mode, you use `-i console` option. The console mode provides a text-based installation process, which is suitable for systems that do not support GUI.

Before you begin, ensure that you have administrator privileges on the target system.

To install the OpenEdge Command Center agent in console mode on UNIX or Linux, complete the following steps:

1. Open the terminal as a `root` user and navigate to the directory containing the installer file.
2. Run the installer in console mode:

```
prompt> ./PROGRESS_OECC_AGENT_2.0.0_LNX_64.bin -i console
```

3. In the **Introduction** section, read the information and press `ENTER`.
4. In the **Install Configurations - Agent Installation Directory** section, either press `ENTER` to accept the default installation directory path, `/usr/oecc/agent` or type a preferred directory path and press `ENTER`.
5. In the **Host Configurations - Java Home Directory** section, type the path to the directory where the JDK is installed and press `ENTER`.
6. In the **Install Configurations - Install Agent as a Service** section, either press `ENTER` to accept the default option 1 to install the agent as a service or type 2 to skip and press `ENTER`.
7. In the **Server Connection** section, do the following:
  1. **OECC Server Host Name:** Type the host name of the server.
  2. **OECC Server Management Port:** Press `ENTER` to accept the default server management port 8001 or type the preferred port and press `ENTER`.
8. In the **Server Connection NoHostVerify** section, press `ENTER` to accept the default option 1 to skip the host name verification or type 2 to verify the host name and press `ENTER`.
9. In the **OpenEdge Installation** section, type path to the directory where OpenEdge is installed and press `ENTER`.
10. In the **Preview** section, review the configuration details and press `ENTER`.
11. After the agent is installed, the **Installation Complete** section displays the message `Progress OpenEdge Command Center Agent has been successfully installed.` Press `ENTER` to exit the installer.

The OpenEdge Command Center agent starts automatically if it is installed as a service. Otherwise, you must start it manually. For information on starting the agent as a process, see [Start the OpenEdge Command Center agent](#) on page 51.

## Silent installation of OpenEdge Command Center agent

A silent installation performs an installation by running the installer executable using the `-i silent -f <response-filename>` command line option. The response file is generated during an interactive installation using the `-r <response-filename>` option:

1. When you start an interactive installation using the `-r <response-filename>` option as an administrator, the data that you enter is automatically recorded in a response file, which you can use for silent installations in the future. The inputs are recorded in the location specified by the `-r` option. If you do not provide a full path, the file is created in the same location as the executable or binary (`exe/bin`).

---

**Note:** You can generate the response file only in the GUI mode of the installer. The installer does not support recording in console mode (`-i console`).

---

2. The installation data captured in the response file becomes available for playback to perform a silent installation through a batch mechanism.

### Response file template

The data captured in the `<response-filename>` file provides a detailed snapshot of the installation choices made during an interactive installation and can be used for silent installations after an interactive installation.

The `<response-filename>` file includes the following details:

- Install configurations
- Server connection
- OpenEdge installation

The following code snippet provides a template for creating an agent silent installation script.

```
# Mon Mar 17 23:12:35 EDT 2025
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Install Configurations
#-----
USER_INSTALL_DIR=C:\\Progress\\OECC\\agent
OECC_JAVA_HOME=C:\\java\\jdk-17.0.3+7
OECC_AGENT_AS_SERVICE=1

#Server Connection
#-----
SERVER_HOST_NAME=localhost
SERVER_PORT=8001
AGENT_NOHOST_VERIFY=1

#OpenEdge Installation
#-----
OE_INSTALL_DIR_1=C:\\Progress\\OpenEdge
```

When you create the response file based upon the template, enter values for the following variables within this template:

For the following variable . . .	. . . specify the following
USER_INSTALL_DIR	The directory in which you want to install the agent. Note that the directory must be empty, otherwise installation is terminated
OECC_AGENT_AS_SERVICE	Whether to install the agent as a service. The possible values are: <ul style="list-style-type: none"> <li>• 0—The agent is neither installed as service nor installed automatically after upon completion of installation.</li> <li>• 1—The agent is started as a service automatically upon the completion of installation.</li> </ul>
OECC_JAVA_HOME	The directory that contains the JDK, which must be version 17.0.3 or later.
SERVER_HOST_NAME	The IP address of the OpenEdge Command Center server.



For the following variable . . .	. . . specify the following
SERVER_PORT	The OpenEdge Command Center server port number.
AGENT_NOHOST_VERIFY	<p>Whether to perform the host validation when connecting the OpenEdge Command Center server with the OpenEdge Command Center agent. The possible values are:</p> <ul style="list-style-type: none"> <li>0—The host name is validated during the mutual TLS handshake and after the installation is complete, the connection is not established automatically.</li> <li>1—The host name is not validated during the mutual TLS handshake and after the installation is complete, the connection is established automatically.</li> </ul>
OE_INSTALL_DIR_1	(Optional) A directory that contains an OpenEdge installation.

## Create the response file

You can generate a response file in two ways:

- Automatically by running the installer with the `-r <response-filename>` option during an interactive installation.
- Manually by creating or modifying a response file based on the sample template provided above.

---

### Note:

- You can generate the response file only in the GUI mode of the installer. The installer does not support recording in console mode (`-i console`).
  - Before creating the response file, ensure that the OpenEdge Command Center agent is not already installed on your system. If it is installed, uninstall it first and then proceed with creating the response file.
- 

To create a response file:

- Open a command-line interface with administrative privileges. On Windows, run the command prompt as an administrator. On Linux, run the terminal as a root user.
- Change to the directory that contains the OpenEdge Command Center agent installer file for your operating system:
  - Windows: `PROGRESS_OECC_AGENT_2.x.x_WIN_64.exe`
  - Linux: `PROGRESS_OECC_AGENT_2.x.x_LNX_64.bin`
  - AIX: `PROGRESS_OECC_AGENT_2.x.x_AIX_64.bin`
- Enter the following command to record installation choices in the `<response-filename>` file:

- Windows:

```
PROGRESS_OECC_AGENT_2.x.x_WIN_64.exe -r <response-filename>
```

- Linux:

```
./PROGRESS_OECC_AGENT_2.x.x_LNX_64.bin -r <response-filename>
```

- AIX:

```
./PROGRESS_OECC_AGENT_2.x.x_AIX_64.bin -r <response-filename>
```

4. Run the installer for OpenEdge Command Center agent by performing the steps in the [Launch the OpenEdge Command Center agent installer](#) on page 44. The <response-filename> file is generated. You can rename the file if necessary.

---

**Note:** You can modify the variable values in the <response-filename> file, but do not change the variable names.

---

### Run the silent installation

To run a silent installation of the agent:

1. Open a command window and change to the directory that contains the silent installation response file.
2. Enter the following command:

- Windows:

```
PROGRESS_OECC_AGENT_2.x.x_WIN_64.bin -i silent -f response-file-name
```

- Linux:

```
./PROGRESS_OECC_AGENT_2.x.x_LNX_64.bin -i silent -f response-file-name
```

- AIX:

```
./PROGRESS_OECC_AGENT_2.x.x_AIX_64.bin -i silent -f response-file-name
```

After you enter the command, the agent installation runs without intervention. A log file of the installation procedure is available in the `install_logs` subdirectory of the agent installation directory.

## Bootstrap policy file

The bootstrap policy file is a JSON configuration file in the `conf` directory. It defines default resources, policies, roles, and user role assignments for an OpenEdge Command Center agent. When the agent starts for the first time, it sends the bootstrap policy to the OpenEdge Command Center server. The server then applies the policy in the Authorization server for policy enforcement. For more information, see [Authorization server](#).

---

**Note:** Progress recommends that you do not change the default settings in the configuration file.

---

## Start the OpenEdge Command Center agent

This topic explains how to start the OpenEdge Command Center agent on the Windows platform and the UNIX or Linux platform. Before starting the agent, ensure that all the configurations are completed.

### Start the OpenEdge Command Center agent on Windows

You can start the OpenEdge Command Center agent on Windows as a service or as a process based on your configuration during the installation.

#### Start the agent installed as a service

To start the OpenEdge Command Center agent:

1. Open the **Task Manager** on your system where the agent is installed as a service using an account with administrator privileges.
2. To start the agent that is installed as a service, right-click on `ProgressOpenEdgeCommandCenterAgent2.0` and click **Start**.

#### Start the agent installed as a process

To start the OpenEdge Command Center agent:

---

**Note:** Progress recommends not to start the agent as a process if you selected the **Install Agent as a Service** option during installation.

---

1. Open a command shell in the **Run as Administrator** mode.
2. Navigate to the directory where the `oeccagent.bat` file is located.
3. Type the following command and press `ENTER`:

```
<directory_path> > oeccagent.bat start
```

For example: `C:\Progress\OECC\Agent > oeccagent.bat start`. Where `C:\Progress\OECC\Agent` is the path where the `oeccagent.bat` file is located.

---

**Note:** Do not use the Proenv environment command shell to start the OpenEdge Command Center agent. It can result in errors.

---

## Start the OpenEdge Command Center agent on UNIX

You can start the OpenEdge Command Center agent on UNIX or Linux as a service or as a process based on your configuration during the installation.

---

**Note:** Do not use the Proenv environment command shell to start the OpenEdge Command Center agent. It can result in errors.

---

### Start the agent installed as a service

To start the OpenEdge Command Center agent:

1. Open the UNIX shell with Super User or `root` privileges.
2. To start the agent that is installed as a service, type the following command:

- On UNIX or Linux:

```
systemctl start ProgressOpenEdgeCommandCenterAgent2.0.service
```

- On AIX

```
startsrc -e "OECC_AGENT=\"$OECC_AGENT\" " -s ProgressOECCAgent2.0
```

### Start the agent installed as a process

To start the OpenEdge Command Center agent on the UNIX platform:

---

**Note:** Progress recommends not to start the agent as a process if you selected the **Install Agent as a Service** option during installation.

---

1. Open the UNIX shell with Super User or **root** privileges.
2. Navigate to the directory where the OpenEdge Command Center agent is installed.
3. Start the OpenEdge Command Center agent. For example:

```
./oeccagent start
```

To know more about the `oeccagent` utility, see [OECCAGENT utility](#).

## Uninstall OpenEdge Command Center agents

The `uninstall` executable file consolidates and formalizes the actions required to remove an OpenEdge Command Center agent instance. The `uninstall` file is located in the `uninstall` subdirectory of the agent installation directory.

## Uninstall OpenEdge Command Center agent on Windows

To uninstall the OpenEdge Command Center agent on the Windows platform:

1. Navigate to the uninstall directory and locate the `Uninstall Progress OpenEdge Command Center Agent` executable file.
2. Run the `Uninstall Progress OpenEdge Command Center Agent` file as an administrator.
3. Follow the **Uninstall OpenEdge Command Center** wizard.
4. After the uninstallation is complete, the **Uninstall Complete** screen displays the message: All items were successfully uninstalled. Click **Done** to exit.

On Windows platforms, you can also uninstall the agent by completing the following steps:

1. Select the **Start** button, then choose **Settings > Apps**.
2. Scroll to and select **Progress OpenEdge Command Center Agent**, then click **Uninstall**.

After you uninstall the agent, it still remains listed on the **Discovered Resources** panel and on the **OECC Agents** page with a status as `OFFLINE`. To completely remove the agent, you must manually delete its entry from the **OECC Agents** page. For details, see [Unregister an agent](#).

## Uninstall OpenEdge Command Center agent on UNIX

To uninstall the OpenEdge Command Center agent on the UNIX platform:

1. Open a command window and change to the `uninstall` subdirectory of the agent installation directory. For example:

```
prompt> cd /usr/oecc/agent/uninstall
```

2. To uninstall the OpenEdge Command Center agent, type the following command:

- On UNIX or Linux:  

```
./Uninstall Progress OpenEdge Command Center Agent -i mode
```
- On AIX  

```
./Uninstall_Progress_OpenEdge_Command_Center_Agent -i mode
```

In the preceding command, *mode* represents one of the following parameters:

- `gui`—Launches the uninstaller in GUI mode and prompts you for responses before uninstalling.
- `console`—Launches the uninstaller in console mode and displays prompts in the console.
- `silent`—Launches the uninstaller in silent mode and proceeds with the uninstall using default settings without prompting for any input. Response files are not supported and will be ignored if provided.

After you uninstall the agent, it still remains listed on the **Discovered Resources** panel and on the **OECC Agents** page with a status as `OFFLINE`. To completely remove the agent, you must manually delete its entry from the **OECC Agents** page. For details, see [Unregister an agent](#).

A log file of the uninstallation process is created in the `$HOME` directory with the name `$HOME/Progress_OpenEdge_Command_Center_Agent _Uninstall_mm_dd_yyyy_hh_mm_ss.log`.

---

### Note:

- If the agent was installed silently, then by default the uninstall process also runs silently.
-



---

# OpenEdge Command Center agent configuration

---

After you install the OpenEdge Command Center agent, the installer places the following configuration files in the installation directory to support agent operations:

- OpenEdge installation configuration file (`installationsInfo.json`)
- Java properties file (`java.properties`)
- Server information file (`serverInfo.json`)
- Agent configuration file (`agentConfig.json`)

These files enable the agent to manage OpenEdge installations, use the Java runtime environment to start and perform its runtime functions, connect with the server, and securely exchange data using TLS settings and certificate-based authentication.

The default location for these files on the Windows platform is `C:\Progress\OECC\Agent\conf`, and that for the Linux platform is `/usr/oecc/agent/conf`. You can modify these files to change the configuration of the OpenEdge Command Center agent. However, Progress recommends retaining the default settings unless you have a specific requirement.

Before making any changes to the configuration files, stop the agent if it is already running. After making the changes, restart the agent to apply the changes.

After you configure the agents, the agent information is available on the **OECC Agents** page. The OpenEdge databases and PAS for OpenEdge instances associated with the agent are discovered and listed on the dashboard.

For details, see the following topics:

- [OpenEdge Installation configuration file](#)

- [Java properties file](#)
- [Server information file](#)
- [Agent configuration file](#)

## OpenEdge Installation configuration file

The OpenEdge installation configuration file (`installationsInfo.json`) specifies the paths to the OpenEdge installations. These paths enable the agent to locate and identify OpenEdge components, such as OpenEdge databases and PAS for OpenEdge instances.

The default location for this file on the Windows platform is `C:\Progress\OECC\Agent\conf`, and that for the Linux platform is `/usr/oecc/agent/conf`.

The sample `installationsInfo.json` file is as follows:

```
{
  "_comment": "Provide OpenEdge complete installation path details. Add any number of
OpenEdge installation entries if required.
In Windows, please escape backslashes for path. Example: C:\\Progress\\OpenEdge",
  "installations": [{
    "path": "C:\\Progress\\OpenEdge"
  }]
}
```

## Java properties file

The Java properties file (`java.properties`) specifies the path to the Java Development Kit (JDK) that the OpenEdge Command Center agent uses to start and perform its runtime functions.

The default location for this file on the Windows platform is `C:\Progress\OECC\Agent\conf`, and that for the Linux platform is `/usr/oecc/agent/conf`.

The sample `java.properties` file is as follows:

```
#Sat Aug 02 20:26:16 IST 2025
JAVA_HOME=C:\Java\jdk-17
```

## Server information file

The server information file (`serverInfo.json`) specifies the host and management port details of the OpenEdge Command Center server that the agent uses to establish communication.

The default location for this file on the Windows platform is `C:\Progress\OECC\Agent\conf`, and that for the Linux platform is `/usr/oecc/agent/conf`.



The sample `serverInfo.json` file is as follows:

```
{
  "_comment" : "Provide OpenEdge Command Center Server url",
  "host" : "localhost",
  "managementPort" : "8001"
}
```

- `host`—Name or IP address of the host machine on which the OpenEdge Command Center server is running. In case of a High Availability (HA) setup, use the load balancer host name or IP address.
- `managementPort`— Port on which the OpenEdge Command Center server is running. The default value is 8001.

## Agent configuration file

The agent information file (`agentConfig.json`) defines the Transport Layer Security (TLS) configuration settings required for secure communication between the OpenEdge Command Center agent and the OpenEdge Command Center server.

The default installation location for this file on the Windows platform is `C:\Progress\OECC\Agent\conf`, and that for the Linux platform is `/usr/oecc/agent/conf`.

The sample `agentConfig.json` file is as follows:

```
{
  "_comment" : "Provide the TLS configuration details which are used to connect to Servers",
  "tsPassPhrase" : "encl:qd5MsIkhdHegD+c7cIsvt3OagtRnxHdfco/sY1PjgYE=",
  "ksPassPhrase" : "encl:i9AmubUlVUCuBu8ZZZUtswiXf67AUPCSXFIY7AitUTE=",
  "pKeyAlias" : "agentKeyPair",
  "rootCAAlias" : "rootCA",
  "nohostverify" : true
}
```

The following table describes the attributes in the `agentConfig.json` file:

Attribute	Description
<code>tsPassPhrase</code>	The encrypted form of password to access the trust store. It is autogenerated and cannot be modified.
<code>ksPassPhrase</code>	The encrypted form of password to access the keystore. It is autogenerated and cannot be modified.
<code>pKeyAlias</code>	The identity of the private key inside the keystore
<code>rootCAAlias</code>	The identity of the root Certificate Authority inside the trust store.
<code>nohostverify</code>	<p>Controls whether the server verifies the host name during mutual TLS handshake. The default value is <code>true</code>. If you want the host name to be validated during the mutual TLS handshake, change its default value from <code>true</code> to <code>false</code>.</p> <hr/> <p><b>Note:</b> When you set <code>nohostverify</code> to <code>false</code>, it performs host validation, which fails with default certificates, resulting in failure of connection between OpenEdge Command Center server and agent. To prevent these failures, you must provide signed certificates to configure mutual TLS authentication with custom certificates, as described in <a href="#">Configure mutual TLS authentication</a> on page 59.</p> <hr/>

**Note:** Progress recommends that you replace the default certificates with custom certificates in production environments.

## Configure mutual TLS authentication

---

When you install the OpenEdge Command Center server and OpenEdge Command Center agent on a Windows or Linux platform, mutual TLS authentication is configured with default certificates. You can configure mutual TLS authentication with your signed certificates.

---

**Note:** Progress recommends using only valid TLS certificates issued by a trusted certificate authority for production environments in OpenEdge Command Center. The `nohostverify` switch is intended for convenience and you must use it only as a temporary measure during development.

---

Before you begin, ensure that you have administrator privileges.

### Configure mutual TLS authentication with custom certificates

To configure mutual TLS authentication with your signed certificates, perform the following steps:

### 1. Configure the OpenEdge Command Center agent to use your signed certificates:

- a. Stop the agent.
- b. Run the following command by providing values for `pKeyAlias`, `pKeyPath`, `certPath`, `rootCAAlias` and `rootCAPath`.

```
java -jar <Agent_Root_Directory>\install\installer-util-2.0.0.jar  
fileName=agentConfig pKeyAlias=<key alias> pKeyPath=<key path> certPath=<.crt  
path> rootCAAlias=<ca alias> rootCAPath=<root ca .crt path>
```

where:

- `pKeyAlias`: Alias for the agent private key.
- `pKeyPath`: Path to the private key file for the agent.
- `certPath`: Path to the certificate file for the agent.
- `rootCAAlias`: Alias for the root CA certificate.
- `rootCAPath`: Path to the root CA certificate file. It must be the same root CA that signed the server certificate.

- c. Restart the agent.

### 2. Configure the OpenEdge Command Center server to use your signed certificates:

- a. Stop the server.
- b. Navigate to the `<Server_Install_Directory>\conf\certs` for Windows or `<Server_Install_Directory>/conf/certs` for Linux.
- c. Add the server certificate files.
- d. Navigate to the `server-config.json` file located in `<Server_Install_Directory>\conf` for Windows or `<Server_Install_Directory>/conf` for Linux, and then open the file.
- e. Update any or all the values for the following attributes in the `server-config.json` file:
  - `key`: Path to the private key file for the server.
  - `keyPassPhrase`: Passphrase for the private key.
  - `certificate`: Path to the public certificate for the server, signed by the root CA.
  - `rootCA`: Path to the root CA certificate.

For more details about attribute descriptions and file structure, see [Server configuration file](#) on page 40.

- f. Restart the server.

Mutual TLS authentication is configured with signed certificates provided by you.

