



Use the OpenEdge Command Center

OpenEdge®

Table of Contents

Preface.....	7
Learn about OpenEdge Command Center.....	9
OpenEdge Command Center console dashboard.....	11
Install and configure OpenEdge Command Center.....	15
Launch the OpenEdge Command Center installer.....	17
Install OpenEdge Command Center in high availability mode.....	19
Silent installation of OpenEdge Command Center.....	21
Set up OpenEdge Command Center with MongoDB Atlas on AWS	23
Deploy OpenEdge Command Center on Windows platform using a ZIP package.....	24
Deploy OpenEdge Command Center on Linux platform using a TAR package.....	26
Uninstall OpenEdge Command Center.....	28
Upgrade OpenEdge Command Center.....	28
Install OpenEdge Command Center Agents.....	31
Silently install OpenEdge Command Center agents.....	33
Deploy OpenEdge Command Center agent on Windows platform using a ZIP package.....	35
Deploy OpenEdge Command Center agent on Unix platform using a TAR package.....	37
Uninstall OpenEdge Command Center agents.....	38
Upgrade OpenEdge Command Center agent.....	39
How to.....	41
Log in to OpenEdge Command Center.....	43
Change or reset passwords.....	43
Configure new OpenEdge Command Center agents.....	44
Manage agent services.....	45
Manage services for OpenEdge Command Center server.....	47
Change logging level.....	47
Configure and manage PAS for OpenEdge instances.....	48
Configure PAS for OpenEdge instances.....	48
Manage PAS for OpenEdge instances.....	61
Manage ABL applications, web applications, and REST services.....	65
View ABL applications across multiple PAS for OpenEdge instances.....	65
Manage ABL applications.....	66
Manage web applications.....	68
Manage REST services.....	69
Monitor OpenEdge resources using the OpenEdge Command Center agent.....	70

OpenTelemetry metrics for OpenEdge database.....	72
OpenTelemetry metrics for PAS for OpenEdge.....	73
Enable OpenEdge Command Center agent to collect performance metrics of OpenEdge Database.....	77
Enable OpenEdge Command Center agent to collect performance metrics of PAS for OpenEdge	80
Set up OpenTelemetry Collector.....	82
Performance impact and resilience of collecting performance metrics.....	84
Set up the APM tool.....	84
Add agent labels.....	85
Update agent labels.....	86
Generate new agent keys.....	86
Search for and filter agents.....	87
Configure email settings.....	88
Add a new user.....	89
Reset the super administrator password.....	90
Set up TLS.....	91
Set up TLS for OpenEdge Command Center server and agent communication.....	91
Set up TLS for OpenEdge Command Center and MongoDB communication.....	92
OpenEdge Command Center reference.....	95
Sign in.....	95
OpenEdge Command Center	96
OpenEdge Command Center agents.....	97
Edit OpenEdge Command Center agents.....	98
OpenEdge Command Center agent keys.....	98
Application servers.....	98
Users.....	99
Email settings.....	99

Copyright

© 2022 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Apache and Kafka are either registered trademarks or trademarks of the Apache Software Foundation in the United States and/or other countries. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

September 2022

Product version: Progress OpenEdge Command Center 1.2

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 9
This section provides an introduction to OpenEdge Command Center and its benefits to an OpenEdge administrator.
- [Install and configure OpenEdge Command Center](#) on page 15
This section provides information about the various tasks required for installing and configuring OpenEdge Command Center.
- [Install OpenEdge Command Center Agents](#) on page 31
This section provides information about the various tasks required for installing and configuring OpenEdge Command Center Agent.
- [How to](#) on page 41
This section provides information about the various tasks that are required to operate the OpenEdge Command Center.
- [OpenEdge Command Center reference](#) on page 95
This section provides a ready reference to the various pages and interface elements of the OpenEdge Command Center.