---

## Reset mutual TLS authentication to use default certificates

To reset mutual TLS authentication to use the default certificates, perform the following steps:

1. Restore default certificates on the OpenEdge Command Center agent:

- a. Stop the agent.
- b. Run the following command:

```
java -jar <Agent_Root_Directory>\install\installer-util-2.0.0.jar  
fileName=agentConfig
```

- c. Restart the agent.

2. Restore default certificates on the OpenEdge Command Center server:

- a. Stop the server.
- b. Navigate to the `orig/certs` folder and copy the default certificates from the folder to the `conf/certs` folder:
  - On Windows, copy certificates from `<Server_Install_Directory>\orig\certs` to `<Server_Install_Directory>\conf\certs`.
  - On Linux, copy certificates from `<Server_Install_Directory>/orig/certs` to `<Server_Install_Directory>/conf/certs`.
- c. Navigate to the `server-config.json` file located in `<Server_Install_Directory>\conf` for Windows or `<Server_Install_Directory>/conf` for Linux, and then open the file.
- d. Update the values of the attributes you previously modified in the `server-config.json` file to their default values. For more details about attribute descriptions and file structure, see [Server configuration file](#) on page 40.
- e. Restart the server.

The configuration of mutual TLS authentication with signed certificates provided by you is reset to the one with default certificates. The `nohostverify` property is also set to its default value of `true`.



---

## View installation log files for OpenEdge Command Center server and agent

---

The installer—whether for the OpenEdge Command Center server or OpenEdge Command Center agent—generates log files in different locations depending on the installation or uninstallation scenario. These log files provide details about installation and uninstallation activities, including any errors or warnings that occur during the process.

The following directories are specified in the log file paths. These locations vary based on the installation settings and the operating system environment.

- `USER_INSTALL_DIR`: The installation directory specified by you during the installation process.
- `HOME`: The home directory of your operating system. On Windows, it is `C:/Users/<username>` and on Linux, it is `/home/<username>`.

### Log file locations

The following table lists the log file locations for different installation and uninstallation scenarios.

**Note:** The log file locations for installation are the same for both the OpenEdge Command Center server and agent. However, the uninstallation log file location differs for the server and agent.

Operation type	Log file location	Description
GUI/Console installation	\$USER_INSTALL_DIR/install_logs/ Install_mm_dd_yyyy_hh_mm_ss.log	Logs events during installation.
Silent installation	\$USER_INSTALL_DIR/install_logs/ Install_mm_dd_yyyy_hh_mm_ss.log	Logs events during silent installation.
	\$HOME/oecc_silent_install.log	Logs errors if the installation fails due to pre-validation conditions.
Uninstallation	<ul style="list-style-type: none"> <li>For server: \$HOME/Progress_OpenEdge_Command_Center_Server_Uninstall_mm_dd_yyyy_hh_mm_ss.log</li> <li>For agent: \$HOME/Progress_OpenEdge_Command_Center_Agent_Uninstall_mm_dd_yyyy_hh_mm_ss.log</li> </ul>	Logs events during uninstallation in this directory. The USER_INSTALL_DIR directory is removed during uninstallation.



## Troubleshoot installation and configuration issues for OpenEdge Command Center server and agent

---

This chapter explains how to identify and resolve common issues that may occur during the installation, startup, and uninstallation of the OpenEdge Command Center server and agent. It is organized into individual scenarios, each describing a specific issue, its possible causes, and recommended solutions to help you diagnose and resolve issues efficiently.

For details, see the following topics:

- [MongoDB installation fails during OpenEdge Command Center server installation](#)
- [OpenEdge Command Center server fails to start after installation](#)
- [OpenEdge Command Center server or agent uninstallation fails](#)
- [OpenEdge Command Center server or agent reinstallation fails after uninstallation](#)
- [OpenEdge Command Center server startup failure in high availability setup](#)

## MongoDB installation fails during OpenEdge Command Center server installation

This topic describes how to troubleshoot the MongoDB installation failures that may occur during the installation of the OpenEdge Command Center server. It outlines common causes and provides recommended solutions to help you complete the installation successfully.

Possible Cause	Recommended Solution
Network connectivity issue	<ol style="list-style-type: none"><li>1. Ensure that the server is connected to a stable internet network.</li><li>2. Ping a public domain (for example, google.com) to verify connectivity.</li></ol>
MongoDB download URL is invalid or unreachable	<ol style="list-style-type: none"><li>1. Navigate to the installation log directory at <code>&lt;Server_Installed_Dir&gt;/install_logs/</code>, and open the <code>Install_&lt;MM_DD_YYYY_H_M_S&gt;.log</code> log file.</li><li>2. Copy the MongoDB download URL and test it in browser or use a command-line tool such as <code>wget</code> or <code>curl</code>.</li><li>3. If the URL is not reachable:<ul style="list-style-type: none"><li>• Check if firewall or proxy settings are not blocking outbound connections to MongoDB's download servers.</li><li>• Configure proxy settings in your environment if a corporate proxy or firewall restricts access to external resources.</li></ul></li></ol>
System does not have sufficient available disk space	Ensure that at least 2 GB of free disk space is available on your system to install the OpenEdge Command Center server and MongoDB.
Installer lacks write permissions to the installation directory	Ensure that the installer has write permissions to the installation directory.

Possible Cause	Recommended Solution
Download failure not related to network	<ol style="list-style-type: none"><li>1. Download the appropriate MongoDB archive for your operating system from the official MongoDB download center.<ul style="list-style-type: none"><li>• For Windows, download the MongoDB .zip archive.</li><li>• For Linux distribution, download the appropriate MongoDB .tgz archive.</li></ul><hr/><b>Note:</b> Progress recommends downloading the latest available service pack in the MongoDB 7.x series that is appropriate for your operating system. to avoid any compatibility issues during the installation.<hr/><ol style="list-style-type: none"><li>2. Rename the downloaded MongoDB package, depending on your operating system:<ul style="list-style-type: none"><li>• For Windows, rename it to mongodb.zip</li><li>• For Linux, rename it to mongodb.tgz</li></ul></li><li>3. Place it in the same directory as the installer executable (.exe or .bin) directory. For more information, see <a href="#">Provide MongoDB package for offline installation</a> on page 34.</li><li>4. Install the OpenEdge Command Center server. For more information, see <a href="#">Install and configure the OpenEdge Command Center server</a> on page 19.</li></ol></li></ol>

## OpenEdge Command Center server fails to start after installation

This topic describes how to troubleshoot the case where the OpenEdge Command Center server does not start after a successful installation. It outlines common causes and provides recommended solutions to help you start the OpenEdge Command Center server.

Possible Cause	Recommended Solution
Unknown error during installation or startup.	<ol style="list-style-type: none"><li>1. Navigate to the installation log directory at <code>&lt;Server_Installed_Dir&gt;/install_logs/</code>, and open the <code>Install_&lt;MM_DD_YYYY_H_M_S&gt;.log</code> log file.</li><li>2. Review the log file for any errors or failures related to MongoDB startup.</li></ol>
Certificate validation failure due to invalid host information in certificates.	<ol style="list-style-type: none"><li>1. Navigate to the installation log directory at <code>&lt;Server_Installed_Dir&gt;/install_logs/</code>, and open the <code>Install_&lt;MM_DD_YYYY_H_M_S&gt;.log</code> log file.</li><li>2. Review the log file for any <code>nohostverify</code> errors. If the log contains an error about connection failure to the Authorization server with host validation, then the certificates used for secure communication do not have valid host information.</li><li>3. Navigate to the <code>&lt;Server_Installed_Dir&gt;/conf/server-config.json</code> file and update the value of <code>nohostverify</code> flag to <code>true</code>.</li></ol>
No permission to data directory in multi-node setup.	Ensure that all the non-primary OpenEdge Command Center servers have permissions to the <code>data</code> directory on the system where the primary server is installed.

## **OpenEdge Command Center server or agent uninstallation fails**

This topic describes how to troubleshoot the case where the uninstallation of the OpenEdge Command Center server or agent fails. It outlines common causes and provides recommended solutions to help you complete the uninstallation successfully.

Possible Cause	Recommended Solution
Residual product entries remain in the configuration file (.com.zerog.registry.xml).	<ol style="list-style-type: none"> <li>Navigate to the following file location: <ul style="list-style-type: none"> <li>On Windows, C:\Program Files\Zero G Registry\.com.zerog.registry.xml</li> <li>On Linux, /var/.com.zerog.registry.xml</li> </ul> <hr/> <p><b>Note:</b> The .com.zerog.registry.xml is a hidden file. Enable viewing hidden files to view this file if needed.</p> <hr/> </li> <li>Open the file, check for the entries related to the OpenEdge Command Center server or agent you want to uninstall, and delete them. <hr/> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>Progress recommends taking the backup of the .com.zerog.registry.xml file before making any changes to it.</li> <li>Do not modify or delete entries for other products, as this file contains configuration data of multiple products.</li> </ul> <hr/> </li> </ol>
Windows registry still contains OpenEdge Command Center server or agent entries.	<ol style="list-style-type: none"> <li>Open the Registry Editor (regedit.exe).</li> <li>Navigate to the Uninstall directory: <pre>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall</pre> </li> <li>Check for any folders related to the OpenEdge Command Center server or agent and delete only those specific folders.</li> </ol>
Data and database folders of the primary OpenEdge Command Center server are not removed.	<p>If uninstalling the primary server, delete the Data and database folders located parallel to the Server installation directory.</p> <hr/> <p><b>Note:</b> Perform this step only if you are certain that the server is the primary one, as these folders may contain data of other servers in a High Availability (HA) setup.</p> <hr/>

## OpenEdge Command Center server or agent reinstallation fails after uninstallation

This topic describes how to troubleshoot the case where the installation of the OpenEdge Command Center server or agent installation fails after successful uninstallation. It outlines the common cause and provides recommended solutions to help you complete the installation successfully.

Possible Cause	Recommended Solution
Residual product information remains after uninstallation.	<ol style="list-style-type: none"><li>1. Navigate to the following file location:<ul style="list-style-type: none"><li>• On Windows: C:\Program Files\Zero G Registry\.com.zerog.registry.xml</li><li>• On Linux: /var/.com.zerog.registry.xml</li></ul><hr/><b>Note:</b> The .com.zerog.registry.xml is a hidden file. Enable viewing hidden files to view this file if needed.<hr/><ol style="list-style-type: none"><li>2. Open the .com.zerog.registry.xml file and check for any server or agent-related entries.</li><li>3. Remove only the server or agent-specific entries from the registry file.</li></ol><hr/><b>Note:</b><ul style="list-style-type: none"><li>• Progress recommends taking the backup of the .com.zerog.registry.xml file before making any changes in it.</li><li>• Do not modify or delete entries for other products as this file contains configuration data of multiple products.</li></ul><hr/></li></ol>



# OpenEdge Command Center server startup failure in high availability setup

This topic describes how to troubleshoot the case where the OpenEdge Command Center server fails to start in a High Availability (HA) setup. It outlines common causes and provides recommended solutions to help you complete the startup process successfully.

Possible Cause	Recommended Solution
Database connectivity issue	<ol style="list-style-type: none"><li>1. Navigate to the installation log directory at <code>&lt;Server_Installed_Dir&gt;/install_logs/</code>, and open the log file named <code>Install_&lt;MM_DD_YYYY_H_M_S&gt;.log</code>.</li><li>2. Check for error messages, such as <code>Closed DB Connections</code>, which indicate a database connectivity issue.</li><li>3. If such errors are present, navigate to the <code>&lt;Data_Dir&gt;/conf/</code> folder and open the <code>db-config.json</code> file.</li><li>4. Verify the values for <code>DB Hostname</code> and <code>DB Port</code> and update them if necessary.</li></ol>
Database unreachable from the non-primary server	<ol style="list-style-type: none"><li>1. Check the connectivity from the non-primary server to the database host and port.</li><li>2. Ensure that the non-primary server is connected to a stable internet network.</li><li>3. Check if the firewall or proxy settings on the non-primary server system is blocking outbound connections. If necessary, update the settings to allow connectivity to the database host and port.</li></ol>



---

## How to

---

Using OpenEdge Command Center, you can perform the following tasks:

For information how to . . .	. . . see
Manage services for OpenEdge Command Center	<ul style="list-style-type: none"><li>• <a href="#">Manage services for OpenEdge Command Center server</a> on page 77</li><li>• <a href="#">Manage services for OpenEdge Command Center agent</a> on page 78</li></ul>
Change the logging level	<a href="#">Change logging level</a> on page 79
Log in	<a href="#">Log in to OpenEdge Command Center</a> on page 80
Set your password	<a href="#">Change or reset passwords</a> on page 82
Configure email settings	<a href="#">Configure email settings</a> on page 82
Mange users	<ul style="list-style-type: none"><li>• <a href="#">Create a new user</a> on page 83</li><li>• <a href="#">Edit user details</a> on page 84</li></ul>
Manage agents	<ul style="list-style-type: none"><li>• <a href="#">Add agent label</a> on page 86</li><li>• <a href="#">Update agent name and label</a> on page 86</li><li>• <a href="#">Search for and filter agents</a> on page 86</li><li>• <a href="#">Unregister an agent</a> on page 87</li></ul>
Manage OpenEdge databases	<ul style="list-style-type: none"><li>• <a href="#">Add a new OpenEdge database connection</a> on page 88</li></ul>

For information how to . . .	. . . see
	<ul style="list-style-type: none"> <li>• <a href="#">Start or stop OpenEdge databases</a> on page 90</li> <li>• <a href="#">Edit OpenEdge database connections</a> on page 90</li> <li>• <a href="#">Remove OpenEdge database connections</a> on page 91</li> <li>• <a href="#">View schema, users, and roles of a selected database</a> on page 92</li> </ul>
Configure PAS for OpenEdge instances	<ul style="list-style-type: none"> <li>• <a href="#">Configure PAS for OpenEdge instances</a> on page 93</li> <li>• <a href="#">Manage ABL applications or ABL web applications</a> on page 102</li> </ul>
Manage PAS for OpenEdge instances	<ul style="list-style-type: none"> <li>• <a href="#">Create a PAS for OpenEdge instance</a> on page 106</li> <li>• <a href="#">Start or stop a PAS for OpenEdge instance</a> on page 109</li> <li>• <a href="#">Delete a PAS for OpenEdge instance</a> on page 109</li> <li>• <a href="#">Obtain process details</a> on page 110</li> </ul>
Manage ABL applications, web applications, and REST services	<ul style="list-style-type: none"> <li>• <a href="#">View ABL applications across multiple PAS for OpenEdge instances</a> on page 111</li> <li>• <a href="#">Manage ABL applications</a> on page 112</li> <li>• <a href="#">Manage web applications</a> on page 114</li> <li>• <a href="#">Manage REST services</a> on page 116</li> <li>• <a href="#">Edit ABL application</a> on page 117</li> </ul>
Create users and manage roles using Authorization server	<ul style="list-style-type: none"> <li>• <a href="#">Log in to Authorization server</a> on page 122</li> <li>• <a href="#">Create a user</a> on page 123</li> <li>• <a href="#">Assign roles to a user</a> on page 124</li> <li>• <a href="#">Remove roles from a user</a> on page 127</li> <li>• <a href="#">Frequently Asked Questions</a> on page 129</li> </ul>
Monitor OpenEdge resources using the OpenEdge Command Center agent	<ul style="list-style-type: none"> <li>• <a href="#">Set up OpenTelemetry Collector</a> on page 133</li> <li>• <a href="#">OpenTelemetry metrics for OpenEdge database</a> on page 134</li> <li>• <a href="#">Enable OpenEdge Command Center agent to collect performance metrics of OpenEdge database</a> on page 136</li> <li>• <a href="#">Sample performance metrics data for OpenEdge database</a> on page 138</li> <li>• <a href="#">OpenTelemetry metrics for PAS for OpenEdge</a> on page 140</li> </ul>

For information how to . . .	. . . see
	<ul style="list-style-type: none"> <li>• <a href="#">Enable OpenEdge Command Center agent to collect performance metrics of PAS for OpenEdge on page 144</a></li> <li>• <a href="#">Sample performance metrics data for PAS for OpenEdge on page 146</a></li> <li>• <a href="#">Performance impact and resilience of collecting performance metrics on page 149</a></li> </ul>

For details, see the following topics:

- [Manage services for OpenEdge Command Center server](#)
- [Manage services for OpenEdge Command Center agent](#)
- [Change logging level](#)
- [Log in to OpenEdge Command Center](#)
- [Change or reset passwords](#)
- [Configure email settings](#)
- [Create a new user](#)
- [Edit user details](#)
- [Manage OpenEdge Command Center agents](#)
- [Manage OpenEdge databases](#)
- [Configure and manage PAS for OpenEdge instances](#)
- [Manage ABL applications, web applications, and REST services](#)
- [Create users and manage roles using Authorization server](#)
- [Set up TLS for OpenEdge Command Center and MongoDB communication](#)
- [Monitor OpenEdge resources using the OpenEdge Command Center agent](#)
- [Reset super admin user details](#)

## Manage services for OpenEdge Command Center server

You can manage the OpenEdge Command Center server service by starting or stopping it as needed on both the Windows and Linux platforms as a user with administrator privileges. These actions are typically performed to apply configuration changes or troubleshoot issues and require administrator or superuser privileges.

## Manage services for OpenEdge Command Center server on Windows

To start or stop the server installed as a service, perform the following steps:

1. Open **Task Manager** on the system where the server is installed using an account with administrator privileges.
2. Go to the **Services** tab and locate `ProgressOpenEdgeCommandCenterServer2.0`.
3. Right click the service name and perform the required action:
  - To start the service, select **Start**.
  - To stop the service, select **Stop**.

## Manage services for OpenEdge Command Center server on Linux

To start or stop the server installed as a service, perform the following steps:

1. Open a terminal with superuser (root) privileges.
2. Run the appropriate command:
  - To start the service:

```
systemctl start ProgressOpenEdgeCommandCenterServer2.0
.service
```

- To stop the service:

```
systemctl stop ProgressOpenEdgeCommandCenterServer2.0
.service
```

# Manage services for OpenEdge Command Center agent

After you start an OpenEdge Command Center agent, the status of the agent is updated in the **OECC Agents** page. Note that the status of an agent cannot be updated from the OpenEdge Command Center. You can start or stop the agent as a service. These actions are typically performed to apply configuration changes or troubleshoot issues and require administrator or superuser privileges.

---

**Note:** Do not use the `Proenv` environment command shell to start the OpenEdge Command Center agent. It can result in errors.

---

## Manage services for OpenEdge Command Center agent on Windows

To start or stop the agent installed as a service on Windows, perform the following steps:

1. Open **Task Manager** on the system where the agent is installed using an account with administrator privileges.
2. Go to the **Services** tab and locate `ProgressOpenEdgeCommandCenterAgent2.0`.
3. Right click the service name and perform the required action:
  - To start the service, select **Start**.
  - To stop the service, select **Stop**.

## Manage services for OpenEdge Command Center agent on UNIX or AIX

To start or stop the agent installed as a service, perform the following steps:

1. Open a terminal with superuser (root) privileges.
2. Run the appropriate command:

- On Linux or UNIX:

- To start the service:

```
systemctl start ProgressOpenEdgeCommandCenterAgent2.0.service
```

- To stop the service:

```
systemctl stop ProgressOpenEdgeCommandCenterAgent2.0.service
```

- On AIX:

- To start the service:

```
startsrc -e "OECC_AGENT=\"${OECC_AGENT}\"" -s ProgressOECCAgent2.0
```

- To stop the service:

```
stopsrc -s ProgressOECCAgent2.0
```

# Change logging level

Log files contain important information about the OpenEdge Command Center server and agents processes running on systems. The information in the log files is especially useful when you debug some issues, such as if an OpenEdge Command Center agent appears offline or as not running.

You can change the logging level to adjust the verbosity of information added to the log files. By default, the logging level for the OpenEdge Command Center server and agent logs is set as `info`. Based on your requirements, you can change the logging level to `debug`, `warn`, or `trace`.

### **Change logging level for the OpenEdge Command Center server logs**

To change logging level for the OpenEdge Command Center server log, complete the following steps:

1. Navigate to the `/data/conf` folder in the OpenEdge Command Center installation directory.
2. Open the `system-config.json` file in a text editor.
3. Change the value of `loglevel` to the required level.
4. Save the changes and close the file.
5. Restart the OpenEdge Command Center server.