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

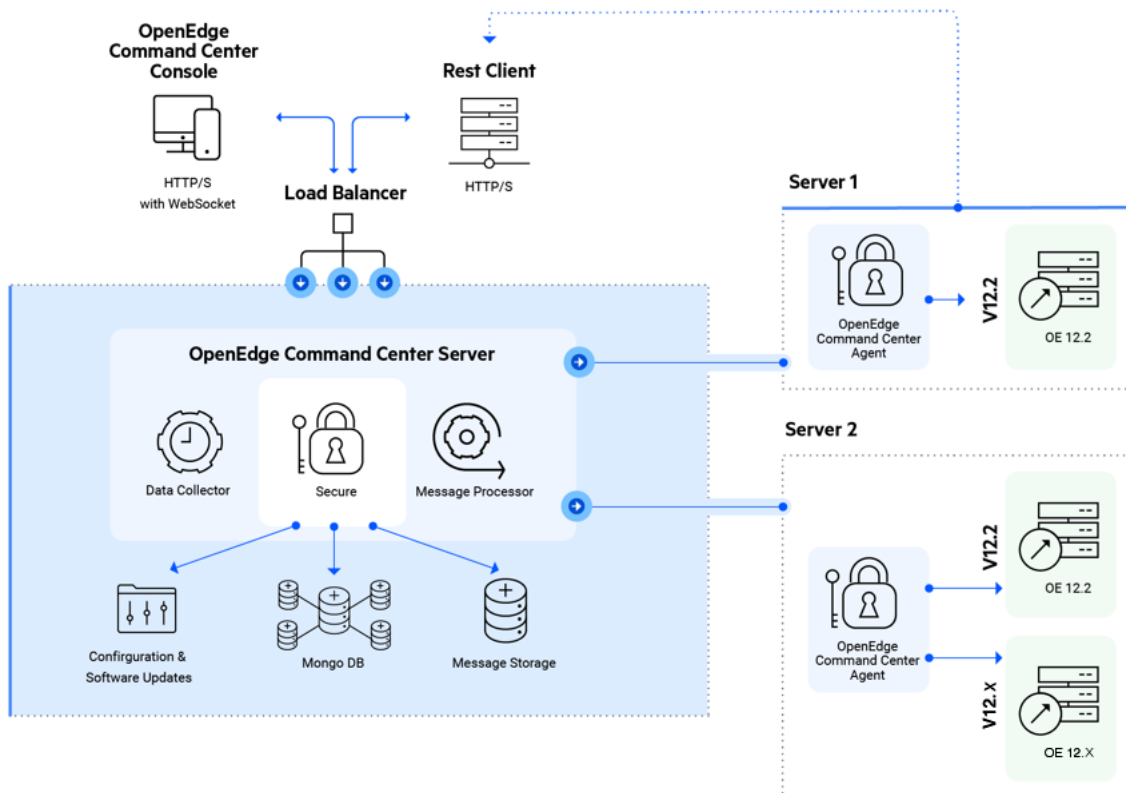
OpenEdge Command Center features the latest UI and UX technologies. Currently, OpenEdge Command Center is built to effectively manage PAS for OpenEdge instances. It aims to incrementally support everything you need to manage instances. It simplifies the administrative overhead for system administrators 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 allowing for a secure connection 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 with interactive swagger documentation to help you add your own resources along the way.

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.

Built for high availability, the OpenEdge Command Center server can be deployed on multiple servers, managed by a load balancer, and unified through a common database. Built-in user management for system administrators and application administrators ensures that you have secure control of OpenEdge Command Center user permissions across all of your instances. For complete resource visibility, OpenEdge Command Center offers automated component discovery for OpenEdge version 12.2.5 and later releases for all PAS for OpenEdge deployments.



OpenEdge Command Center server

The OpenEdge Command Center server powers the OpenEdge Command Center web console and APIs. OpenEdge Command Center uses a MongoDB database and a file store to store data. You can deploy the server as single node or, if configured for high availability, a multi-node cluster. For high availability, the server works with all load balancers that support HTTP/HTTPS transports and websocket protocols, such as Nginx, Apache HTTP Server, AWS, ELB/ALB, and more.

Database

The OpenEdge Command Center uses MongoDB as its internal configuration database. MongoDB is a document database that stores data in JSON-like documents. All the OpenEdge Command Center configurations and details of discovered OpenEdge components (such as PAS for OpenEdge instances) are stored in MongoDB. When OpenEdge Command Center is configured for high availability, multiple server instances of OpenEdge Command Center can be linked by the database. In the event of a planned or unplanned outage of an OpenEdge Command Center server, other OpenEdge Command Center servers will balance the load without impacting the end user.