### **Change logging level for the OpenEdge Command Center agent logs**

To change logging level for the OpenEdge Command Center agent logs, complete the following steps:

1. Navigate to the `resources` folder in the OpenEdge Command Center agent installation directory.
2. Open the `log4j2.properties` file in a text editor.
3. Change the value of `logger.app.level` to the required level.
4. Save the changes and close the file.
5. Restart the OpenEdge Command Center agent.

## **Log in to OpenEdge Command Center**

This topic provides information on user accounts created on the successful completion of the OpenEdge Command Center server and MongoDB installation. It also describes how to access the OpenEdge Command Center dashboard and outlines the steps required to log in using the default super admin user account.

### **Default super admin and built-in accounts**

After a successful installation of the OpenEdge Command Center server and MongoDB, the following accounts are created automatically:

- A default super admin user account for the initial login to the OpenEdge Command Center dashboard.
- A built-in user account for internal use in the OpenEdge Command Center database.

#### **Default super admin account**



The default super admin credentials for initial access to the OpenEdge Command Center dashboard are as follows:

- Username: admin
- Password: admin

---

**Note:**

- Progress recommends that you change the default password immediately after the initial login.
- If the server you installed is an additional server in a high availability setup, you can use the same credentials as the primary server to log in to the OpenEdge Command center dashboard.

---

The default email address for the super admin user is `admin@oecc.com`. You must change this default email address to a preferred one using the `resetsuperadmin` utility. Otherwise, you cannot add new user accounts. You can also use the `resetsuperadmin` utility to optionally update the other super admin user details, including the password, first name, and last name. For more information, see [Reset super admin user details](#) on page 150 and [RESETSUPERADMIN utility](#) on page 153.

**Built-in database user account**

The built-in user credentials created for internal use in the OpenEdge Command Center database are as follows:

- Username: dbadmin
- Password: `<encrypted password>`

## Log in to OpenEdge Command Center dashboard

To log in to OpenEdge Command Center dashboard, perform the following steps:

1. Enter `https://host[:port]` in the browser address bar.

The host is the name of a system on which OpenEdge Command Center is installed, and the optional port number is the web server port. By default, this port is 8000. A sign-in form appears, prompting you to enter your login credentials.

---

**Note:** If OpenEdge Command Center operates in high availability mode, and you are using a load balancer, then omit the port number when you specify the load balancer host name.

---

2. If you are logging in for the first time, enter your login credentials and click **Sign in**.
3. After you log in to OpenEdge Command Center for the first time, you must establish initial configurations before you can use it.

On OpenEdge Command Center, the menu bar consists of the following functional options:

- Dashboard
- OECC Agents
- OpenEdge Databases
- PASOE Instances
- ABL Applications
- Users
- OECC System Settings

- Email Settings

---

**Note:** If OpenEdge Command Center detects no activity for more than 30 minutes, your session times out.

---

Upon first login to the OpenEdge Command Center console dashboard, Progress recommends changing the default admin password. For information about changing the default password after the first login, see [Change or reset passwords](#) on page 82.

## Change or reset passwords

You can change or reset your password after you have logged in to OpenEdge Command Center.

To change your password:

1. On the OpenEdge Command Center, go to your user account option on the top-right corner.
2. Select **Change password**.
3. On the **Change Password** page, enter information in the following fields:
  - **Old Password**
  - **New Password**
  - **Confirm Password**

Note that the password you create must have:

- Between 8-40 characters
- A mixture of uppercase and lowercase letters
- At least one numeral
- At least one of the special characters: ! @ \$ % ^ & ( ) \_ + = [ ] |

In addition, a password must not contain the following:

- Your username
- A previously used password

4. Click **Change Password**.

## Configure email settings

To create a user, you must first set up the email settings. Email settings can be set up by a super administrator or an administrator.

OpenEdge Command Center supports all standard mail servers (Gmail, Hotmail, Yahoo, and others).

---

**Note:** New users can be created only after the email settings are configured.

---

To configure email settings:

1. Go to **Email Settings**.
2. On the **Email Settings** page, enter information in the following fields:
  - **SMTP Host name**
  - **SMTP Port name**
3. Select the **Secure Connection** checkbox to enable a secure connection (HTTPS).
4. Select the **Allow Only Trusted Certificates** checkbox to enable using trusted certificates. This checks for valid certificate. It is enabled by default.
5. Alternatively, use the **STARTTLS Options** to customize your secure connection.
  - Ignore STARTTLS
  - Use STARTTLS when available
  - Require STARTLS
6. Select the **SMTP Authentication** checkbox to enable SMTP authentication and enter the following:
  - **Mail server (SMTP) username**
  - **Mail server (SMTP) password**
7. Enter a valid email address in the **Default email sender** field.

## Create a new user

During installation, the first user to be set up is given the super administrator role

---

**Note:** New users can be created only after the email settings are configured. See here, [Configure email settings](#) on page 82.

---

To add a new user:

1. Go to **Users**, and click **New User**.
2. Enter the following information:
  - **First name**
  - **Last name**
  - **Username**
  - **(Optional) Description**
3. Choose a role from the drop-down list:
  - **Administrator**—An administrator can create users and perform all actions, but cannot assign a super administrator role.
  - **No access**—If a user is set to this role, then he or she cannot access the OpenEdge Command Center.

---

**Note:** Information about character length for each field is available inline. Ensure that the details you enter conform to the rules.

---

4. An email is sent to the email address entered, and you are prompted to set your login credentials.

After a new user is created, you can view the following information on the **Users** page on the dashboard:

- Username
- Role
- Email
- Description (whether the user was created during installation or added as a new user)
- Created at
- Last login

By default, columns are sorted by time stamps, but you can sort them as desired.

After you create a new user account, the system does not grant the user access to any remote resources by default. You must explicitly grant access by assigning roles in the Authorization server using the REST APIs. For more information, see "Authorization server" in *OpenEdge Command Center REST APIs*.

Until you assign roles, the user can access only basic user management operations, such as viewing users and updating their own profile.

## Edit user details

You can edit the first name, last name, description, email, and role of a user. To update the email address and role, you receive a verification code through email, for added security. The other updates are applied immediately.

To update the details of a user:

1. In the OpenEdge Command Center console, click **Users**. The **Users** page appears.
2. Select the user whose details you want to edit. The **Edit User** page appears with the following fields enabled for editing:
  - **First Name**
  - **Last Name**
  - **Email**
  - **Description**
  - **Roles**
3. Edit the required fields and click **Save**.
  - If the changes are for first name, last name, and description, the updates are applied immediately.
  - If the changes are for email address and role, the **Identity Verification** dialog box appears.
4. In the **Verification Code** field, enter the code that you received on your email to complete the verification.
5. Click **Verify**. After successful verification, the updates are applied.

## Manage OpenEdge Command Center agents

The **OECC Agents** page lets you view and manage the agents linked to your OpenEdge deployments. This page displays the following details of the OpenEdge Command Center agents:

- **Name**—Name of the agent.
- **Labels**—Labels that you assign to the agent to categorize and filter it.
- **Host Name**—Host name of the system where the agent is running.
- **OS Name**—Name of the operating system on which agent is running.
- **OS Version**—Version of the operating system on which agent is running.
- **OS Family**—Classification of the operating system on which agent is running.
- **Version**—Version of the agent.
- **Status**—Indicates whether the agent is running or offline.
- **OECC Agent Start Time**—The date and time when the agent last started.
- **IP Address**—The IP address of the system where the agent runs.

From this page, you can perform the following tasks:

- Search and filter agents using defined parameters
- Add or edit labels to organize agents
- Edit agent names
- Unregister agents when necessary

## Add agent label

You can add agent labels for the agents that are configured on OpenEdge Command Center. Adding labels allows you to easily filter development, test, or production components of the agents.

Add agent labels:

1. Go to **OECC Agents**.
2. Select an agent, and click **Actions**.
3. Select **Add Labels** from the drop-down list.
4. Enter the label in the **Labels** field, and click **Save**.

---

### Note:

- You can enter up to five labels per agent.
  - The maximum number of characters allowed in a label is 40. The supported characters are alphanumeric, dot (.), underscore (\_), and hyphen (-). Other special characters are not supported.
- 

## Update agent name and label

To update OpenEdge Command Center agent name and labels:

1. Go to **OECC Agents**.
2. Click the agent. The **Edit Agent** page is displayed.
3. On the **Edit Agent** page, update the required fields:
  - **Name**—Name of the agent host
  - **Labels**—Labels associated with corresponding agent
4. Click **Save** to update the agent information.

You can view agent labels on the **OECC Agents** page.

## Search for and filter agents

You can search for and filter Command Center agents based on the defined parameters.

To search for Command Center agents:

1. Go to **OECC Agents**.
2. Place your cursor in the **Type here to filter** space on the search bar above the listed agents.
3. Select one of the following options from the drop-down list, and then choose one of the available criteria that you want to filter by:
  - **Agent Name**
  - **Labels**
  - **Host Name**
  - **OS**
  - **Version**
  - **Status**
  - **IP Address**
4. Enter the required information. For example, if you select **Labels**, then enter the label name that you want to filter by. OpenEdge Command Center supports the use of the asterisk (\*) wildcard character in filter specifications.

The filtered agents are displayed.

## Unregister an agent

You can unregister an agent to remove it from OpenEdge Command Center when the agent is offline.

To unregister an agent, perform the following steps:

1. In the **OpenEdge Command Center** console, click **OECC Agents**.  
The **OECC Agents** page appears.
2. Select the check box next to the agent with an **OFFLINE** status that you want to unregister.
3. On the **Actions** menu, click **Unregister OECC agent**.  
The **Unregister Agents** popup window appears.
4. Click **Unregister Agents**.

A notification confirms that the agent was successfully unregistered. Optionally, you can refresh the notification and view the outcome of the operation by clicking the **bell** icon.

## Manage OpenEdge databases

This topic describes how you can manage the OpenEdge databases using OpenEdge Command Center.

The **OpenEdge Databases** tab enables you to manage OpenEdge databases. When you click this tab, the **OpenEdge Databases** page appears. On this page, you can view both the running databases that are automatically discovered and the database connections that you have previously added. You can add new database connections, start or stop databases, and edit or remove existing database connections. You can view the following details of the OpenEdge databases:

- **Name**—Name of the database.
- **Labels**—Labels that are assigned to the database.
- **Path**—Complete path of the database to which you are connected.
- **Agent**—Name of the OpenEdge Command Center agent.
- **Status**—Indicator of whether the database is running.
- **Port/Service Name**—Port number or service name of the database.
- **Version**—Version of the database.
- **Host Name**—Name of the machine where the database is hosted.
- **OpenEdge Installation**—The OpenEdge installation where the database is present.

The details of the databases are organized in columns. You can view or hide specific columns using the **Add/Remove Columns** button. When you click this button, the **Add/Remove Columns** picker appears, displaying a list of column names along with toggle buttons. You can use the toggle button next to each column name to view or hide the corresponding column on the page. You can refresh the content on the page by clicking **Refresh**.

The **OpenEdge Databases** page also lets you log in to any running OpenEdge database to view its schema, users, and user roles details.

### Filter OpenEdge databases

You can quickly search and filter the databases using the **Type here to filter** field. It allows you to select one of the following options from the drop-down list and choose the available criteria to filter by:

- **Name**
- **Status**
- **Labels**
- **Host Name**
- **Version**
- **Agent Name**

## Add a new OpenEdge database connection

This section describes how you can add an OpenEdge database connection using OpenEdge Command Center.



To add an OpenEdge database connection, perform the following steps:

1. In the OpenEdge Command Center console, click **OpenEdge Databases**.

The **OpenEdge Databases** page appears.

2. Click **+ Add New Connection**.

The **New Database Connection** page appears.

3. Specify the following OpenEdge database details:

In the following field . . .	. . . do the following
<b>OpenEdge Installation</b>	Select the OpenEdge installation where the database is present.
<b>Database Folder Path</b>	Specify the complete path of the database which you want to connect. For example, <code>/usr/dlcwrk/mydb/database1.db</code> .
<b>Database Name</b>	Displays the name of the database. It is automatically populated after you enter the complete path of the database.
<b>Labels</b>	Lets you distinguish between database resources. Select existing or create new labels to assign them to the database.
<b>Port/Service Name</b>	Specify the port number or service name for connecting to the database.
<b>User ID</b>	<p>Specify a user ID with Database Administrator (DBA) privileges to connect to the database.</p> <hr/> <p><b>Note:</b> The User ID can contain only alphanumeric characters and certain special characters: underscore ( _ ), dash (-), and number sign (#).</p> <hr/>
<b>Password</b>	Specify a password for the user ID.
<b>Confirm Password</b>	Re-enter the password.
<b>Other Parameters</b>	<p>Specify the list of optional parameters, separated by space, to connect to the database. For example, to specify the Maximum Clients per Server and the Maximum Servers parameters, enter the following:</p> <p><code>-Ma 10 -Mn 1</code></p> <hr/> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• If the OpenEdge database is running, the parameters used while starting the database are appended to the parameters you enter.</li> <li>• If the OpenEdge database is stopped, the <code>-db</code> and <code>-s</code> parameters are prepended by default to the parameters you enter.</li> </ul> <hr/>

4. Optional. Click **Test Connection** to verify whether the values entered in the respective fields are correct
5. Click **Save**.

A notification popup window appears, displaying a message that the database connection is in progress. Optionally, you can refresh the notification and view the outcome of the operation by clicking the bell icon. After the connection is successfully established, the **OpenEdge Databases** page displays the database details and its current status.

## Start or stop OpenEdge databases

From the OpenEdge Command Center console, you can start or stop one or more OpenEdge databases, as follows:

1. In the OpenEdge Command Center console, click **OpenEdge Databases**.

The **OpenEdge Databases** page appears.

2. Select the check box next to each database that you want to start or stop.

---

**Note:** You can start only those databases whose status is displayed as **STOPPED**, and stop only those databases whose status is displayed as **RUNNING**.

---

3. To start or stop one or more databases, perform either of the following set of steps respectively:

- To start one or more databases, from the **Actions** menu, click **Start**.

A notification popup window appears, displaying a message that the start operation is in progress. Optionally, you can refresh the notification and view the outcome of the operation by clicking the bell icon. After the connection is established successfully, the database details appear on the **OpenEdge Databases** page, and the database status is displayed as **RUNNING**.

- To stop one or more databases, from the **Actions** menu, click **Stop**. In the popup window, type **stop** and click **Stop**.

A notification popup window appears, displaying a message that the start operation is in progress. Optionally, you can refresh the notification and view the outcome of the operation by clicking the bell icon. After the connection is established successfully, the database details appear on the **OpenEdge Databases** page, and the database status is displayed as **STOPPED**.

## Edit OpenEdge database connections

From the OpenEdge Command Center console, you can edit OpenEdge database connections, as follows:

1. In the OpenEdge Command Center console, click **OpenEdge Databases**.

The **OpenEdge Databases** page appears.

2. Click the name of the OpenEdge database whose connection details you want to update.

The **Edit Database Connection** page appears.

3. Update the values in any or all of the following fields, as required.

Field	Description
<b>Labels</b>	Lets you distinguish between database resources. Select existing or create new labels to assign them to the database.
<b>Port/Service Name</b>	Specify the port number or service name for connecting to the database.
<b>User ID</b>	Specify a user ID with Database Administrator (DBA) privileges to connect to the database.  <b>Note:</b> The User ID can contain only alphanumeric characters and certain special characters such as underscore ( _ ), dash (-), and number sign (#).
<b>Password</b>	Specify a password for the user ID.
<b>Confirm Password</b>	Re-enter the password.
<b>Other Parameters</b>	Specify the list of optional parameters, separated by space, to connect to the database. For example, to specify the <b>Maximum Clients per Server</b> and the <b>Maximum Servers</b> parameters, enter the following:  -Ma 10 -Mn 1

- Optional. Click **Test Connection** to verify your entered values are correct.

---

**Note:** **Test Connection** is available only if the database is in running status.

---

- Click **Save**.

A notification popup window appears, displaying a message that the database connection details are updated successfully. Optionally, you can refresh the notification and view the outcome of the operation by clicking the bell icon.

## Remove OpenEdge database connections

From the OpenEdge Command Center console, you can remove one or more OpenEdge database connections, as follows:

- In the OpenEdge Command Center console, click **OpenEdge Databases**.  
The **OpenEdge Databases** page appears.
- Select the check box next to each database connection that you want to remove.
- On the **Actions** menu, click **Delete Connection**. The **Delete Connections** popup window appears.

4. In the **Type delete to confirm** field, type **delete**.
5. Click **Delete Connections**.

A notification popup window appears, displaying a message that the selected database connections are removed. Optionally, you can refresh the notification and view the outcome of the operation by clicking the **bell** icon. After the database connections are removed successfully, the corresponding database details no longer appear on the **OpenEdge Databases** page.

## View schema, users, and roles of a selected database

From the **OpenEdge Command Center** console, you can view details of schema, users, and roles of a running database, as follows:

1. In the OpenEdge Command Center console, click **OpenEdge Databases**.  
The **OpenEdge Databases** page appears.
2. Select the checkbox next to the running OpenEdge database for which you want to view the details. The **<database\_name>** pane appears at the bottom of the page, displaying three disabled tabs: **Schema**, **Users**, and **Roles**.
3. Log into the database by clicking **Login**. The **Database Authentication** dialog box appears.
  - a) In the **Database User ID** field, type the username.
  - b) In the **Database Password** field, type the password.
  - c) Click **Authenticate**.The **Schema**, **Users**, and **Roles** tabs are enabled.

4. Click each of the **Schema**, **Users**, or **Roles** tab to view the corresponding details of the database.
  1. To view the details about database schema and their tables and columns, click the **Schema** tab. The following sections appear:
    - **Tables**: Lists the tables within the database.
    - **Columns**: Lists the columns that are associated with the table.
    - **Details**: Lists the column details, such as field, datatype, display format, and default value.

You can quickly search for tables and columns by clicking the search icon next to the corresponding section title. You can get the latest data from the OpenEdge database by clicking **Refresh**.

2. To view the users who have access to the database, and their usernames and associated roles, click the **Users** tab. The following sections appear:
  - **Users**: Lists all the users within the database.
  - **Details**: Lists the user details, such as username and roles assigned to the user.

You can quickly search for users by clicking the search icon next to the **Users** section title. You can get the latest data from the OpenEdge database by clicking **Refresh**.

3. To view details about various system-defined roles, click the **Roles** tab. The following sections appear:
  - **Roles**: Lists the system-defined roles.
  - **Details**: Lists the role details, such as created by, type, and description.

You can quickly search for roles by clicking the search icon next to the **Roles** section title. You can get the latest data from the OpenEdge database by clicking **Refresh**.

## Configure and manage PAS for OpenEdge instances

After you have configured an agent, the PAS for OpenEdge instances associated with that agent become discoverable on OpenEdge Command Center. The instances are available on the **PAS for OpenEdge Instances** page on the OpenEdge Command Center dashboard.

You can view the following information about the PAS for OpenEdge instances:

- **Name**—Name of the PAS for OpenEdge instance.
- **Labels**—All labels that are assigned to that server; for example: `test`, `production`, or `development`.
- **Status**—Indicator of whether the PAS for OpenEdge instance is running.
- **Host Name**—Name of the machine where the instance is hosted.
- **Install Path**—Location of where the instance is installed on the agent.
- **Version**—Version of the PAS for OpenEdge instance.
- **Catalina Base**—Path of the `CATALINA_BASE` directory.
- **IP Address**—IP address of the PAS for OpenEdge instance host.
- **Agent**—Name of the PAS for OpenEdge instance agent

## Configure PAS for OpenEdge instances

This topic describes how you can configure PAS for OpenEdge instances using the OpenEdge Command Center console.

### Filter PAS for OpenEdge instance properties

The **Edit PAS For OpenEdge Instance** page displays many configuration properties. You can use a filter to easily locate the property you want to modify.

To filter the properties of the PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click **PASOE Instances**.

The console displays a page that lists all PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.

2. Click the name of the PAS for OpenEdge instance whose configuration you want to modify.

The **Edit PAS For OpenEdge Instance** page is displayed.

3. In the search field, enter the name, label, or section header of the property that you want to locate. You can also enter the property name as specified in the `catalina.properties` file. For example, enter `psc.as.executor.maxthreads` (as it appears in the `catalina.properties` file) to locate the **Max Threads** property. Only the **Max Threads** property field is displayed on the page.