File store

The file store is a repository for your database connectivity information, security configuration, logging configuration, agent binaries, first user details, and so on, for your PAS for OpenEdge instances across all your deployments.

When OpenEdge Command Center is installed in high availability mode, the file store can be accessed with read and write permissions from all nodes. To use high availability mode, you configure MongoDB on your first node machine on which you install OpenEdge Command Center. Then on subsequent nodes, you point the MongoDB configuration to the first node. This allows you to have a single central MongoDB configuration, which frees you from the need to reconfigure MongoDB individually on each additional node on which you install OpenEdge Command Center.

As new versions of OpenEdge Command Center agents are released, you can download them from the Progress Electronic Software Distribution portal and copy them to the file store. From the file store, the new agent version can be distributed to all of your agent instances.

Command Center agents

A OpenEdge Command Center agent is a lightweight process that 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 (12.2.5 and later) installations. 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. You can also use the OpenEdge Command Center agent to collect performance metrics of OpenEdge resources, such as OpenEdge database and PAS for OpenEdge.

After the agent is installed, it can begin functioning autonomously, monitoring OpenEdge components. You need only to ensure that the agent is up and running. To validate a OpenEdge Command Center agent, you generate an agent key by using the OpenEdge Command Center console or APIs. You can then configure the server connection details for the agent and the OpenEdge Command Center server.

Browser clients

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

The OpenEdge Command Center is a cloud-ready OpenEdge management console capable of managing multiple OpenEdge resources and installations across various machines and versions of OpenEdge.

For details, see the following topics:

- [OpenEdge Command Center console dashboard](#)

OpenEdge Command Center console dashboard

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

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 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 notifications

The top right area of the console dashboard displays banner notifications, alerting you to outstanding tasks that need to be completed such as:

- **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.
- **Agent keys**—Before an agent can communicate with the OpenEdge Command Center server, click this link to generate the keys that are needed to establish a secure network channel. Going forward, every time you configure a new agent, you must generate these keys. This banner notification remains displayed and is always available.

Newly discovered agents and PAS for OpenEdge instances

After you have configured one or more agents, the **Newly Discovered** panel lists all of those agents and also the PAS for OpenEdge instances that those agents have discovered. That is, for every agent that has been configured in a PAS for OpenEdge installation and that is running, all PAS for OpenEdge instances discovered by that agent are listed in this panel.

You can click on a PAS for OpenEdge instance to view its current running status, its labels, and other details. Within the view of an instance, you can also select the checkbox for an instance and start or stop that instance, and perform other actions as appropriate.

From the **Newly Discovered** panel, you can also click on an agent to view the PAS for OpenEdge instances that are managed by the agent, as well as details about each instance, such as its assigned labels, host details, and running status.





Quick links




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

- OpenEdge Command Center online help, which is posted on the Progress Information Hub
- 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 OpenEdge Command Center agents page, from which you can create and manage agents across all of your OpenEdge deployments, as well as generate agent keys. 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 Configure new OpenEdge Command Center agents on page 44 and Manage agent services on page 45.</p>
	<p>The PAS for OpenEdge instances 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, or delete PAS for OpenEdge instances, and you can also modify the configuration instances. For more information, see Configure and manage PAS for OpenEdge instances on page 48.</p>
	<p>The users page, from which you can create and manage users and user information, such as name, email, and role for your OpenEdge Command Center instances.</p> <p>For more information, see Add a new user on page 89.</p>

Click to display
	<p>The agent keys page, from which you can generate new agent keys, or disable or delete keys that are no longer needed. After an agent key is created, you can associate it with a specific agent to authorize that agent to be used with the OpenEdge Command Center.</p> <p>For more information, see Generate new agent keys on page 86.</p>
	<p>The console settings page, from which you can manage general settings for OpenEdge Command Center. From this tab you can manage database settings, update settings, agent update 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 Configure email settings on page 88.</p>

Install and configure OpenEdge Command Center

Before you install OpenEdge Command Center, 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, and determining the installation method to use.

Installation prerequisites

The OpenEdge Command Center server is supported on the following operating system platforms:

- Ubuntu 18.04 LTS
- Oracle Linux 8
- Red Hat Enterprise Linux 8
- SUSE Linux Enterprise Server 15
- CentOS Linux 8
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)

Before you install OpenEdge Command Center, you must download MongoDB 4.2.12 or above and set up MongoDB with basic authentication mode.

Note: MongoDB 5.x is currently not supported by OpenEdge Command Center.

OpenEdge Command Center supports the following types of MongoDB:

- MongoDB Community Server

- MongoDB Atlas running on AWS, Azure, and Google Cloud Platform (GCP)
- MongoDB Enterprise Edition

Each version of MongoDB is available from the following location:

<https://www.mongodb.com>

Note the name and login credentials of a designated database user, which you need to provide during the OpenEdge Command Center installation.

Installation modes

There are several ways you can install OpenEdge Command Center:

- [Launch the OpenEdge Command Center installer](#) on page 17—Typically used for a complete installation of OpenEdge Command Center server and console components.
- [Install OpenEdge Command Center in high availability mode](#) on page 19—Installs multiple server instances to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.
- [Silent installation of OpenEdge Command Center](#) on page 21—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. You then use the response file to perform noninteractive, batch mode style installations on other machines.

You can also specify the mode in which you want to install OpenEdge Command Center:

- GUI mode—Launches the installer and prompts you for responses before uninstalling.
- Console/terminal mode—The install 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 in silent mode.

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

For details, see the following topics:

- [Launch the OpenEdge Command Center installer](#)
- [Install OpenEdge Command Center in high availability mode](#)
- [Silent installation of OpenEdge Command Center](#)
- [Set up OpenEdge Command Center with MongoDB Atlas on AWS](#)
- [Deploy OpenEdge Command Center on Windows platform using a ZIP package](#)
- [Deploy OpenEdge Command Center on Linux platform using a TAR package](#)
- [Uninstall OpenEdge Command Center](#)
- [Upgrade OpenEdge Command Center](#)

Launch the OpenEdge Command Center installer

To install OpenEdge Command Center, download the software image from the Progress Software Download Center and launch the interactive installation program. The installation program is available for the Linux and Windows platforms. The installation files available for the platforms are as follows:

Platform	Installer file name
Windows	PROGRESS_OECC_SERVER_1.x.x_WIN_64.exe
Linux	PROGRESS_OECC_SERVER_1.x.x_LNX_64.bin

To launch the installer, you must have administrator privileges on the machine where you are installing OpenEdge Command Center Server. The installer prompts you to provide information including:

- The host where OpenEdge Command Center is installed.
- Information about available OpenEdge Command Center configurations.
- The database used with the OpenEdge Command Center.
- A designated user with super administrator privileges.

To install the OpenEdge Command Center, complete the following steps:

1. 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 needs to complete the installation.

2. Change to the directory that contains the installer file.

3. Run the installer file to launch the installation procedure. For example, on the Linux platform:

```
prompt> ./PROGRESS_OECC_SERVER_1.1.0_LNX_64.bin
```

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

4. Read the information on the **Introduction** page, verify that all the other applications are closed, and click **Next**.
5. Read the End User License Agreement (EULA). If the terms are acceptable, check **I accept the terms of the License Agreement**, and click **Next**.
6. On the **Host Configurations** page, enter the port number to be used by OpenEdge Command Center (the default is 8000).
7. If you want to enable the security layer, check **SSL/TLS** and specify the following details:
 - **Hostname**—The name of the OpenEdge Command Center host
 - **Key File**—The private key that is used for encryption
 - **Certificate file**—The public certificate of the CA that has signed the server's TLS certificate. Also known as the root certificate.

8. On the **Install Configurations** page:

- a. Enter the installation directory path. The default installation location for the Linux platform is `/usr/openedge_command_center`. The default location for the Windows platform is `C:\Progress\OpenEdge_Command_Center`.
- b. Select **Install as a service** if you want to install OpenEdge Command Center as a service. This provides you with the ability to launch OpenEdge Command Center as a service on Linux platforms.
- c. Enter the Data Directory path and click **Next**.

The default Data Directory path for the Linux platform is `/OpenEdge/Data`. Similarly, the default path for the Windows platform is `C:\OpenEdge\Data`.