## Edit PAS for OpenEdge instance properties

This topic explains how to edit the properties of a PAS for OpenEdge instance on the **Edit PAS for OpenEdge Instance** page:

To edit the properties of a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.

The console displays a page that lists all PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.

2. Click the name of the PAS for OpenEdge instance whose configuration you want to modify.

The **Edit PAS for OpenEdge Instance** page is displayed.

3. In the **Info** section, update values for the following properties:

Field	Description
<b>Instance Name</b>	Name of the PAS for OpenEdge instance.
	<b>Note:</b> The PAS for OpenEdge instance name is case-sensitive and must be at least 5 characters long. It can include any character except periods (.) or square brackets ([ ]). The name must be unique among all configured PAS for OpenEdge instance names.
<b>Labels</b>	One or more labels assigned to the instance. Use the drop-down box to select one or more labels, or create one or more new labels to assign.

4. Click **HTTPS** to expand the HTTPS connection properties section.

Provide values for the following properties:

Property	Default value	Description
<b>HTTPS Connector</b>	ON	Use the ON/OFF toggle switch to enable or disable the HTTPS connector respectively.
<b>Port</b>	8443	Specifies the HTTPS protocol connector port number.
<b>Connection Timeout</b>	20000	Specifies the time, in milliseconds, to wait between the establishment of a TCP (TLS) connection by a client and the arrival of the first HTTPS request.
<b>SSL Session Timeout</b>	86400	Specifies the time, in seconds, after which the TLS session ends.
<b>Server Key Alias</b>	test	Specifies the alias name of the keystore entry holding the server's private key and public key certificate.

Property	Default value	Description
<b>Server Key Password</b>	password	Specifies the password to use when accessing the TLS keystore.
<b>Store Type</b>	PKCS12	Specifies the type of Java keystore format used by Apache Tomcat keystore.
<b>Max Queue Size</b>	100	Specifies the maximum size of the HTTPS connector message queue.
<b>Max Connections</b>	-1	Specifies the maximum number of TCP socket connections per HTTPS connector.
<b>Client Authentication</b>	none	Specifies whether to enable or disable TLS client authentication by the HTTPS connector. The options are <b>required</b> , <b>none</b> , and <b>optional</b> . The default is none.
<b>Certificate Trust Type</b>	JKS	Specifies the type of Java certificate store format used by <code>tomcat-certstore.jks</code> that holds the root or intermediate CA certificates. These certificates are used to validate the clients using TLS client authentication.
<b>Certificate Store Password</b>	password	Specifies the Java certificate store password used to access <code>tomcat-certstore.jks</code> that holds the root or intermediate CA certificates. These certificates are used to validate the clients using TLS client authentication.
<b>Encryption Protocol</b>	TLSv1.2	Specifies the HTTPS protocol selected for secure communication. If required, you can also edit this value in the <code>catalina.properties</code> file.
<b>Enabled Ciphers</b>	ALL	Specifies the list of cipher suites enabled for secure communication. This property can either be all the cipher suites or a comma-separated list of cipher suites supported by JSSE.
<b>Bind On Init</b>	false	Check box to control when to bind the socket used by the connector.
<b>Compression</b>	on	Check box to enable GZIP compression for HTTPS transports.

- Click **HTTP** to expand the HTTP connection properties section.

Provide values for the following properties:

Property	Default value	Description
<b>HTTP Connector</b>	ON	Use the ON/OFF toggle switch to enable or disable the HTTP connector respectively.
<b>Port</b>	8090	Specifies the HTTP protocol connector port number.
<b>Connection Timeout</b>	20000	Specifies the time, in milliseconds, to wait between the establishment of a TCP connection by a client and the arrival of the first HTTP request.
<b>Max Connections</b>	-1	Specifies the maximum number of TCP socket connections per HTTP connector.
<b>Max Queue Size</b>	100	Specifies the maximum size of HTTP connector message queue.
<b>URI Encoding</b>	ISO-8859-1	<p>Specifies the character encoding used to decode the URI bytes after decoding the URL.</p> <hr/> <p><b>Note:</b> This value is set to the default value of the Apache Tomcat server, and it affects both the HTTP and HTTPS connectors.</p> <hr/>
<b>Bind On Init</b>	false	Check box to control when to bind the socket used by the connector.
<b>Compression</b>	on	Check box to enable GZIP compression for HTTP transports.

6. Click **Server Options** to expand the Server Options section.

Provide values for the following properties:

Property	Default value	Description
<b>Shutdown Port</b>	—	<p>Specifies the port number to shutdown the server that is running.</p> <p>The values can range from 1024 to 65535. To disable the shutdown port, set the value to -1.</p> <p>You must specify a value in Windows, but this property is optional in UNIX.</p>



Property	Default value	Description
<b>Shutdown Password</b>	SHUTDOWN	<p>Specifies a private shutdown port access code to prevent one server instance from being shutdown by anyone.</p> <hr/> <p><b>Note:</b> If the shutdown port is specified, you must change this value to avoid insecure configuration.</p> <hr/>
<b>Stuck Session Valve</b>	ON	Specifies whether the stuck session valve is enabled to monitor and manage sessions that become unresponsive or exceed a defined execution time.
<b>Stuck Thread Threshold</b>	600	Specifies the maximum amount of time, in seconds, an active HTTP request can be running before it is considered stuck and is reported in the server log file.
<b>Max Threads</b>	300	Specifies the maximum number of OS process threads the PAS for OpenEdge Server can use.
<b>Minimum Spare Threads</b>	10	Specifies the number of spare threads the server reserves for future client operations.
<b>Web Application Directory</b>	webapps	<p>Specifies the location of the directory where the web applications are to be deployed. If not specified, then the default directory of the Apache Tomcat server, <code>webapps</code> is used.</p> <p>If a relative path is specified, it must be relative to the instance's root directory. If an absolute path is used, it must conform to a single platform type.</p>
<b>Common Library Path</b>	—	<p>Specifies a comma-delimited list of library paths. For example,  <code>local/server/common/*.jar,local/server/common/x.jar</code>.</p> <p>The delimiter is platform dependent, and the format of the path must conform to the common library path format of the Apache Tomcat server (<a href="https://tomcat.apache.org/tomcat-9.0-doc/class-loader-howto.html">https://tomcat.apache.org/tomcat-9.0-doc/class-loader-howto.html</a>).</p>

Property	Default value	Description
<b>Auto Deploy WAR Files</b>	false	Select the checkbox to enable the security settings used by the Apache Tomcat server for deploying web applications.  The default value depends on whether the PAS instance is created as a development or a production security configuration. In a production configuration, the default is <code>false</code> . In a development configuration, the default is <code>true</code> .
<b>Unpack WAR Files</b>	true	Select the checkbox to allow unpacking of web archive ( <code>.war</code> ) files when the PAS for OpenEdge instance is started.
<b>Version Logger</b>	ON	Use the <b>ON/OFF</b> toggle to enable or disable logging the command line arguments passed to Java when the Apache Tomcat server is started.
<b>Log Command Line Arguments</b>	true	Select the checkbox to log the command line arguments passed to Java when the Apache Tomcat server is started.
<b>Log Environment Variables</b>	false	Select the checkbox to log the current environment variables when the Apache Tomcat server is started.
<b>Log Java System Properties</b>	false	Select the checkbox to log the current Java system properties when the Apache Tomcat server is started.

7. Click **Request Options** to expand the Request Options section.

Provide values for the following properties:

Property	Default value	Description
<b>Max POST Request Size</b>	2097152	Specifies the maximum size, in bytes, of a connector's POST message body.
<b>Max Pipeline Requests</b>	100	Specifies the maximum number of pipelined HTTP keepalive requests before the TCP socket to the client is closed.

Property	Default value	Description
<b>Message Timeout</b>	10000	Specifies the maximum time, in milliseconds, to wait for asynchronous messages to complete.
<b>Compression Minimum Size</b>	2048	Specifies the minimum size, in bytes, of message that will be compressed, in bytes. This property is applicable to both HTTPS and HTTP transports.
<b>Compression MIME Types</b>	text/html, text/xml, text/javascript, text/css, application/json	Specifies a comma-separated list of MIME types that must be compressed. This property is applicable to both HTTPS and HTTP transports.

8. Click **JVM Settings** to expand the JVM Settings section.

Set the JVM arguments to configure Java environment settings for the PAS for OpenEdge instance. For example, set `-XX:NewSize` and `-XXMaxNewSize` to specify the minimum and maximum heap size used in garbage collection.

9. Click **Logging Configuration** to expand the Logging Configuration section.

Provide values for the following properties:

Property	Recommended setting	Description
<b>Catalina Logging Level</b>	INFO	Sets log level for the core Apache Tomcat server. By default, the logging level is set to INFO, but you can change it to WARN, FINE, FINER, ERROR, DEBUG, or TRACE, as required.
<b>OpenEdge ABL Logging Level</b>	WARN	Sets the log level for ABL application (oeabl.war) Session Manager and Spring Security logging.
<b>Authentication Logging Level</b>	ERROR	Sets the log level for ABL application login event logging.

Property	Recommended setting	Description
<b>Authorization Logging Level</b>	ERROR	Sets the log level for ABL application URL access event logging.
<b>OpenEdge STS Logging Level</b>	WARN	Sets the log level for the OpenEdge Authentication Gateway server Security Token Service web application.

10. Click **MS Agent Log Configuration** to expand the Agent Log Configuration section.

Provide values for the following properties:

Property	Description
<b>MS Agent Log Entry Types</b>	Specifies the types of log entries to write to the log file specified by the Client Logging and DataServer Logging startup parameters. If <code>allowRuntimeUpdate</code> is set to <code>true</code> , then changes to the property are applied without restarting the PAS for OpenEdge instance
<b>MS Agent Log Level</b>	Specifies the logging level for each entry type. You can select values from 0 to 4. If <code>allowRuntimeUpdate</code> is set to <code>true</code> , then changes to the property are applied without restarting the PAS for OpenEdge instance.

For more information about the Agent Log Configuration properties, see "Troubleshoot problems with an instance" in *Manage Progress Application Server (PAS) for OpenEdge*.

11. After modifying properties, you must restart the PAS for OpenEdge instance for most of the changes to take effect. However, if `allowRuntimeUpdate` is set to `true`, then changes to the **MS Agent Log Entry Types** and **MS Agent Log Level** properties are applied without restarting the PAS for OpenEdge instance.

## Clone a PAS for OpenEdge instance

You can clone a PAS for OpenEdge instance to quickly create identical PAS for OpenEdge instances and help you set up load balancing. You can create up to eight identical PAS for OpenEdge instances in a single clone operation. For cloning, the platform of the destination OpenEdge installations must be the same as the source PAS for OpenEdge instance. Also, if the source PAS for OpenEdge instance refers to external files or folders, the cloned instances may not work as expected.

To clone a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.

The **PAS for OpenEdge Instances** page displays a list of all PAS for OpenEdge instances that are associated with all the currently configured OpenEdge Command Center agents.

2. Select the check box for the PAS for OpenEdge instance that you want to clone.
3. On the **Actions** menu, select **Clone**.

The **Clone PAS for OpenEdge Instance** page appears.

4. On the **Clone PAS for OpenEdge Instance** page, enter the following details:

In the following field . . .	. . . do the following
<b>Instance Name</b>	<p>Specify a name for all the destination PAS for OpenEdge instances. By default, this value is the name of the cloned PAS for OpenEdge instance. However, you can specify a different name based on the requirements. This field is mandatory.</p> <hr/> <p><b>Note:</b> The PAS for OpenEdge instance name is case-sensitive. It must be unique among all configured PAS for OpenEdge instances and can include any character except periods (.) or square brackets ([ ]).</p> <hr/>
<b>Instance Size</b>	View the size of the cloned PAS for OpenEdge instance. This value is automatically calculated by OpenEdge Command Center.
<b>Labels</b>	Use the drop-down list to select one or more labels, or create one or more new labels to assign. You can have a maximum of seven labels for a PAS for OpenEdge instance. All the labels of the source PAS for OpenEdge instance are automatically added to the field. If the total number of labels is less than seven, then a new label, <code>cloned_from_&lt;source&gt;</code> is added to the field.
<b>OpenEdge Installation</b>	<p>Use the drop-down box to select the destination OpenEdge installations for cloning the PAS for OpenEdge instance. You can select up to eight different OpenEdge installations as destinations for cloning.</p> <p>If you select a destination that already has a PAS for OpenEdge instance with the same name, the destination appears in red color, which indicates that the cloning operation cannot proceed. Selecting the <b>Overwrite duplicate PAS for OpenEdge instance</b> option removes the red color and allows you to proceed with the cloning.</p>
<b>Overwrite duplicate PAS for OpenEdge instance</b>	Select the check box to overwrite an existing PAS for OpenEdge instance in the destination, which has the same name as the source PAS for OpenEdge instance.
<b>Start PAS for OpenEdge instance after it is cloned</b>	Select the check box to start the PAS for OpenEdge instances immediately after they are created in the destination installations.

5. Click **Clone Instance**.

The notifications in the OpenEdge Command Center console inform you about the progress of the cloning process. As the cloned PAS for OpenEdge instances are created, they are displayed on the **PAS for OpenEdge Instances** page. If you selected the **Start PAS for OpenEdge instance after it is cloned** check box, the newly cloned instances are started and their status changes to **RUNNING**.

If a cloned PAS for OpenEdge instance fails to start because of a port conflict in the destination machine, update the configuration of the cloned instance to use a unique port, from the **Edit PAS for OpenEdge Instance** page.

## Manage ABL applications or ABL web applications

A PAS for OpenEdge instance can have several deployed OpenEdge ABL applications on it. In the OpenEdge Command Center, you can access, deploy, and undeploy your ABL and web applications on the PAS for OpenEdge instances tab.

### Access your ABL applications or ABL web applications

In the OpenEdge Command Center, an ABL application is hosted on a PAS for OpenEdge instance and is accessible from a PAS for OpenEdge client. OpenEdge supports REST, WEB, SOAP, and APSV transport services for accessing the ABL application logic.

To access your ABL and web applications:

1. On the OpenEdge Command Center user interface, click the **PASOE Instances** tab on the side menu.  
The PAS for OpenEdge instances page is displayed and shows a list of your PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.
2. Select the check-box next to the instance that hosts the ABL application or web application.  
The **Applications** window is displayed on the lower part of the screen.
3. Select the ABL application that you want to view.  
The web application name, its deployment path, number of services, and the status the four transports is displayed.
4. Click the ABL application to view or edit its properties. The **Edit ABL Application** page appears, displaying the properties of the corresponding ABL application. For more information, see [Edit ABL application](#) on page 117.

---

**Note:** The OpenEdge Command Center release does not support viewing independent web applications such as `manager`, `oemanager`, `oedbg`. However, the OpenEdge Command Center needs a manager application to deploy or undeploy applications. When you create a new PAS for OpenEdge instance, OpenEdge Command Center provides an option to deploy a manager application and define login credentials. It is highly recommended that you do not use the default Apache Tomcat credentials to enable security for your manager application.

---

### Deploy ABL application

To deploy an ABL application on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.  
The **PAS for OpenEdge Instances** page appears, listing all the instances associated with the currently configured OpenEdge Command Center agents.
2. Select the checkbox next to the instance on which you want to deploy the ABL application. The **Applications** pane appears at the bottom of the page.
3. Click **Deploy**. The **Deploy Application** dialog box appears.
4. Select the **ABL Application** option as the application type.
5. In the **Select Application File** field, click **Select File** to browse to the location of the OpenEdge Archive (OEAR) file containing the ABL application and select the file.

**Note:**

- You can deploy ABL applications as an OEAR file only. For information about the OEAR file, see "Create an OpenEdge Application Archive using tcman export" and "Create an OpenEdge Application Archive using an Ant Build" in *Manage Progress Application Server (PAS) for OpenEdge*.
- If you are deploying an OEAR file on an instance that already contains ABL applications or web applications with the same names as those included in the OEAR file, you must undeploy the existing applications first.
- The OEAR file does not need to have the same name as the ABL application.
- You can upload an OEAR file only if its size is less than or equal to 523,239,424 bytes (499 MB). If you want to upload a larger file, update the `system-config.json` file by adding the `maxFileUploadSize` parameter with appropriate value and restart the OpenEdge Command Center server. The maximum value you can set is 3,221,225,472 bytes (3 GB). For more information, see [OpenEdge Command Center server configuration](#) on page 37.

6. Based on the status of the PAS for OpenEdge instance, the dialog box displays either the **Deploy** or **Deploy & Restart** button. The following table summarizes different scenarios:

If	Then	
Status of PAS for OpenEdge instance	Deploy Application dialog box displays	Required action
Running	The <b>Deploy &amp; Restart</b> button	Click <b>Deploy &amp; Restart</b> .
Stopped	The <b>Deploy</b> button	Click <b>Deploy</b> .

**Note:** The deployment of the ABL application on the PAS for OpenEdge instance is independent of the deployment status of the Apache Tomcat Manager application.

A popup appears, displaying the notification that the deploy operation is successfully submitted. You can click the bell icon to refresh and view the deployment status. After the successful deployment, the ABL application appears in the **ABL Applications** section of the **Applications** pane.

**Note:** If an ABL application is deployed on a stopped PAS for OpenEdge instance, you must start the instance to access the ABL application services. For information on how to start a PAS for OpenEdge instance, see [Start or stop a PAS for OpenEdge instance](#) on page 109.

## Deploy web application

To deploy a web application into an ABL application on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.

The **PAS for OpenEdge Instances** page appears, listing all the instances associated with the currently configured OpenEdge Command Center agents.

2. Select the checkbox next to the instance on which you want to deploy the web application. The **Applications** pane appears at the bottom of the page.

- Click **Deploy**. The **Deploy Application** dialog box appears.
- Select the **Web Application** option as the application type.
- In the **Select ABL Application** field, type a new ABL application name or select an existing one from the list.

---

**Note:** If you type a new ABL application name, an ABL application with that name will be created and the web application will be deployed into it.

---

- In the **Select Application File** field, click **Select File** to browse to the location of the WAR file containing the web application and select the file.

---

**Note:**

- If you are deploying a WAR file into an ABL application that already contains web applications with the same names as those included in the WAR file, you must undeploy the existing applications first.
  - You can upload a WAR file only if its size is less than or equal to 523,239,424 bytes (499 MB). If you want to upload a larger file, update the `system-config.json` file by adding the `maxFileUploadSize` parameter with appropriate value and restart the OpenEdge Command Center server. The maximum value you can set is 3,221,225,472 bytes (3 GB). For more information, see [OpenEdge Command Center server configuration](#) on page 37.
- 

- In the **Web Application Name** field, type the name of the web application.

The web application name is automatically detected from the WAR file and is displayed in the **Web Application Name** field, by default. You can change the application name, if needed.

- Based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, the dialog box displays either the **Deploy** or **Deploy & Restart** button. The following table summarizes different scenarios:

If		Then	
Status of PAS for OpenEdge instance	Status of Apache Tomcat Manager Application	Deploy Application dialog box displays	Required action
Running	Deployed	The <b>Enter Apache Tomcat Manager credentials</b> section and the <b>Deploy</b> button	Enter the credentials and click <b>Deploy</b> .
Running	Not deployed	The <b>Deploy &amp; Restart</b> button	Click <b>Deploy &amp; Restart</b> .
Stopped	NA	The <b>Deploy</b> button	Click <b>Deploy</b> .

---

**Note:** If you enter incorrect credentials, the application deployment becomes a normal deployment, requiring the PAS for OpenEdge instance to restart.

---



A popup window appears, displaying the notification message that the deploy operation is successfully submitted. You can click the bell icon to refresh and view the deployment status. After the successful deployment, the web application appears in the **Web Application** section.