Note: The Data Directory is a shared path, which is suitable for installing OpenEdge Command Center in high availability mode, as explained in [Install OpenEdge Command Center in high availability mode](#) on page 19.

9. On the **Database Configurations** page:

- a. Enter the **Hostname/IP Address** information.
- b. Enter the port number. (The default port number is 27017.)

Note: Specifying a port number is not required if you select **Yes** for **Use srv record**.

- c. Enter the credentials for an existing MongoDB user, as well as the database authentication type:

- Username
- Password
- Database authentication If the connection to the database is not successful, the installation cannot be completed.

10. On the **First User Setup** page, specify the following values for the super administrator:

- First Name
- Last Name
- Email
- Username—You must specify a minimum of 5 characters. The supported characters are: alphanumeric characters, period (.), underscore (_), and hyphen (-).
- Password—A valid password must contain the following:
 - 8-40 characters
 - Mixture of uppercase and lowercase letters
 - At least one number
 - At least one of the special characters: ! @ \$ % ^ & () _ + = [] |

The password must not contain your username or a previously-used password.

- Confirm Password

A user with super administrator privileges is created.

11. Review the following information before you complete the installation to ensure that it is correct:

- Product Name—OpenEdge Command Center.
- Install Folder—Path where OpenEdge Command Center is installed.
- Data Directory—Path where the database is installed.
- Disk Space Information—Amount of space required or occupied by OpenEdge Command Center.

12. The **Finish Installation** section indicates the successful installation of the OpenEdge Command Center.

Install OpenEdge Command Center in high availability mode

Installing OpenEdge Command Center in high availability mode provides failover capabilities in the event that one machine that runs OpenEdge Command Center becomes unavailable. When OpenEdge Command Center is configured for high availability, multiple installations of OpenEdge Command Center can be linked by the database. In the event of a planned or unplanned outage of an OpenEdge Command Center machine, other OpenEdge Command Center machines will balance the load without creating a negative impact on the end user.

To configure additional machines with OpenEdge Command Center, you install OpenEdge Command Center on each machine in the same way as you do for the first machine. However, when you specify a data directory on the **Install Configurations** page, you must specify the same data directory that you configured on the first machine. Then all the database connection details are picked up automatically, which makes for a simpler installation on the secondary machines.

Prerequisites

Before you install OpenEdge Command Center for high availability mode, complete the following steps:

1. Ensure that you have installed at least one instance OpenEdge Command Center on another machine before you begin to install it on a second.
2. Obtain the OpenEdge Command Center installer file that was used for the prior OpenEdge Command Center installation. For example, `PROGRESS_OECC_SERVER_1.x.x_LNX_64.bin` or `PROGRESS_OECC_SERVER_1.x.x_WIN_64.exe` for the Linux and Windows platform respectively.

Install OpenEdge Command Center

On each additional machine that you want in your high availability deployment of OpenEdge Command Center, complete the following steps:

1. 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 needs to complete the installation.
2. Open a command window and change to the directory that contains the installer file.
3. 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.
4. On the **Host Configurations** page, enter the port number (the default port number is 8000).
5. On the **Install Configurations** page:
 - a. Enter the installation directory path. The default installation location for the Linux platform is `/usr/openedge_command_center`. The default location for the Windows platform is `C:\Progress\OpenEdge_Command_Center`.
 - b. Select **Install as a service** if you want to install OpenEdge Command Center as a service.
 - c. Enter the Data Directory path.
This is the shared data directory path that was configured during the installation of your first machine. The installer obtains the database configurations, first user information, and security configurations from this shared data directory. The installer does not prompt for backend configurations and first user setup details, but skips to the **Review** section.

6. **Review** and **Finish** the installation.

The installation of OpenEdge Command Center in high availability mode is complete.

Configure a load balancer

The following code example shows the configuration file, `Nginx.conf`, for the Nginx load balancer. To configure Nginx, modify this configuration file in the location shown in **bold**. In this location, you specify the IP address and port number of each OpenEdge Command Center host in your deployment.

```
user  nginx;
worker_processes  1;
```

```

error_log /var/log/nginx/error.log warn;
pid /var/run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    map $http_upgrade $connection_upgrade {
        default upgrade;
        '' close;
    }
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    #sendfile on;
    #tcp_nopush on;

    keepalive_timeout 65;

    upstream backend {
        ip_hash;
        server ip-address:port;
        server ip-address:port;
    }

    server {
        listen 80;
        server_name $hostname;

        location / {
            proxy_pass http://backend;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header Host $host;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection $connection_upgrade;
        }
    }
}

```

Silent installation of OpenEdge Command Center

An interactive installation prompts you for information and records your values in a series of dialog boxes. The installation program immediately uses this data to set up OpenEdge Command Center.

By contrast, a silent installation performs an installation entirely by script, and is a two-step process:

1. When you start an interactive installation, the data that you enter is automatically recorded in a response file. The default name for this file is `response.properties`, and it is created in the `install` subdirectory of your OpenEdge Command Center installation directory.
2. The installation data that is captured in the response file becomes available for play back to perform a silent installation through a batch mechanism.

Response file contents

The data captured in the `response.properties` file provides a detailed snapshot of the installation choices made during an interactive installation.

The `response.properties` file includes:

- Host configurations
- Install configurations
- Database configurations
- First user setup

The following example shows an excerpt from the automatically-generated `response.properties` file:

```
# Wed Nov 11 03:12:34 EST 2020
# 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_SSL_SELECTED=1
OECC_HOST_NAME=centos7164
OECC_SSL_KEY_FILE=/tmp/key
OECC_SSL_CERTIFICATE_FILE=/tmp/cert
```

```
#Install Configurations
#-----
USER_INSTALL_DIR=/usr1/OECC
OECC_INSTALL_AS_SERVICE=1
OECC_DATA_DIR=/OpenEdge/Data1
```

```
#Database Configurations
#-----
MONGO_DB_HOST=IP-address
MONGO_DB_SRV_NO=1
MONGO_DB_PORT=27017
MONGO_DB_SRV_YES=0
MONGO_DB_USER=myAdmin
MONGO_DB_PASS=password
MONGO_DB_AUTH_DB=admin
```

```
#First User Setup
#-----
OECC_FIRST_USER_NAME=admin
OECC_FIRST_USER_LAST_NAME=user
OECC_USER_EMAIL=admin@progress.com
OECC_USER_NAME=admin
OECC_USER_PASSWORD=password
OECC_USER_CONF_PASSWORD=password
```

Create the response file

To create a response file:

1. Open a command window and change to the directory that contains the OpenEdge Command Center installer file, `PROGRESS_OECC_SERVER_1.x.x_LNX_64.bin` or `PROGRESS_OECC_SERVER_1.x.x_WIN_64.exe` for the Linux and Windows platform respectively.
2. Enter the following command to record installation choices in the `response.properties` file:
 - For the Linux platform, `PROGRESS_OECC_SERVER_1.x.x_LNX_64.bin -r /response.properties-file`
 - For the Windows platform, `PROGRESS_OECC_SERVER_1.x.x_WIN_64.exe -r /response.properties-file`
3. Run the OpenEdge Command Center installer file by performing the steps in [Launch the OpenEdge Command Center installer](#) on page 17.

Note: You can cancel the GUI installer after you have entered all the required information for the `.properties` file.

4. The `.properties` file is generated. You can rename the file, if necessary.

Run the silent installation

1. Open a command window and change to the directory that contains the `response.properties` file.
2. Enter the following command:
 - For the Linux platform, `./PROGRESS_OECC_SERVER_1.x.x_LNX_64.bin -i silent -f /response.properties-file`
 - For the Windows platform, `PROGRESS_OECC_SERVER_1.x.x_WIN_64.exe -i silent -f /response.properties-file`

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

Note: You can modify the contents of the `response.properties` file, but Progress recommends that you do not change any of the parameters other than passwords.

Set up OpenEdge Command Center with MongoDB Atlas on AWS

MongoDB Atlas is a fully managed, database-as-a-service (DBaaS) platform managed and administered by MongoDB. OpenEdge Command Center can be deployed with MongoDB as a managed database service from a cloud vendor.