## Undeploy ABL application

To undeploy an ABL application from a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.  
The **PAS for OpenEdge instance** page appears, listing all the instances associated with the currently configured OpenEdge Command Center agents.
2. Select the checkbox next to the instance from which you want to undeploy the ABL application. The **Applications** pane appears at the bottom of the page.
3. In the **ABL Applications** section, select the checkbox next to the ABL application that you want to undeploy.
4. From the **Actions** menu, select **Undeploy ABL Application**. The **Undeploy ABL Application** dialog box appears, displaying either the **Undeploy** or **Undeploy & Restart** button, based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application.
5. Based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, the dialog box displays either the **Undeploy** or **Undeploy & Restart** button. The following table summarizes different scenarios:

If		Then	
Status of PAS for OpenEdge instance	Status of Apache Tomcat Manager Application	Undeploy ABL Application dialog box displays	Required action
Running	Deployed	The <b>Enter Apache Tomcat Manager credentials</b> section and the <b>Undeploy</b> button	Enter the credentials and click <b>Undeploy</b> .
Running	Not deployed	The <b>Undeploy &amp; Restart</b> button	Click <b>Undeploy &amp; Restart</b> .
Stopped	NA	The <b>Undeploy</b> button	Click <b>Undeploy</b> .

A popup window appears, displaying the message that the undeploy operation is successfully submitted. You can click the bell icon to refresh and view the undeployment status. After the successful undeployment, the ABL application no longer appears in the **ABL Applications** section of the **Applications** pane.

## Undeploy web applications

To undeploy one or more web applications from an ABL application on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.  
The **PAS for OpenEdge Instances** page appears, listing all the instances associated with the currently configured OpenEdge Command Center agents.
2. Select the checkbox next to the instance that contains the ABL application from which you want to undeploy the web applications. The **Applications** pane appears at the bottom of the page.
3. In the **ABL Applications** section, select the checkbox next to the ABL application that contains the web applications that you want to undeploy. The web applications associated with the ABL application appear in the **Web Application** section.
4. Select the checkbox next to each web application that you want to undeploy.
5. From the **Actions** menu, select **Undeploy Web Applications**. The **Undeploy Web Applications** dialog box appears.
6. Based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, the dialog box displays either the **Undeploy** or **Undeploy & Restart** button:

If		Then	
Status of PAS for OpenEdge instance	Status of Apache Tomcat Manager Application	Undeploy Web Applications Dialog Box displays	Required action
Running	Deployed	The <b>Enter Apache Tomcat Manager credentials</b> section and the <b>Undeploy</b> button	Enter the credentials and click <b>Undeploy</b> .
Running	Not deployed	The <b>Undeploy &amp; Restart</b> button	Click <b>Undeploy &amp; Restart</b> .
Stopped	NA	The <b>Undeploy</b> button	Click <b>Undeploy</b> .

A popup window appears, displaying the notification message that the undeploy operation is successfully submitted. You can click the bell icon to refresh and view the undeployment status. After the successful undeployment, the web application no longer appears in the **Web Applications** section.

---

**Note:** If you undeploy all the web applications from an ABL application, the ABL application is automatically undeployed from the PAS for OpenEdge instance.

---

## Manage PAS for OpenEdge instances

This topic describes how you can manage PAS for OpenEdge instances using OpenEdge Command Center.

### Create a PAS for OpenEdge instance

To create a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.

The console displays a screen that lists all PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.

2. Click **New**.

The **New PAS Instance** screen is displayed. Use this screen to specify the following details:

In the following field . . .	. . . do the following
<b>Instance Name</b>	<p>Specify a name for the PAS for OpenEdge instance. This is a mandatory field.</p> <hr/> <p><b>Note:</b> The PAS for OpenEdge instance name is case-sensitive. It can include any character except periods (.) or square brackets ([ ]). The name must be unique among all configured PAS for OpenEdge instance names.</p> <hr/>
<b>OpenEdge Installation</b>	Use the drop-down box to select the OpenEdge installation that corresponds to the PAS for OpenEdge instance that you want to create.
<b>Labels</b>	Use the drop-down box to select one or more labels, or create one or more new labels to assign.
<b>Security Model</b>	<p>Specify one of the following security models:</p> <ul style="list-style-type: none"> <li>• <b>Production</b> If you select this model, you can make configuration changes to adjust security settings to ensure your application operates correctly in a production instance.</li> <li>• <b>Developer</b> Developer mode minimizes or eliminates any accessibility restrictions, so a developer can quickly use the product “out of the box” to develop, test, and debug applications.</li> </ul>
<b>Instance Directory</b>	<p>Specify the path of the PAS for OpenEdge instance.</p> <hr/> <p><b>Note:</b> If you do not provide the path of the instance directory, the PAS for OpenEdge instance is created in the working directory set during OpenEdge installation. The name of the instance is used as the name of the directory where the PAS for OpenEdge installation is created. The directory must not already exist (either when provided, or when using the default location).</p> <hr/>

In the following field . . .	. . . do the following
<b>HTTP Port</b>	<p>Specify an unused port number to be associated with the PAS for OpenEdge instance HTTP port. By default, this is set to 8080.</p> <hr/> <p><b>Note:</b> Each new PAS for OpenEdge instance that you create uses the default configuration. However, the port number must be unique for each PAS for OpenEdge instance for the instance to operate properly. If you specify a port number that is used by another PAS for OpenEdge instance, you are prompted to confirm whether you want to use the port number.</p> <hr/>
<b>HTTPS Port</b>	<p>Specify an unused port number associated with the PAS for OpenEdge instance HTTPS port. By default, this is set to 8443.</p> <hr/> <p><b>Note:</b> If you specify a port number that is used by another PAS for OpenEdge instance, you are prompted to confirm whether you want to use the port number.</p> <hr/>
<b>Shutdown Port</b>	<p>Specify an unused port number for shutdown. If you are creating a PAS for OpenEdge instance on a Windows machine, this is a mandatory field.</p> <hr/> <p><b>Note:</b> If you specify a port number that is used by another PAS for OpenEdge instance, you are prompted to confirm whether you want to use the port number.</p> <hr/>
<b>Login</b>	<p>Enter the login ID of the Apache Tomcat Manager web application that hosts the PAS for OpenEdge instance. If you are using the Apache Tomcat Web server shipped with OpenEdge, then the default login ID is <code>tomcat</code>.</p>
<b>Password</b>	<p>Enter the password of the Apache Tomcat Manager web application that hosts the PAS for OpenEdge instance. If you are using the Apache Tomcat Web server shipped with OpenEdge, then the default password is <code>tomcat</code>.</p>

- If you want to start the PAS for OpenEdge instance immediately after creating it, make sure that the **Start PAS instance after it is created** is enabled.
- To enable online deployment of ABL applications for your PAS for OpenEdge instance, select the '**Deploy Manager application to enable online deployment**' option. If you select the option for a developer instance

of PAS for OpenEdge, all web applications, such as `manager` and `oemanager`, are deployed. If you select the option for a production instance of PAS for OpenEdge, only the Manager web application is deployed. OpenEdge Command Center uses the Manager application to load the application deployment status in PAS for OpenEdge.

5. Click **Create PAS Instance**.

## Start or stop a PAS for OpenEdge instance

From the OpenEdge Command Center console, you can start or stop one or more local PAS for OpenEdge instances.

To start or stop one or more PAS for OpenEdge instances:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.  
The console displays a screen that lists all PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.
2. Select the check box for each PAS for OpenEdge instance that you want to start or stop.

---

**Note:** You can start or stop a PAS for OpenEdge instance depending on what its current status is.

---

3. From the **Actions** menu, select **Start** or **Stop**, as appropriate.  
A notification popup is displayed that shows the start or stop operation in progress.
4. Click the **Refresh** button to view the change in status of the corresponding PAS for OpenEdge instance.

---

**Note:** After you initiate a stop operation for multiple PAS for OpenEdge instances, a notification message is displayed indicating the stop operation is successfully initiated. You can see the success or failure of each PAS for OpenEdge instance stop operation from the separate notifications section.

---

## Delete a PAS for OpenEdge instance

To delete one or more PAS for OpenEdge instances:

1. In the OpenEdge Command Center console, click **PASOE Instances**.  
The console displays a screen that lists all PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.
2. Select the check box for each PAS for OpenEdge instance that you want to delete.
3. In the **Actions** menu, click **Stop**, if the instances are running.
4. In the **Actions** menu, click **Delete**.

A confirmation dialog box is displayed, prompting you to confirm your selection.

5. In the confirmation dialog box, beneath the field labeled **Type delete to confirm**, enter `delete` and click **Delete**.

---

**Note:** After you initiate a delete operation for a PAS for OpenEdge instance, a notification message is displayed indicating that the delete operation is successfully initiated. You can see the success or failure of each PAS for OpenEdge instance delete operation from the separate notifications section.

---

## Obtain process details

On the **PAS for OpenEdge Instances** screen, you can view the following information about the Progress Application Server (PAS for OpenEdge instances):

- Name—Name of the PAS for OpenEdge instance.
- Labels—Any labels that are assigned to that server, for example: test, production, development.
- Status—If the PAS for OpenEdge instance is running.
- Hostname—Name of the machine where the instance is hosted.
- Install path—The location where the instance is installed on the agent.
- Version—The version of the PAS for OpenEdge instance.

To view the process details for a running PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **PASOE instances** tab.

The console displays a screen that lists all PAS for OpenEdge instances that are associated with all currently configured OpenEdge Command Center agents.

2. Select the check box for the PAS for OpenEdge instance for which you want to obtain process details.
3. In the **Actions** menu, click **Details**.

The Process Details window is displayed, showing the following information for each process that is running in the instance:

- Process type
- PID
- State
- CPU usage
- Memory usage
- Timestamp displaying when the process was started

---

**Note:** The Process Details window is not dynamically refreshed. To obtain the latest process details for the instance, click the refresh button.

---

## Manage ABL applications, web applications, and REST services

The **ABL Applications** tab enables you to manage ABL applications deployed across multiple PAS for OpenEdge instances. The tab provides a consolidated view of ABL applications across multiple PAS for OpenEdge instances and the associated web applications and REST services.

This topic discusses how to manage ABL applications and their components using the **ABL Applications** tab.

## View ABL applications across multiple PAS for OpenEdge instances

To view the ABL applications across multiple PAS for OpenEdge instances, click the **ABL Applications** tab in the OpenEdge Command Center console. The **ABL Applications** page appears, displaying a list of ABL applications and PAS for OpenEdge instances where the applications are deployed. By default, the first ABL application listed on this page is selected, and its details appear in the **Web Applications** and **Services** panes. You can view the details of any other listed ABL application by selecting it. The panes update automatically to display the details of the selected application.

You can sort the list by clicking the column header, and then clicking the arrow next to the header to toggle between ascending (A to Z) and descending (Z to A) order.

If the list of ABL applications is very long, you can filter them by entering an appropriate search string. You can filter the ABL applications based on their name, host name, and the PAS for OpenEdge instance they are deployed on.

The list of ABL applications is automatically refreshed periodically. However, to manually refresh the list, click the refresh icon.

From this page, you can deploy and undeploy ABL applications, web applications, and services. For more information, see [Manage ABL applications](#) on page 112.

If you click any ABL application, the **Edit ABL Application** page appears, where you can view, filter, and edit the properties of the corresponding ABL application. For more information, see [Edit ABL application](#) on page 117.

### Web Applications pane

The **Web Applications** pane displays the web applications deployed on the ABL application selected on the **ABL Applications** page. The details of web applications are displayed in separate cards. Each card displays the following information about a web application:

- Name
- Service Count
- Path
- URI
- Secure URI

You can sort the web application cards by name or service counts. Click the **Refresh** button in the **Web Applications** pane to refresh the pane and the corresponding **Services** pane.

For more information about managing web applications, see [Manage web applications](#) on page 114.

### Services pane

The **Services** pane displays the services deployed on the web application selected in the Web Applications pane. The details of services are displayed in separate cards. Each card displays the following information about a service:

- URI
- Secure URI
- Service Version
- Service Descriptor
- Service Location

You can sort the service cards by name. To refresh the content in the **Services** pane, click the refresh button.

---

**Note:** Currently, only REST services are displayed in the **Services** pane.

---

For more information about managing services, see [Manage REST services](#) on page 116.

## Manage ABL applications

You can manage ABL applications from the **ABL Applications** page by performing the following tasks:

- Deploy ABL applications
- Undeploy ABL applications

### Deploy ABL application

To deploy an ABL application on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.  
The **ABL Applications** page appears, listing all ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.
2. On the **ABL Applications** page, click **Actions > Deploy**. The **Deploy Application** dialog box appears.
3. In the **Select PASOE Instance** drop-down list, expand the agent node and then select the PAS for OpenEdge instance on which you want to deploy the ABL application.
4. Select the **ABL Application** option as the application type.
5. In the **Select Application File** field, click **Select File** to browse to the location of the OpenEdge Archive (OEAR) file containing the ABL application and select the file.

---

**Note:**

- You can deploy ABL applications as an OEAR file only. For information about the OEAR file, see "Create an OpenEdge Application Archive using tcman export" and "Create an OpenEdge Application Archive using an Ant Build" in *Manage Progress Application Server (PAS) for OpenEdge*.
  - If you are deploying an OEAR file on an instance that already contains ABL applications or web applications with the same names as those included in the OEAR file, you must undeploy the existing applications first.
  - The OEAR file does not need to have the same name as the ABL application.
  - You can upload an OEAR file only if its size is less than or equal to 523,239,424 bytes (499 MB). If you want to upload a larger file, update the `system-config.json` file by adding the `maxFileUploadSize` parameter with appropriate value and restart the OpenEdge Command Center server. The maximum value you can set is 3,221,225,472 bytes (3 GB). For more information, see [OpenEdge Command Center server configuration](#) on page 37.
- 

6. Based on the status of the PAS for OpenEdge instance, the dialog box displays either the **Deploy** or **Deploy & Restart** button. The following table summarizes different scenarios:



If	Then	
Status of PAS for OpenEdge Instance	Deploy Application dialog box displays	Required action
Running	The <b>Deploy &amp; Restart</b> button	Click <b>Deploy &amp; Restart</b> .
Stopped	The <b>Deploy</b> button	Click <b>Deploy</b> .

**Note:** The deployment of the ABL application on the PAS for OpenEdge instance is independent of the deployment status of the Apache Tomcat Manager application.

A popup window appears, displaying the notification that the deploy operation is successfully submitted. You can click the bell icon to refresh and view the deployment status. After the successful deployment, the ABL application appears on the **ABL Applications** page.

**Note:** If an ABL application is deployed on a stopped PAS for OpenEdge instance, you must start the instance to access the ABL application services. For information on how to start a PAS for OpenEdge instance, see [Start or stop a PAS for OpenEdge instance](#) on page 109.

## Undeploy ABL application

To undeploy an ABL application from a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.

The **ABL Applications** page appears, listing all ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.

2. Select the ABL application you want to undeploy, and click **Actions > Undeploy**. The **Undeploy ABL Application** dialog box appears.
3. Undeploy the ABL application. Based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, the dialog box displays either the **Undeploy** or **Undeploy & Restart** button. The following table summarizes different scenarios:

If		Then	
Status of PAS for OpenEdge instance	Status of Apache Tomcat Manager Application	Undeploy ABL Application dialog box displays	Required action
Running	Deployed	The <b>Enter Apache Tomcat Manager credentials</b> section and the <b>Undeploy</b> button	Enter the credentials and click <b>Undeploy</b> .
Running	Not deployed	The <b>Undeploy &amp; Restart</b> button	Click <b>Undeploy &amp; Restart</b> .
Stopped	NA	The <b>Undeploy</b> button	Click <b>Undeploy</b> .

A popup window appears, displaying the notification that the undeploy operation is successfully submitted. You can click the bell icon to refresh and view the undeployment status. After the successful undeployment, the ABL application no longer appears on the **ABL Applications** page.

For information about securing ABL applications, see [Secure online deployment of a new ABL application](#).

## Manage web applications

You can manage web applications from the **ABL Applications** tab by performing the following tasks:

- Deploy web applications
- Undeploy web applications

### Deploy web application

To deploy a web application into an ABL application on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.  
The **ABL Applications** page appears, listing all ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.
2. Click **Actions > Deploy**. The **Deploy Application** dialog box appears.
3. In the **Select PASOE Instance** drop-down list, expand the agent node and then select the PAS for OpenEdge instance on which you want to deploy the web application.
4. Select the **Web Application** option as the application type.
5. In the **Select ABL Application** field, type a new ABL application name or select the existing one from the drop-down list.

---

**Note:** If you type a new ABL application name, an ABL application with that name will be created and the web application will be deployed into it.

---

6. In the **Select Application File** field, click **Select File** to browse to the location of the WAR file containing the web application and select the file.

---

**Note:**

- If you are deploying a WAR file into an ABL application that already contains web applications with the same names as those included in the WAR file, you must undeploy the existing applications first.
  - You can upload a WAR file only if its size is less than or equal to 523,239,424 bytes (499 MB). If you want to upload a larger file, update the `system-config.json` file by adding the `maxFileUploadSize` parameter with appropriate value and restart the OpenEdge Command Center server. The maximum value you can set is 3,221,225,472 bytes (3 GB). For more information, see [OpenEdge Command Center server configuration](#) on page 37.
- 

7. In the **Web Application Name** field, type the name of the web application.

**Note:** The web application name is automatically detected from the WAR file and is displayed in the **Web Application Name** field by default. You can change the application name if needed.

8. Based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, the dialog box displays either the **Deploy** or **Deploy & Restart** button. The following table summarizes different scenarios:

If		Then	
Status of PAS for OpenEdge instance	Status of Apache Tomcat Manager Application	Deploy Application dialog box displays	Required action
Running	Deployed	The <b>Enter Apache Tomcat Manager credentials</b> section and the <b>Deploy</b> button	Enter the credentials and click <b>Deploy</b> .
Running	Not deployed	The <b>Deploy &amp; Restart</b> button	Click <b>Deploy &amp; Restart</b> .
Stopped	NA	The <b>Deploy</b> button	Click <b>Deploy</b> .

**Note:** If you enter the incorrect Manager credentials, the application deployment becomes a normal deployment and requires the PAS for OpenEdge instance to restart.

A popup window appears, displaying the notification that the deploy operation is successfully submitted. You can click the bell icon to refresh and view the deployment status. After the successful deployment, the web application appears in the **Web Application** pane when you select the corresponding ABL application.

## Undeploy web application

To undeploy a web application from an ABL application on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.

The **ABL Applications** page appears, listing all ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.

2. Select the ABL application that contains the web application you want to undeploy. The associated web applications appear in the **Web Applications** pane.
3. Locate the card for the web application that you want to undeploy and then click **Undeploy** on the card. The **Undeploy Web Applications** dialog box appears.
4. Based on the status of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, the dialog box displays either the **Undeploy** or **Undeploy & Restart** button:

If		Then	
Status of PAS for OpenEdge instance	Status of Apache Tomcat Manager Application	Undeploy Web Applications dialog box displays	Required action
Running	Deployed	The <b>Enter Apache Tomcat Manager credentials</b> section and the <b>Undeploy</b> button	Enter the credentials and click <b>Undeploy</b> .
Running	Not deployed	The <b>Undeploy &amp; Restart</b> button	Click <b>Undeploy &amp; Restart</b> .
Stopped	NA	The <b>Undeploy</b> button	Click <b>Undeploy</b> .

A popup window appears, displaying the notification that the undeploy operation is successfully submitted. You can the bell icon to refresh and view the undeployment status. After the successful undeployment, the web application no longer appears in the **Web Applications** pane.

## Manage REST services

From the **ABL Applications** tab, you can manage REST services in your web applications by performing the following tasks:

- Deploy services
- Undeploy services

### Deploy services

To deploy a service in an existing web application:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.  
The **ABL Applications** page is displayed.
2. On the **ABL Applications** page, select an ABL application.  
The web applications and services deployed in the selected ABL application are displayed in the **Web Applications** and **Services** pane.
3. In the **Web Applications** pane, select the web application where you want to deploy a service.
4. In the **Services** pane, click **Deploy Service**.  
The **Deploy Service** dialog box is displayed.
5. In the **Select service file** field, click **Select .paar**, browse to the location of the service file ( `.paar` ), and select the file.

**Note:** You can upload a PAAR file only if its size is less than or equal to 523,239,424 bytes (499 MB). If you want to upload a larger file, update the `system-config.json` file by adding the `maxFileUploadSize` parameter with appropriate value and restart the OpenEdge Command Center server. The maximum value you can set is 3,221,225,472 bytes (3 GB). For more information, see [OpenEdge Command Center server configuration](#) on page 37.

6. In the **Service name** field, type a name for the service.

---

**Note:** The name is automatically detected from the service ( `.paar` ) file and is displayed, by default. You can change the service name as desired.

---

7. Click **Deploy**.

A message is displayed confirming that the request to deploy the service is submitted.

8. Optional. Check notifications to view the status of service deployment.
9. After the service is deployed, it appears in the **Services** pane. If the associated web application or ABL application is stopped, you must start it to view the deployed service.

## Undeploy services

To undeploy a service:

1. In the **Services** pane, locate the card of the service you want to undeploy.
2. In the service card, click **Undeploy**.

The **Undeploy Service** box is displayed.

3. Click **Undeploy**.

A message is displayed confirming that the request to undeploy a service is submitted.

4. Optional. Check notifications to confirm if the service was undeployed successfully.

## Edit ABL application

This topic explains how you can filter and edit the properties of an ABL application.

On the **Edit ABL Application** page, you can view, filter, and edit the properties of an ABL application. All the properties are categorized into the following sections.

- MS Agent Startup Configurations
- MS Agent Session Procedures
- MS Agent Procedures
- MS Agent Logging Settings
- Session Manager Performance Tuning and Limit Settings
- Session Manager Timeouts

On this page, you can view a message at the top that displays the information on the current running status of the ABL application. You can use the search field to locate a specific property. You can also use the **Show all runtime updatable properties** toggle button to view the properties that you can modify without restarting the PAS for OpenEdge instance. However, this button is available only when the ABL application is running and enabled for runtime updates.

## Filter ABL application properties

The **Edit ABL application** page displays all the properties of an ABL application. You can use a filter to easily locate the property you want to modify.

To filter the properties of the ABL application:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.  
The **ABL Applications** page appears, listing all the ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.
2. On the **ABL Applications** page, click the name of the ABL application.  
The **Edit ABL Application** page appears, displaying the properties of the corresponding ABL application.
3. In the search field, enter the name, label, or section header of the property to locate it. You can also search the property using its name as specified in the `openedge.properties` file. For example, enter *workDir* (as in the `openedge.properties` file) to locate the **MS Agent Startup Directory** property.  
Only the **MS Agent Startup Directory** property field is displayed on the **Edit ABL Application** page.

## Edit ABL application properties

To edit the properties of an ABL application deployed on a PAS for OpenEdge instance:

1. In the OpenEdge Command Center console, click the **ABL Applications** tab.  
The **ABL Applications** page appears, listing all the ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.
2. On the **ABL Applications** page, click the name of the ABL application whose properties you want to modify.  
The **Edit ABL Application** page appears, displaying the properties of the corresponding ABL application. These properties are categorized into the following sections:
  - MS Agent Startup Configurations
  - MS Agent Session Procedures
  - MS Agent Procedures
  - MS Agent Logging Settings
  - Session Manager Performance Tuning and Limit Settings
  - Session Manager Timeouts
3. In the **MS Agent Startup Configurations** section, you can edit values for the following properties:

Field	Description
<b>MS Agent Startup Directory</b>	Specifies the path to the agent startup working directory.
<b>MS Agent Startup Parameter</b>	Specifies the server and agent startup parameters that each process uses when the broker starts it. For example, you can specify the <code>Database (-db)</code> parameter to connect to the application database. You can update this property dynamically. Dynamic changes affect only new MS Agents that are started after the update.
<b>PROPATH</b>	Specifies the PROPATH, which is a Progress environment variable, that contains a list of directories that the ABL Virtual Machine (AVM) uses to search for files and procedures to run. In this field, you can add, edit, delete, or reorder the PROPATH entries.

4. Click the **MS Agent Session Procedures** section to expand it, and then you can edit the values for the following properties:

Field	Description
<b>Activate Procedure</b>	Specifies the activate procedure for the session. This procedure must be a valid procedure on the PROPATH of the application service.
<b>Deactivate Procedure</b>	Specifies the deactivate procedure for the session. This procedure must be a valid procedure on the PROPATH of the application service.
<b>Connect Procedure</b>	Specifies the connect procedure for the session-managed sessions. This procedure must be a valid procedure on the PROPATH of the application service.
<b>Disconnect Procedure</b>	Specifies the disconnect procedure for session-managed sessions. This procedure must be a valid procedure on the PROPATH of the application service.
<b>Session Startup Procedure</b>	Specifies a startup procedure for the server. This procedure must be a valid procedure on the PROPATH of the application service.
<b>Session Startup Procedure Parameter</b>	Specifies the startup parameter that each session uses when the MS Agent starts it. You can update this property dynamically. Dynamic changes affect only new MS Agents that are started after the update.
<b>Session Shutdown Procedure</b>	Specifies the shutdown procedure for the server. This procedure must be a valid procedure on the PROPATH of the application service.

5. Click the **MS Agent Procedures** section to expand it, and then you can edit the values for the following properties:

Field	Description
<b>MS Agent Startup Procedure</b>	Specifies a startup procedure used for a multi-session agent. This procedure must be a valid procedure on the PROPATH of the application service.
<b>MS Agent Startup Procedure Parameter</b>	Specifies a character parameter that is provided as an input into the <code>agentStartupProc</code> procedure.
<b>MS Agent Shutdown Procedure</b>	Specifies a shutdown procedure that is used for a multi-session agent. This procedure must be a valid procedure on the PROPATH of the application service.

6. Click the **MS Agent Logging Settings** section to expand it, and then you can edit the values for the following properties:

Field	Description
<b>Log File Name</b>	Specifies the MS Agent log file that contains the location, name, and roll-over details of the MS Agent. If you want the MS Agent log file roll-over details at midnight, then add <code>{yyy-MM-dd}</code> . For example: <code>&lt;path-to&gt;/&lt;instance name&gt;.agent.{yyyy-MM-dd}.log</code> .
<b>Logging Level</b>	Specifies the logging level for messages written into the MS Agent log buffer. The acceptable value range is 1 to 4.
<b>Log Entry Types</b>	Specifies a single entry or comma-delimited list of logging entry types for the MS Agent log buffer. By default, this parameter is set to <code>uBroker.basic</code> .

7. Click the **Session Manager Performance Tuning and Limit Settings** section to expand it, and then you can edit the values for the following properties:

Field	Description	Minimum value
<b>Minimum Number of MS Agents</b>	Specifies the minimum number of MS Agents expected to be active at any given time. If the number of MS Agents drops below this threshold, a client request triggers the session manager to start additional MS Agents to match this number.	1
<b>Maximum Number of MS Agents</b>	Specifies the maximum number of concurrent MS Agent operating the system processes that an individual ABL application can start on the AppServer.	1
<b>Initial Number of MS Agents</b>	Specifies the number of MS Agents to be started when the AppServer starts.	1
<b>Maximum Connections per MS Agent</b>	Specifies the maximum number of concurrent TCP connections allowed between the session manager and the MS Agent.	1
<b>Maximum ABL Sessions per MS Agent</b>	Specifies the maximum number of sessions an MS Agent can run.	1
<b>Maximum Number of MS Agents to Start</b>	Specifies the maximum number of MS Agents that can be started simultaneously. If this value is set to zero or not defined, no limit is enforced.	0

8. Click the **Session Manager Timeouts** section to expand it, and then you can edit the values for the following properties:



Field	Description	Minimum value
<b>Request Wait Timeout</b>	Specifies the maximum amount of time in milliseconds, for which a request waits in the session manager for a connection to become available before the request is rejected.	0
<b>Connection Wait Timeout</b>	Specifies the maximum amount of time in milliseconds, for which the session manager waits for a connection to be freed before creating a new connection.	0
<b>Idle MS Agent Timeout</b>	Specifies the timeout value in milliseconds, for an idle MS Agent. If an MS Agent is idle for longer than the specified timeout value, the session is deleted when the <code>idleResource</code> cleanup is done.	0
<b>Idle Connection Timeout</b>	Specifies the timeout value in milliseconds, between an AppServer client and the session manager. If a connection is idle for longer than the specified timeout value, the session manager terminates the connection by automatically disconnecting it from the AppServer.	0
<b>Idle Resource Timeout</b>	Specifies the timeout value, in milliseconds, to determine the frequency with which the PAS for OpenEdge server checks for idle resources. Any resource (for example, connection, MS Agent, or client session) that is not accessed for longer than the specified timeout for that property, will be terminated. If this property is set to zero, idle resource checking is disabled.	0
<b>Idle Session Timeout</b>	Specifies the timeout value in milliseconds for an idle session in the session manager. When using HTTP sessions, the APSV transport uses this value to set the expiration time of the HTTP session, which defaults to 30 minutes and is the same value that other transports use. The expiration of HTTP sessions is controlled in <code>web.xml</code> and does not require <code>idleResourceTimeout</code> to be set because it is managed by Tomcat.	0
<b>MS Agent Listener Timeout</b>	Specifies the maximum amount of time in milliseconds for which the session manager waits for an MS Agent to start, when the connection is established.	0

9. After editing the required properties, click **Apply**.

The **Confirm Changes** dialog box appears, displaying the details of the edited properties. The buttons in the dialog box vary depending on the running status of the ABL application and type of the properties edited:

- If the ABL application is running and you have edited:
  - Runtime updatable properties — the dialog box displays **Save** and **Cancel** buttons. Click **Save** to apply your changes.
  - Both types of properties or only the properties that require restart of the PAS for OpenEdge instance — the dialog box displays **Save**, **Save and Restart**, and **Cancel** buttons:

- When you click **Save**, changes to the properties that do not require a restart of the PAS for OpenEdge instance are applied immediately, while changes to those properties requiring a restart will be applied after the PAS for OpenEdge instance restarts.
- When you click **Save and Restart**. The **Confirm Restart** popup window appears. In the **Type restart to confirm** field, type *restart* and click **Restart** to restart the PAS for OpenEdge instance and apply changes to the properties. The ABL application will be unavailable during the restart.
- If the ABL application is not running, the dialog box displays only **Save** and **Cancel** buttons, irrespective of the type of properties edited. Click **Save** to save your changes. The changes to the properties will be applied after the ABL application is in running state.

## Create users and manage roles using Authorization server

The Authorization server employs a Role-Based Access Control (RBAC) to manage access to systems and their resources, including the OpenEdge Command Center server, the OpenEdge Command Center agent, and the Authorization server itself. It assigns permissions to specific roles instead of individual users, simplifying the administration of access control.

You can create users and assign or remove roles for a specific user in the Authorization server using the Authorization server REST APIs. This chapter covers tasks, such as logging in, creating users, assigning and removing roles with examples, and frequently asked questions.

---

**Note:** The instructions in this chapter are written for Swagger UI, however, you can perform similar tasks using Postman.

---

### Prerequisites

You must have the `AUTHZ_ADMIN` role to access the Authorization server and perform the tasks, such as creating users and managing roles in the Authorization server.

## Log in to Authorization server

You can log in to the Authorization server as a user with the necessary privileges using both the OpenEdge Command Center server and Authorization server REST APIs.

To log in to the Authorization server:

1. Open a web browser and access the Swagger UI of the OpenEdge Command Center server by navigating to `https://<hostname>:<port>/openapi/`
2. Locate the `Authenticate your session` API with endpoint `POST-/api/auth/login` and expand it.
3. To enable the text area, click **Try it out**.

4. In **Request body**, type `admin` as username and password details in JSON format:

```
{
  "userName": "admin"
  "password": "<password>"
}
```

5. Click **Execute**. If authentication is successful, you see a JWT token in JSON format. For example:

```
{
  "idToken": "eyJhbGciOiJIUzI1NiJ9.eyJpZCI6ImFkbWluIiwiaWF0IjoxNTk1NDg2ODY3fQ.PZDjDXkQvpmSHWYXpt8JcYGeqEWX_8ehZonMY2aFHaa",
  "expiresIn": 240
}
```

6. Open another web browser and access the Swagger UI of the Authorization server by navigating to :  
`https://<hostname>:<port>/openapi-authz/`

7. Click **Authorize**.

8. In the **Available authorizations** dialog box, perform the following steps:

- a) In the **Value** field, enter the JWT token that you obtained in Step 5.
- b) Click **Authorize** and **Close**.

After successful authorization, you can create users, assign roles, and remove roles in the Authorization server.

## Create a user

The `Create a user` API enables you to create a user in the Authorization server.

---

**Note:** Before you begin, ensure that you have created that specific user in the OpenEdge Command Center server.

---

To create a user in the Authorization server:

1. Log in to the Authorization server as a user with necessary privileges. For more information, see [Log in to Authorization server](#) on page 122.
2. Locate the `Create a user` API with endpoint `POST-/authz/api/users` and expand it.
3. To enable the text area, click **Try it out**.
4. In **Request body**, type the username in JSON format:

```
{
  "userName": "<Valid username>"
}
```

where, `userName` is the name of the user that you want to create.

5. Click **Execute**.

If the user creation is successful, you see the following success message.

```
{
  "message": "Request successful. The user is created in the Authorization Server."
}
```

## Assign roles to a user

You can assign roles to users for granting them the required permission to access a system and perform specific tasks.

To assign roles to a user:

1. Log in to the Authorization server as a user with necessary privileges. For more information, see [Log in to Authorization server](#) on page 122.
2. Locate the Assign or remove roles API with endpoint `PUT-/authz/api/users` and expand it.
3. To enable the text area, click **Try it out**.
4. In the **Parameters** section, select `assignRoles` for the **action** parameter.
5. In **Request body**, provide user details and roles in JSON format, as follows:

```
{
  "userName": "string",
  "rolesToAssign": [{
    "roleURN": "string",
    "system": "string"
  }]
}
```

The following table describes the attributes in the request body:

Attribute name	Description
userName	Specifies the user to whom the roles need to be assigned.
roleURN	<p>Identifies the roles within the Authorization server. It indicates what a specific role can access and where it is used. Its format includes the resource name it represents, role name, and, partition IDs (only when assigning roles to a user for an agent).</p> <p>The following are the possible values:</p> <ul style="list-style-type: none"> <li>• <code>role:oecc/oecc_admin</code></li> <li>• <code>role:authz/authz_admin</code></li> <li>• <code>role:agent/&lt;partitionid&gt;/agent_admin</code></li> <li>• <code>role:agent/&lt;partitionid&gt;/agent_resource_user</code></li> </ul> <p>For more information about roleURN, see <a href="#">Roles in Authorization server</a> on page 16.</p> <p>If you enter <code>role:agent/&lt;partitionid&gt;/agent_admin</code> or <code>role:agent/&lt;partitionid&gt;/agent_resource_user</code> as a roleURN value, you can get the agent partition ID using the Retrieve specific agent details API on the OpenEdge Command Center server. For more information, see "Retrieve specific agent details" in <i>OpenEdge Command Center REST API Reference</i>.</p>
system	<p>Specifies the system on which the user with a specific role can access and perform tasks. The possible values are:</p> <ul style="list-style-type: none"> <li>• <code>oecc</code> - Indicates the OpenEdge Command Center server.</li> <li>• <code>authz</code> - Indicates the Authorization server.</li> <li>• <code>&lt;partitionid&gt;</code> - Indicates the partition ID of the OpenEdge Command Center agent.</li> </ul>

**6. Click Execute.**

If the roles assignment is successful, you see the response body in this format:

```
{
  "message": "Request successful. Roles are assigned to \"userName\"."
}
```

**Example: Assign OECC\_ADMIN and AUTHZ\_ADMIN roles**

This example demonstrates the request and response bodies for assigning the OECC\_ADMIN and AUTHZ\_ADMIN roles to the user named, James.Smith. This action grants the user access to the oecc (OpenEdge Command Center server) and authz (Authorization server) systems to do the following tasks:

System	Tasks
oecc	Manage the OpenEdge Command Center server, including viewing the details of server and database settings.
authz	Log in to the Authorization server and perform these tasks: <ul style="list-style-type: none"><li>• Create users</li><li>• Manage roles</li></ul>

**Request body**

Following are the contents of the request body in JSON format:

```
{
  "userName": "James.Smith",
  "rolesToAssign": [
    {
      "roleURN": "role:oecc/oecc_admin",
      "system": "oecc"
    },
    {
      "roleURN": "role:authz/authz_admin",
      "system": "authz"
    }
  ]
}
```

**Response body**

Following are the contents of the response body in JSON format:

```
{
  "message": "Request successful. Roles are assigned to \"James.Smith\"."
}
```

## Example: Assign AGENT\_ADMIN and AGENT\_RESOURCE\_USER roles

This example demonstrates the request and response bodies for assigning the AGENT\_ADMIN and AGENT\_RESOURCE\_USER roles to the user named, Sarah.Jones to access the oecagent1 OpenEdge Command Center agent that has partition ID as db7253b679d9abc133904d4bf59d75f110c7023e57184d351be187f631d58ab8. This role assignment grants access of OpenEdge Command Center agent to the user, to do the following tasks:

- Perform actions on OpenEdge resources, including PAS for OpenEdge instances and OpenEdge databases that the agent manages.
- Log in to the Authorization server, create users, and assign the AGENT\_ADMIN and AGENT\_RESOURCE\_USER roles to the user named Sarah.Jones .

### Request body

Following are the contents of the request body in JSON format:

```
{
  "userName": "Sarah.Jones",
  "rolesToAssign": [{
    "roleURN":
"role:agent/db7253b679d9abc133904d4bf59d75f110c7023e57184d351be187f631d58ab8/agent_admin",
    "system": "db7253b679d9abc133904d4bf59d75f110c7023e57184d351be187f631d58ab8"
  }, {
    "roleURN":
"role:agent/db7253b679d9abc133904d4bf59d75f110c7023e57184d351be187f631d58ab8/agent_resource_user",
    "system": "db7253b679d9abc133904d4bf59d75f110c7023e57184d351be187f631d58ab8"
  }]
}
```

### Response body

Following are the contents of the response body in JSON format:

```
{
  "message": "Request successful. Roles are assigned to \"Sarah.Jones\"."
}
```

## Remove roles from a user

Remove roles from a user to ensure that they no longer have permissions to access the system.

To remove roles from a user:

1. Log in to the Authorization server as an admin user. For more information, see [Log in to Authorization server](#) on page 122.
2. Locate the `Assign or remove roles` API with endpoint `PUT-/authz/api/users` and expand it.
3. To enable the text area, click **Try it out** to enable the text area.
4. In the **Parameters** section, select `removeRoles` for the **action** parameter.
5. In **Request body**, provide user details and roles in JSON format.

```
{
  "userName": "string",
  "rolesToRemove": [
    "string"
  ]
}
```

The following table describes the attributes in the request body:

Attribute name	Description
userName	Specifies the user whose roles need to be removed.
roleURN	Identifies the role that needs to be removed from the user. For more information about roleURN, see <a href="#">Roles in Authorization server</a> on page 16.

6. Click **Execute**. If the removal of roles is successful, you see the response body in this format:

```
{
  "message": "Request successful. These roles are removed for the user \"userName\": \"roleURN\" "
}
```

## Example

The following example demonstrates the request and response bodies for removing the `AUTHZ_ADMIN` role for the user named, `JessicaWilson`.

### Request body

Following are the contents of the request body in JSON format:

```
{
  "userName": "JessicaWilson",
  "rolesToRemove": [
    "role:authz/authz_admin"
  ]
}
```

### Response body



Following are the contents of the response body in JSON format:

```
{
  "message": "Request successful. These roles are removed for the user \"JessicaWilson\": \"role:authz/authz_admin\""
}
```

## Frequently Asked Questions

This topic covers common scenarios for managing user access to OpenEdge Command Center agent and its OpenEdge resources.

### How do I give a new user access to an existing OpenEdge Command Center agent to manage its OpenEdge resources?

To give a new user access to an existing OpenEdge Command Center agent to manage the OpenEdge resources, ensure that the following prerequisites are met, and then complete the steps:

#### Prerequisites

- You have the `AGENT_ADMIN` role for the agent.
- The new user is already created in the OpenEdge Command Center server.
- You have obtained the agent partition ID for the agent using the `Retrieve specific agent details` API on the OpenEdge Command Center server. For more information, see "Retrieve specific agent details" in *OpenEdge Command Center REST API Reference*.

#### Steps

1. Log in to the Authorization server as a user with the required privileges. For more information, see [Log in to Authorization server](#) on page 122.
2. Create the user in the Authorization server. For more information, [Create a user](#) on page 123.
3. Assign the `AGENT_RESOURCE_USER` role to the user. For more information, see [Assign roles to a user](#) on page 124.

### How do I give an existing user access to a new OpenEdge Command Center agent?

To give an existing user access to a new OpenEdge Command Center agent for managing OpenEdge resources and assigning roles to other users in the Authorization Server, ensure that the following prerequisites are met, and then complete the steps:

#### Prerequisites

- You have the `AGENT_ADMIN` role for the agent.
- You have obtained the agent partition ID for the new OpenEdge Command Center agent using the `Retrieve specific agent details` API on the OpenEdge Command Center server. For more information, see "Retrieve specific agent details" in *OpenEdge Command Center REST API Reference*.

### Steps

1. Log in to the Authorization server as a user with the required privileges. For more information, see [Log in to Authorization server](#) on page 122.
2. Assign the `AGENT_ADMIN` and `AGENT_RESOURCE_USER` roles to the user. For more information, see [Assign roles to a user](#) on page 124.

## Set up TLS for OpenEdge Command Center and MongoDB communication

You can enable TLS for secure communication between the OpenEdge Command Center server and MongoDB. You can configure the following types of authentication:

- Server authentication
- Mutual authentication

### Server authentication

When using server authentication, the MongoDB server sends a certificate to the OpenEdge Command Center server to authenticate itself and ensure secure communication. To configure TLS server authentication:

1. In MongoDB installation, open the `bin/mongod.cfg` file in an editor.

---

**Note:** If the MongoDB installation is on the Linux platform, open the `etc/mongod.conf` file.

---

2. In the `network interface` section of the file, add the `tls` node.
3. In the `tls` node, add the following fields and enter the required values:

Field	Description
<code>mode</code>	Set value to <code>requireTLS</code> or <code>preferTLS</code> .
<code>certificateKeyFile</code>	Path of the public certificate of the MongoDB server that is signed by the Certificate Authority (CA).

4. Save your changes to the `bin/mongod.cfg` or `etc/mongod.conf` file and restart the MongoDB server.
5. In the OpenEdge Command Center server installation, open the `data/conf/db-config.json` file in an editor.
6. Add the `tls` field and set its value to `true`.
7. In `connectionOptions`, add the `sslCA` field.
8. For `sslCA`, enter the path of the public certificate of the CA that is used to validate the certificates presented by the OpenEdge Command Center server.
9. Save your changes to the `data/conf/db-config.json` file and restart the OpenEdge Command Center server.

After the OpenEdge Command Center server is started, the TLS handshake with the MongoDB server occurs and a secure channel is established.

## Mutual authentication

When using mutual authentication, the OpenEdge Command Center server and the MongoDB server authenticate with each other before creating a secure communication channel. To configure TLS mutual authentication:

1. In MongoDB installation, open the `bin/mongod.cfg` file in an editor.

---

**Note:** If the MongoDB installation is on the Linux platform, open the `etc/mongod.conf` file.

---

2. In the `network interface` section of the file, add the `tls` node.
3. In the `tls` node, add the following fields and enter the required values:

Field	Description
<code>mode</code>	Set value to <code>requireTLS</code> or <code>preferTLS</code> .
<code>certificateKeyFile</code>	Path of the public certificate of the MongoDB server that is signed by the CA.
<code>CAFile</code>	Path of the file that contains the certificate chain for verifying the OpenEdge Command Center server's certificates.

4. Save your changes to the `bin/mongod.cfg` or `etc/mongod.conf` file and restart the MongoDB server.
5. In the OpenEdge Command Center server installation, open the `data/conf/db-config.json` file in an editor.
6. Add the `tls` field and set its value to `true`.
7. In `connectionOptions`, add the following fields and enter the required values:

Field	Description
<code>sslCA</code>	Path of the public certificate of the CA that is used to validate the certificates presented by the MongoDB server.
<code>sslKey</code>	The private key used for encryption.
<code>sslCert</code>	Path of the public certificate of the OpenEdge Command Center server that is signed by the CA.

8. Save your changes to the `data/conf/db-config.json` file and restart the OpenEdge Command Center server.

After the OpenEdge Command Center server is started, the TLS handshake with the MongoDB server occurs and a secure channel is established.

For more information about configuring MongoDB for TLS, see the following articles:

- <https://docs.mongodb.com/manual/tutorial/configure-ssl/>
- <https://docs.mongodb.com/manual/tutorial/configure-ssl-clients/>

# Monitor OpenEdge resources using the OpenEdge Command Center agent

The OpenEdge Command Center agents can collect performance metrics of the following OpenEdge resources:

- OpenEdge database
- PAS for OpenEdge

The OpenEdge Command Center agent supports 12.2 and later versions of these OpenEdge resources.

Administrators can use these metrics to understand performance issues and accordingly tune the OpenEdge resources for optimal performance. The performance metrics are collected using the OpenTelemetry (OTel) standards. For more information about OpenTelemetry, see the [OpenTelemetry](#) documentation.

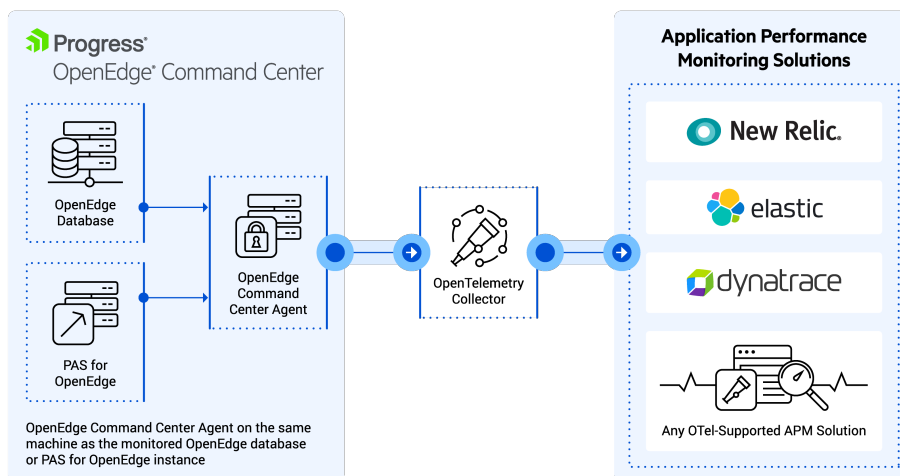
Since OTel is a vendor-agnostic and open-source technology, you can use any market-leading Application Performance Monitoring (APM) vendor solutions, such as Elastic APM, Dynatrace, NewRelic, and so on, to view the performance metrics.

## Deployment architecture for monitoring OpenEdge resources

The components required to monitor OpenEdge resources are as follows:

- OpenEdge Command Center agent
- OTel Collector
- APM tool

The following diagram depicts the deployment architecture for monitoring OpenEdge resources using the OpenEdge Command Center agent:



**OpenEdge Command Center agent**—The OpenEdge Command Center agent is co-located with the OpenEdge resource you want to monitor. The agent monitors the OpenEdge resource, captures the required performance metrics, and then uses OpenTelemetry Protocol (OTLP) to transfer metrics data to OTel Collector.

**OTel Collector**—The OTel Collector is an application that processes telemetry data and sends it out to various destinations. To monitor the OpenEdge resources, the OTel Collector processes the performance metrics data collected by the OpenEdge Command Center agent and then exports it to the APM tool.

**Application Performance Monitoring (APM) tool**—APM tool is software that enables the observation and analysis of application performance. The tools may have data visualization capabilities that help administrators analyze performance and identify the bottlenecks. You can use market-leading APM tools that support the OTel standards, such as Elastic APM, Dynatrace, NewRelic, and so on, to view the performance metrics of OpenEdge resources. The APM tool uses the data exported by the OTel Collector.

## Set up OpenTelemetry Collector

Set up OpenTelemetry (OTel) Collector to collect, process, and export performance metrics data of OpenEdge resources from the OpenEdge Command Center agent to various destinations, such as Application Performance Monitoring (APM) tool.

To set up OTel Collector, perform the following steps:

1. Download and install the appropriate version of OTel Collector for your platform. The minimum supported version is 0.31 and the last certified version is 0.82. For more information about installing OTel Collector, see [OpenTelemetry Collector documentation](#).

---

**Note:** You can install OTel Collector on any system, but Progress recommends installing it on a different system from the one hosting the OpenEdge Command Center agent for optimal performance. You can also configure multiple agents to share performance metrics data with the same OTel Collector.

---

2. Open the `config.yml` file of the OTel Collector installation directory in an editor. For Windows, the `config.yml` file is present at `<OTel Collector installation>/otbin/windows/bin`. For Linux, the file is present at `<OTel Collector installation>/otbin/linux/bin`.

The `config.yml` file contains the following sections:

- **receivers**—Provide details about how OTel Collector can get data from the OpenEdge Command Center agent.
  - **processors**—Provide details about what OTel Collector does with the received data.
  - **exporters**—Provide details about where OTel Collector sends data for the Application Performance Monitoring (APM) tools.
3. In the **receivers** node, ensure that the value of the `endpoint` property is the same as specified for the `exporter.endpoint` property in the `otagentodb.yaml` or `otagentpasoe.yaml` files.
  4. Edit the `config.yml` file and provide information for the following properties in the **exporters** node:
    - **Set logging:** `logLevel` to `debug`.
    - **Set file:** `path` to `./export.json`. This is the JSON file where OTel Collector saves metrics data for the APM tool.
    - **Set `otlp/elastic:`** `endpoint` to the location of the APM tool. For example, you may set the value to `localhost:8200`.
  5. Edit other properties listed in the `config.yml` file per your requirements. To know more about these properties, see the [OpenTelemetry Collector documentation](#).
  6. Save the changes made to the `config.yml` file.

Here is a sample `config.yml` file:

```
receivers:
  otlp:
    protocols:
      grpc:
      http:
  otlp/withendpoint:
    protocols:
      grpc:
        endpoint: localhost:4317

exporters:
  logging:
    logLevel: debug
  file:
    path: ./export.json
  otlp/elastic:
    endpoint: localhost:8200
    insecure: true

processors:
  batch:
  service:
    pipelines:
      traces:
        receivers: [otlp, otlp/withendpoint]
        exporters: [logging, otlp/elastic]
      metrics:
        receivers: [otlp, otlp/withendpoint]
        exporters: [logging, file, otlp/elastic]
```

7. Start OTel Collector after updating the `config.yml` file by completing the following steps:

- a) Open a Command window and browse to the OTel Collector installation folder.
- b) Start OTel Collector by specifying the `config.yml` file you updated. Use the following command:

```
<OTel Collector executable> --config config.yml
```

For example on the Windows platform, use the following command:

```
otelcontribcol-0.82.0-windows_amd64.exe --config config.yml
```

## OpenTelemetry metrics for OpenEdge database

The OpenEdge Command Center agent can monitor an OpenEdge database and collect the following performance metrics.

The OpenEdge database metrics follow the naming convention `progress_oedb_<metric name>`. The prefix `progress_oedb` indicates that the metric is specific to the OpenEdge database.

Metric Name	Description
<code>summary_commits_total</code>	The number of transactions all users have committed.
<code>summary_undos_total</code>	The total number of transactions rolled back.
<code>record_updates_total</code>	The total number of records updated.

Metric Name	Description
record_reads_total	The total number of records read.
record_creates_total	The total number of records created.
record_deletes_total	The total number of records deleted.
summary_dbwrites_total	The total number of database blocks written to disk.
summary_dbreads_total	The total number of database blocks read.
summary_biwrites_total	The total number of Before-Image (BI) blocks written to disk.
summary_bireads_total	The total number of BI blocks read.
summary_aiwrites_total	The total number of After-Image (AI) blocks written to disk.
summary_recllocks_total	The total number of record locks used.
summary_recwaits_total	The total number of times users have waited to access a locked record.
summary_chkpts_total	The total number of checkpoints that have been performed.
summary_flushed_total	The total number of database buffers that have been flushed to disk because they were not written by the time the checkpoint ended.
recllock_waits_percent	The percentage of record accesses that resulted in a record lock wait, which occurs when the database engine must wait to access a locked record.
bibuf_waits_percent	The percentage of BI buffer waits, which occur when the database engine must wait to access a BI buffer.
aibuf_waits_percent	The percentage of AI buffer waits, which occur when the database engine must wait to access an AI buffer.
apw_writes_percent	The percentage of database blocks written to disk by the Asynchronous Page Writer (APW).
biw_writes_percent	The percentage of BI blocks written to disk by the Before-Image Writer (BIW).
aiw_writes_percent	The percentage of AI blocks written to disk by the After-Image Writer (AIW).
buffer_hits_percent	The percentage of buffer hits for both the primary and alternate buffer pools. A buffer hit occurs when the database engine locates a record in the buffer pool and does not have to read the record from the disk.
primary_hits_percent	The percentage of buffer hits for the primary buffer pool.

Metric Name	Description
<code>alternate_hits_percent</code>	The percentage of buffer hits for the alternate buffer pool.
<code>instance_running_status</code>	<p>The operational status of an OpenEdge database. It uses numerical value 1 or -1 to represent the status.</p> <ul style="list-style-type: none"><li>• 1 indicates that the database is running.</li><li>• -1 indicates that the database is stopped.</li></ul>

## Enable OpenEdge Command Center agent to collect performance metrics of OpenEdge database

You can enable the OpenEdge Command Center agent to collect performance metrics of an OpenEdge database by specifying details in the `otagentoedb.yaml` file. The file is present in the `conf` folder of the OpenEdge Command Center agent installation.

Follow these steps to enable the agent to collect performance metrics for an OpenEdge database:



1. Open the `otagentoedb.yaml` file in an editor.
2. In the `exporter` node of the `otagentoedb.yaml` file, provide values for the following properties of the OpenEdge Command Center agent connection to the OTel Collector:
  - `name`—A name for the OpenTelemetry exporter. Ensure that the value is set to `otlp`.
  - `endpoint`—The target URL to which the exporter sends the performance metrics data. The OTel Collector receives the metrics data at this endpoint. Make sure to use the same endpoint when you configure the OTel Collector.
  - `protocol`—The transport protocol used to export the metrics data. Use `grpc` as the value for this property.
  - `timeout`—The maximum time the OTLP exporter waits for each batch export.
  - `connectionretry`—The number of times the OpenEdge Command Center agent tries to connect to the OTel Collector in case of a connection failure. To know more about the impact of connection failure and how the connection is restored, see [Performance impact and resilience of collecting performance metrics](#) on page 149.
3. In the `oedbInstances` node, provide values for the following properties of the OpenEdge databases to be monitored:
  - `dbname`—The name of the database to be monitored.
  - `host`—The IP address of the database host.
  - `port`—The port on which the database is running.
  - `user`—The username of the database user.

---

**Note:** You must provide username of either a DBA user or a user with the SELECT permissions on the following virtual system tables (VSTs):

- `_ActSummary`
  - `_ActRecord`
  - `_ActPWs`
  - `_ActBILog`
  - `_ActAILog`
  - `_ActBuffer`
- 

- `password`—The password of the database user.
- 

**Note:** The password can be in cleartext or encoded using the `genpassword` utility, which is a password encryption utility provided with the OpenEdge database.

---

- `metricsregex`—A regular expression (regex) to ensure that only the specified database performance metrics whose names match the pattern you have configured are collected. When left blank, the agent captures all the defined metrics.
- 

**Note:** You can use only the `*` quantifier to create a regular expression.

---

- `otherdbconnparams`—Any other optional SQL JDBC connection parameters to be used for connecting to the database, separated by a semicolon (;).
- `dbschedule`—The time interval at which the agent must capture the metrics data. This property works in conjunction with the `dbduration` property. OpenTelemetry limits the frequency for posting data to a maximum of two times per minute or once every 30 seconds. Progress recommends to send metrics data once per minute.
- `dbduration`—The unit of time interval at which the agent must capture the metrics data. The possible values can be seconds, minutes, hours, or days. This property works in conjunction with the `dbschedule` property.

---

**Note:** You can provide details of multiple OpenEdge databases on your machine under the `oedbInstances` node and collect their metrics data using a single OpenEdge Command Center agent.

---

#### 4. Save the changes made to the `otagentoedb.yaml` file.

Here is a sample `otagentoedb.yaml` file with details of two OpenEdge database instances:

```
exporter:
  name: "otlp"
  endpoint: "http://10.248.0.150:4317"
  protocol: "grpc"
  timeout: 10
  connectionretry: 20

oedbInstances:
- dbname: sports
  host: localhost
  port: 2022
  user: ssl
  password: ssl
  metricsregex:
  otherdbconnparams:
  dbschedule: 30
  dbduration: SECONDS
- dbname: testdb2
  host: localhost
  port: 3111
  user: admin
  password: xxx
  metricsregex:
  otherdbconnparams:
  dbschedule: 30
  dbduration: SECONDS
```

After updating the `otagentoedb.yaml` file, restart the OpenEdge Command Center agent.

## Sample performance metrics data for OpenEdge database

When you configure OpenTelemetry (OTel) Collector to save the performance metrics data for an OpenEdge database in a JSON file and start the OTel Collector, the generated data is stored in the JSON file. You can choose to analyze this data directly or use an APM tool for detailed analysis.

The sample performance metrics data in the JSON file for the OpenEdge database is as follows:

```
{
  "resourceMetrics": [
    {
      "resource": {
        "attributes": [
          {
            "key": "agent_guid", "value": {"stringValue": "bdcd2d48-a600-46ce-89fd-9f9adc52a186"}},
          {
            "key": "hostname", "value": {"stringValue": "windowssrv2019"}},
          {
            "key": "port", "value": {"stringValue": "8686"}},
          {
            "key": "resource_name", "value": {"stringValue": "otoedb1"}},
          {
            "key": "service_name", "value": {"stringValue": "otoedb"}},
          {
            "key": "telemetry_sdk_language", "value": {"stringValue": "Java"}},
          {
            "key": "telemetry_sdk_name", "value": {"stringValue": "openTelemetry"}},
          {
            "key": "telemetry_sdk_os", "value": {"stringValue": "Windows"}},
          {
            "key": "telemetry_sdk_version", "value": {"stringValue": "1.15.0"}}
        ]
      },
      "scopeMetrics": [
        {
          "scope": {
            "name": "progress_oedb_otoedb1",
            "version": "1.0.0"
          },
          "metrics": [
            {
              "name": "progress_oedb_record_deletes_total",
              "description": "The number of records deleted",
              "unit": "cumulative",
              "sum": {
                "dataPoints": [
                  {
                    "startTimeUnixNano": "1718708278551640300",
                    "timeUnixNano": "1718708308566911000",
                    "asInt": "0"
                  }
                ],
                "aggregationTemporality": 2
              }
            },
            ...
          ]
        }
      ]
    }
  ]
}
```

### Resource-level attributes

The resource-level attributes are key-value pairs that describe the characteristics of a monitored OpenEdge database including details about the OpenEdge Command Center agent, service name, and host name. These attributes remain constant across all collected metrics for that particular OpenEdge database and provide essential metadata for analysis and filtering metric data.

The following code snippet shows the resource-level attributes in the JSON file:

```
{
  "resourceMetrics": [
    {
      "resource": {
        "attributes": [
          { "key": "agent_guid", "value": { "stringValue": "bdcd2d48-a600-46ce-89fd-9f9adc52a186" } },
          { "key": "hostname", "value": { "stringValue": "windowssrv2019" } },
          { "key": "port", "value": { "stringValue": "8686" } },
          { "key": "resource_name", "value": { "stringValue": "otoedb1" } },
          { "key": "service_name", "value": { "stringValue": "otoedb" } },
          { "key": "telemetry_sdk_language", "value": { "stringValue": "Java" } },
          { "key": "telemetry_sdk_name", "value": { "stringValue": "openTelemetry" } },
          { "key": "telemetry_sdk_os", "value": { "stringValue": "Windows" } },
          { "key": "telemetry_sdk_version", "value": { "stringValue": "1.15.0" } }
        ]
      }
    }
  ]
}
```

The following table describes each resources-level attribute:

Attribute	Description
agent_guid	Specifies the unique identifier for the OpenEdge Command Center agent.
hostname	Specifies the name of the host system where the agent is running.
port	Specifies the port number on which the monitored OpenEdge database is running.
resource_name	Specifies the name of the OpenEdge database that is monitored.
service_name	Specifies the name of the telemetry service generating metric data.
telemetry_sdk_language	Specifies the programming language of the SDK used for metric data collection.
telemetry_sdk_name	Specifies the name of the telemetry SDK.
telemetry_sdk_os	Specifies the operating system of the host running the telemetry service.
telemetry_sdk_version	Specifies the version of the telemetry SDK used.

## OpenTelemetry metrics for PAS for OpenEdge

The OpenEdge Command Center agent can monitor a PAS for OpenEdge instance and collect the following performance metrics.

The PAS for OpenEdge instance metrics follow the naming convention `progress_pasoe_<metric name>`. The prefix `progress_pasoe` indicates that the metric is specific to the PAS for OpenEdge instance.

Metrics Type	Metric Name	Description
REST transport	expression_errors_total	The total number of expression errors.
	failed_requests_total	The total number of failed requests.
	successful_run_requests_total	The total number of requests for which response was received successfully.
	successful_requests_total	The total number of requests successfully sent to the PAS for OpenEdge server.
	connect_requests_total	The total number of connection requests.
	status_requests_total	The total number of status type requests.
	requests_total	The total number of requests.
	successful_connect_requests_total	The total number of successful connection requests.
	service_unavailable_requests_total	The total number of requests for which services were not available.
	run_requests_total	The total number of run requests.
SOAP transport	url_notfound_errors_total	The total number of errors because of incorrectly supplied URLs.
	active_requests_total	The total number of requests that are in the ACTIVE state.
	wSDL_requests_total	The total number of WSDL requests.
	successful_requests_total	The total number of successful SOAP requests to the PAS for OpenEdge instance.
	method_notallowed_errors_total	The total number of errors caused because the requested method is not authorized.
	http_requests_errors_total	The total number of HTTP requests that resulted in errors.
	http_requests_total	The total number of HTTP requests.
	processor_errors_total	The total number of SOAP processor errors.

Metrics Type	Metric Name	Description
APSV transport	forbidden_requests_total	The total number of requests that failed with the 403 error code.
	disconnect_errors_total	The total number of disconnection errors.
	connect_errors_total	The total number of connection errors.
	disconnect_requests_total	The total number of disconnect requests.
	session_requests_total	The total number of session requests.
	session_errors_total	The total number of session errors.
WEB transport	head_requests_total	The total number of HEAD requests.
	trace_requests_total	The total number of TRACE requests.
	options_requests_total	The total number of OPTIONS requests.
	patch_requests_total	The total number of PATCH requests.
	get_requests_total	The total number of GET requests.
	servlet_requests_total	The total number of SERVLET requests.
	delete_requests_total	The total number of DELETE requests.
	put_requests_total	The total number of PUT requests.
	post_requests_total	The total number of POST requests.
	successful_servlet_requests_total	The total number of successful SERVLET requests.
	head_errors_total	The total number of HEAD requests that resulted in errors.
	trace_errors_total	The total number of TRACE requests that resulted in errors.

Metrics Type	Metric Name	Description
	options_errors_total	The total number of OPTIONS requests that resulted in errors.
	patch_errors_total	The total number of PATCH requests that resulted in errors.
	get_errors_total	The total number of GET requests that resulted in errors.
	delete_errors_total	The total number of DELETE requests that resulted in errors.
	put_errors_total	The total number of PUT requests that resulted in errors.
	post_errors_total	The total number of POST requests that resulted in errors.
	ablruntime_errors_total	The total number of ABL runtime errors.
	ablconnect_errors_total	The total number of ABL connection errors.
	failed_servlet_requests_total	The total number of SERVLET requests that resulted in errors.
Common	all_requests_total	The total number of requests to the PAS for OpenEdge instance.
	applications_total	The total number of applications deployed on the PAS for OpenEdge instance.
	agents_total	The total number of all agents spawned to execute the server requests.
	available_agents_total	The total number of agents with the AVAILABLE status.
	agent_sessions_total	The total number of sessions including all agents of the PAS for OpenEdge server.
	client_connections_total	The total number of client connections to the PAS for OpenEdge instance.
	client_sessions_total	The total number of client sessions connected to the PAS for OpenEdge instance.
	init_sessions_total	The total number of initial sessions configured for the PAS for OpenEdge instance.

Metrics Type	Metric Name	Description
	<code>idle_sessions_total</code>	The total number of sessions with the IDLE state.
	<code>starting_sessions_total</code>	The total number of starting sessions configured for the PAS for OpenEdge instance.
	<code>available_sessions_total</code>	The total number of sessions in the AVAILABLE state.
	<code>reserved_sessions_total</code>	The total number of sessions in the RESERVED state.
	<code>stopped_sessions_total</code>	The total number of sessions in the STOPPED state.
	<code>instance_running_status</code>	<p>The operational status of a PAS for OpenEdge instance. It uses numerical value 1 or -1 to represent the status.</p> <ul style="list-style-type: none"> <li>• 1 indicates that the PAS for OpenEdge instance is running.</li> <li>• -1 indicates that the PAS for OpenEdge instance is stopped.</li> </ul>

## Enable OpenEdge Command Center agent to collect performance metrics of PAS for OpenEdge

You can enable the OpenEdge Command Center agent to collect performance metrics of a PAS for OpenEdge instance by specifying details in the `otagentpasoe.yaml` file. The file is present in the `conf` folder of the OpenEdge Command Center agent installation.

Follow these steps to enable the agent to collect performance metrics of a PAS for OpenEdge instance:



1. Open the `otagentpasoe.yaml` file in an editor.
2. In the `exporter` node of the `otagentpasoe.yaml` file, provide values for the following properties of the OpenEdge Command Center agent connection to the OTel Collector:
  - `name`—A name for the OpenTelemetry exporter. Ensure that the value is set to `otlp`.
  - `endpoint`—The target URL to which the exporter sends the performance metrics data. The OTel Collector receives the metrics data at this endpoint. Make sure to use the same endpoint when you configure the OTel Collector.
  - `protocol`—The transport protocol used to export the metrics data. Use `grpc` as the value for this property.
  - `timeout`—The maximum time the OTLP exporter waits for each batch export.
  - `connectionretry`—The number of times the OpenEdge Command Center agent tries to connect to the OTel Collector in case of a connection failure. To know more about the impact of connection failure and how the connection is restored, see [Performance impact and resilience of collecting performance metrics](#) on page 149.
3. Under the `pasInstances` node of the YAML file, provide values for the following properties of the PAS for OpenEdge instances to be monitored:
  - `pasdir`—The location of the PAS for OpenEdge instance.

---

**Note:** Make sure that a PAS for OpenEdge already exists at the specified location before you provide the value for the `pasdir` property.

---

- `passchedule`—The time interval at which the agent must capture the metrics data. This property works in conjunction with the `pasduration` property. OpenTelemetry limits the frequency for posting data to a maximum of two times per minute or once every 30 seconds. Progress recommends sending metrics data once per minute.
- `pasduration`—The unit of time interval at which the agent must capture the metrics data. The possible values can be seconds, minutes, hours, or days. This property works in conjunction with the `passchedule` property.
- `metricsregex`—A regular expression (regex) to ensure that only the specified PAS for OpenEdge instance performance metrics whose names match the pattern you have configured are collected. When left blank, the agent captures all the defined metrics.

---

**Note:** You can use only the `*` quantifier to create a regular expression.

---

4. Save the changes made to the `otagentpasoe.yaml` file.

Here is a sample `otagentpasoe.yaml` file with details of two PAS for OpenEdge instances:

```
exporter:
  name: "otlp"
  endpoint: "http://localhost:4317"
  protocol: "grpc"
  timeout: 10
  connectionretry: 20

pasInstances:
  - pasdir: "C:/OpenEdge/WRK/oepas5"
```

```
passchedule: 30
pasduration: SECONDS
metricsregex:
- pasdir: "C:/OpenEdge/WRK/oepas2"
  passchedule: 30
  pasduration: SECONDS
  metricsregex:
```

After updating the `otagentpasoe.yaml` file, restart the OpenEdge Command Center agent.

## Sample performance metrics data for PAS for OpenEdge

When you configure OpenTelemetry (OTel) Collector to save the performance metrics data for a PAS for OpenEdge instance in a JSON file and start the OTel Collector, the generated data is stored in the JSON file. You can choose to analyze this data directly or use an APM tool for detailed analysis.

The sample performance metrics data in the JSON file for the PAS for OpenEdge instance is as follows:

```
{
  "resourceMetrics": [
    {
      "resource": {
        "attributes": [
          {"key": "agent_guid", "value": {"stringValue": "ABCD"}},
          {"key": "hostname", "value": {"stringValue": "windowssrv2019"}},
          {"key": "resource_name", "value": {"stringValue": "RetailMgmt"}},
          {"key": "service_name", "value": {"stringValue": "otpasoe"}},
          {"key": "telemetry_sdk_language", "value": {"stringValue": "Java"}},
          {"key": "telemetry_sdk_name", "value": {"stringValue": "openTelemetry"}},
          {"key": "telemetry_sdk_os", "value": {"stringValue": "Windows"}},
          {"key": "telemetry_sdk_version", "value": {"stringValue": "1.15.0"}}
        ]
      },
      "scopeMetrics": [
        {
          "scope": {
            "name": "progress_oepas_C:/OE_128/wrk/RetailMgmt",
            "version": "1.0.0"
          },
          "metrics": [
            {
              "name": "Progress_pasoe_get_errors_total",
              "description": "The number of GET requests that resulted in errors.",
              "unit": "cumulative",
              "sum": {
                "dataPoints": [
                  {
                    "attributes": [
                      {"key": "ablapp", "value": {"stringValue": "RetailMgmt"}},
                      {"key": "transport", "value": {"stringValue": "WEB"}},
                      {"key": "webapp", "value": {"stringValue": "ROOT"}}
                    ],
                    "startTimeUnixNano": "1718893655587297400",
                    "timeUnixNano": "1718893685609868500",
                    "asInt": "0"
                  },
                  {
                    "attributes": [
                      {"key": "ablapp", "value": {"stringValue": "Customer"}},
                      {"key": "transport", "value": {"stringValue": "WEB"}},
                      {"key": "webapp", "value": {"stringValue": "Orders"}}
                    ],
                    "startTimeUnixNano": "1718893655587297400",
                    "timeUnixNano": "1718893685609868500",
                    "asInt": "0"
                  }
                ]
              }
            },
            ...
          ]
        },
        ...
      ]
    },
    ...
  ]
}
```

### Resource-level attributes

The resource-level attributes are key-value pairs that describe the characteristics of a monitored PAS for OpenEdge instance, including details about the OpenEdge Command Center agent, service name, and host name. These attributes remain constant across all collected metrics for that particular PAS for OpenEdge instance and provide essential metadata for analysis and filtering metric data.

The following code snippet shows the resource-level attribute in the JSON file:

```
{
  "resourceMetrics": [
    {
      "resource": {
        "attributes": [
          {"key": "agent_guid", "value": {"stringValue": "ABCD"}},
          {"key": "hostname", "value": {"stringValue": "windowssrv2019"}},
          {"key": "resource_name", "value": {"stringValue": "RetailMgmt"}},
          {"key": "service_name", "value": {"stringValue": "otpasoe"}},
          {"key": "telemetry_sdk_language", "value": {"stringValue": "Java"}},
          {"key": "telemetry_sdk_name", "value": {"stringValue": "openTelemetry"}},
          {"key": "telemetry_sdk_os", "value": {"stringValue": "Windows"}},
          {"key": "telemetry_sdk_version", "value": {"stringValue": "1.15.0"}}
        ]
      }
    }
  ]
  ...
}
```

The following table describes each resources-level attribute:

Attribute	Description
agent_guid	Specifies the unique identifier for the OpenEdge Command Center agent.
hostname	Specifies the name of the host system where the agent is running.
resource_name	Specifies the name of the PAS for OpenEdge instance that is monitored.
service_name	Specifies the name of the telemetry service generating metric data.
telemetry_sdk_language	Specifies the programming language of the SDK used for metric data collection.
telemetry_sdk_name	Specifies the name of the telemetry SDK.
telemetry_sdk_os	Specifies the operating system of the host running the telemetry service.
telemetry_sdk_version	Specifies the version of the telemetry SDK used.

### Metric-level attributes

The metric-level attributes are key-value pairs within the data point of a recorded metric. They provide additional contextual information about the measurement being taken. These attributes are dynamic and allow you to view, filter, and perform granular analysis of metric data.

The following code snippet shows the metric-level attributes in the JSON file:

```
...
"metrics": [
  {
    "name": "Progress_pasoe_get_errors_total",
    "description": "The number of GET requests that resulted in errors.",
    "unit": "cumulative",
    "sum": {
      "dataPoints": [
        {
          "attributes": [
            { "key": "ablapp", "value": { "stringValue": "RetailMgmt" } },
            { "key": "transport", "value": { "stringValue": "WEB" } },
            { "key": "webapp", "value": { "stringValue": "ROOT" } }
          ],
          "startTimeUnixNano": "1718893655587297400",
          "timeUnixNano": "1718893685609868500",
          "asInt": "0"
        },
        {
          "attributes": [
            { "key": "ablapp", "value": { "stringValue": "Customer" } },
            { "key": "transport", "value": { "stringValue": "WEB" } },
            { "key": "webapp", "value": { "stringValue": "Orders" } }
          ],
          "startTimeUnixNano": "1718893655587297400",
          "timeUnixNano": "1718893685609868500",
          "asInt": "0"
        }
      ],
      "aggregationTemporality": 2
    }
  },
  ...
]
```

## Performance impact and resilience of collecting performance metrics

The OpenEdge Command Center agent runs on the same machine as the monitored OpenEdge resource and regularly interacts with the resource for collecting the performance metrics data. However, this action has a negligible impact on the performance of the OpenEdge resource.

Installing OTel Collector on the same machine as the OpenEdge Command Center agent and the monitored OpenEdge resource can impact the performance of the OpenEdge resource. So, it is recommended to install OTel Collector on a different machine.

You can further reduce the performance impact by increasing the time interval at which the agent scrapes the metrics data. To increase the time interval:

- When monitoring an OpenEdge database, increase the value of the `dbschedule` property in the `otagentodb.yaml` file.
- When monitoring a PAS for OpenEdge instance, increase the value of the `paschedule` property in the `otagentpasoe.yaml` file.

Contact Progress Technical Support if you have any queries on the performance impact.

When the monitored OpenEdge resources are running, the OpenEdge Command Center agent continues to collect metrics data and sends it to the OTel Collector. The collection of metrics data ceases when the OpenEdge Command Center agent stops. If the monitored OpenEdge resource stops and then restarts, the collection of metrics data resumes if both the OpenEdge Command Center agent and OTel Collector are running.

If the OTel Collector stops or the connection between the OpenEdge Command Center agent and the OTel Collector is disrupted, the Command Center agent tries to reconnect as per the value configured for the `connectionretry` property in the `otagentoedb.yaml` or `otagentpasoe.yaml` file.

- If the connection is restored within the configured retry attempts, the Command Center agent sends the performance data to the OTel Collector.
- If the connection is not restored within the configured retry attempts, the Command Center agent stops sending the performance data to the OTel Collector and ceases collecting the data from the OpenEdge resource. You must restart both the OpenEdge Command Center agent and the OTel Collector to resume monitoring of the OpenEdge resource.

If the connection between the OpenEdge Command Center agent and the OTel Collector is disrupted due to an incorrectly configured YAML file on the Command Center agent, update the configuration file and restart the Command Center agent.

## Reset super admin user details

You can modify the following details of the super admin user after launching the OpenEdge Command Center server:

- First name
- Last name
- Password
- Email address
- Description

To modify the super admin user details, perform the following steps:

1. Open a command-line interface with administrative privileges. On Windows, run the command prompt as an administrator. On Linux, run the terminal as a `root` user.
2. Change to the `utils` directory within the directory where the OpenEdge Command Center server is installed.
  - On Windows, go to `cd C:\Progress\OECC\Server\utils`.
  - On Linux, go to `cd /Progress/OECC/server/utils`.
3. To modify one or more details of a super admin user, run the following command:

```
resetsuperadmin [--firstname <first name>] | [--lastname <last name>] | [--pwd  
<password>] | [--email <email>] | [--description <description>]
```

Replace each placeholder with the appropriate value. For detailed information about the syntax and parameters, see [RESETSUPERADMIN utility](#) on page 153.

---

## OpenEdge Command Center utilities

---

This chapter describes the OpenEdge Command Center utilities in alphabetical order. It describes the purpose, syntax, and parameters for each utility.

For details, see the following topics:

- [OECCAGENT utility](#)
- [OECCSERVER utility](#)
- [RESETSUPERADMIN utility](#)

### OECCAGENT utility

OpenEdge Command Center provides the `oeccagent` utility to manage the OpenEdge Command Center agent. You can use this utility to start or stop the agent as a process for planned maintenance, troubleshooting, and so on.

This utility is located in the directory where the OpenEdge Command Center agent is installed.

#### Syntax

```
oeccagent [start | stop]
```

## Parameters

`start`

Starts the OpenEdge Command Center agent as a process.

`stop`

Stops the OpenEdge Command Center agent.

# OECCSERVER utility

OpenEdge Command Center provides the `oeccserver` utility to manage the OpenEdge Command Center server and MongoDB. You can use this utility to start or stop these components individually or together for planned maintenance, troubleshooting, and so on.

This utility is located in the directory where the OpenEdge Command Center server is installed.

## Syntax

```
oeccserver [start | stop | startdatabase | stopdatabase]
```

## Parameters

`start`

Starts the OpenEdge Command Center server as a process and MongoDB.

`stop`

Stops only the OpenEdge Command Center server.

`startdatabase`

Starts only MongoDB.

`stopdatabase`

Stops only MongoDB.



# RESETSUPERADMIN utility

OpenEdge Command Center provides the `resetsuperadmin` utility to manage the superuser administrator details. As an administrator, you can use this utility to modify the following details:

- First name
- Last name
- Password
- Email address
- Description

The `resetsuperadmin` utility is located in the `utils` directory within the directory where the OpenEdge Command Center server is installed.

For example,

- On Windows, `C:\Progress\OECC\Server\utils`
- On Linux, `/Progress/OECC/server/utils`

For more information, see [Reset super admin user details](#) on page 150.

## Syntax

```
resetsuperadmin [--firstname <first name>] | [--lastname <last name>] | [--pwd
<password>] | [--email <email>] | [--description <description>]
```

For example:

```
resetsuperadmin [--firstname John] | [--lastname Smith] | [--pwd P@ssw0rd123!] |
[--email superadmin@gmail.com] | [--description Primary user of the OpenEdge
Command Center server]
```

## Parameters

`--firstname <first name>`

Specifies the first name to be updated. Only alphanumeric characters are allowed.

For example, `--firstname "John"`

`--lastname <last name>`

Specifies the last name to be updated. Only alphanumeric characters are allowed.

For example, `--lastname "Smith"`

`--pwd <password>`

Specifies the new password for the user account. The password must meet the following requirements:

- length of 8 to 40 characters
- A mixture of uppercase and lowercase letters
- At least one numeral
- At least one of the special characters: ! @ \$ % ^ ( ) \_ + = [ ] |

For example, `--pwd "P@ssw0rd123!"`

`--email <email>`

Specifies the new email address for the user account.

For example, `--email "superadmin@gmail.com"`

`--description <description>`

Specifies the description for the user account.

For example, `--description "Primary user of the OpenEdge Command Center server"`

---

## OpenEdge Command Center performance results

---

The following information shows performance results of OpenEdge Command Center under various scenarios. Note that actual performance may vary depending on workload, network conditions, system tuning, and so on.

### Test system configuration

- RAM: 32 GB
- CPU: 8-core CPU
- Hard disk: 100 GB

### Performance results

- Agent-level performance—The tests evaluated a single agent managing different combinations of OpenEdge resources.
  - PAS for OpenEdge instances—The agent was able to manage up to 40 PAS for OpenEdge instances.
  - OpenEdge databases—The agent was able to manage up to 800 OpenEdge databases.
  - Both PAS for OpenEdge instances and OpenEdge databases—The agent was able to manage up to 30 PAS for OpenEdge instances and 200 OpenEdge databases.
- Server-level performance—The tests evaluated a single server managing multiple agents with a varying number of OpenEdge resources.
  - The server was able to manage 10 to 15 agents.

Performance varies based on the number of resources, including PAS for OpenEdge instances, ABL applications, web applications, and OpenEdge databases that each agent handles. You can use these performance results to plan and optimize your OpenEdge Command Center deployments.