To set up OpenEdge Command Center with MongoDB Atlas:

1. Ensure that you have a MongoDB Atlas installation with valid credentials and host name URL.
2. Launch the OpenEdge Command Center installer, as described in [Launch the OpenEdge Command Center installer](#) on page 17, and enter the **Host Configurations** and **Install Configurations** information.
3. On the **Database Configuration** page, enter the **Hostname/IP Address** information.
4. Select **Yes** for **Use SRV Record**. A service record is a specification of data in the domain name system defining the location that is, the host name and port number of servers for specified services.
5. Enter the username and password of the MongoDB Atlas instance.
6. Enter the Authentication Database information (set to **Admin** by default).
7. Click **Next**, and finish the remainder of the installations steps.

After the installation is complete, OpenEdge Command Center is set up with MongoDB Atlas in the cloud.

Deploy OpenEdge Command Center on Windows platform using a ZIP package

You can use installation package, to deploy the OpenEdge Command Center server on different Windows platforms. You can download the installation package, `PROGRESS_OECC_SERVER_1.x.x_WIN_64.zip`, from the Progress Software Download Center.

Before you deploy OpenEdge Command Center, you must set up MongoDB as the configuration database.

To deploy the OpenEdge Command Center server on a Windows platform, complete the following steps:

1. On your Windows computer, create a folder for OpenEdge Command Center installation files. For example, `C:\OECC_SERVER`.
2. In the installation folder, create a `conf` folder. For example, `C:\OECC_SERVER\conf`.
3. On your Windows computer, create a server data folder for the OpenEdge Command Center server data files. For example, `C:\OECC_DATA\data`.
4. In the server data folder, create another `conf` folder. For example, `C:\OECC_DATA\data\conf`.
5. Extract the `PROGRESS_OECC_SERVER_1.x.x_WIN_64.zip` file to the installation folder (`C:\OECC_SERVER`).
6. In the extracted folder, browse to the `orig` folder. Copy the specified files from the `orig` folder, place them in the folders you created, and rename them as follows:

File in the <code>orig</code> folder	New location and file name
<code>db-config.json.orig</code>	<Server data folder>\conf\db-config.json For example, <code>C:\OECC_DATA\data\conf\db-config.json</code>
<code>firstuser-config.json.orig</code>	<Server data folder>\conf\firstuser-config.json For example, <code>C:\OECC_DATA\data\conf\firstuser-config.json</code>

File in the orig folder	New location and file name
system-config.json.orig	<Server data folder>\conf\system-config.json For example, C:\OECC_DATA\data\conf\system-config.json
server-config.json.orig	<Installation folder>\conf\server-config.json For example, C:\OECC_SERVER\conf\server-config.json

7. Open the <Server data folder>\conf\db-config.json file in an editor and provide the following details of MongoDB:

- **dbHostNameAndPort:** The IP address and port of the MongoDB database. For example, 172.29.16.152:27017.
- **user and password:** The credentials used by the OpenEdge Command Center server to access the MongoDB database.
- **authSource:** Set the value to admin.

An example of the db-config.json file is as follows:

```
{
  "dbHostNameAndPort": "172.29.17.112:27017",
  "srvRecord": false,
  "connectOptions": {
    "useNewUrlParser": true,
    "useCreateIndex": true,
    "useFindAndModify": false,
    "autoIndex": true,
    "poolSize": 10,
    "bufferMaxEntries": 0,
    "connectTimeoutMS": 10000,
    "socketTimeoutMS": 45000,
    "useUnifiedTopology": true,
    "auth": {
      "user": "username",
      "password": "password"
    },
    "authSource": "admin"
  },
  "tls": false
}
```

8. Save the changes and close the file.

9. Open the <Server data folder>\conf\firstuser-config.json file in an editor and provide the following details of the first user:

- **firstName and lastName:** First and last names of the first user.
- **userName:** The username used by the first user to access OpenEdge Command Center.
- **email:** The email address of the first user.
- **password:** The password used by the first user to access OpenEdge Command Center.
- **description:** A description text about the first user.

10. Save the changes and close the file.

11. Open the <Installation folder>\conf\server-config.json file in an editor and provide the following details:
 - `port`: The port on which the OpenEdge Command Center server starts.
 - `dataDir`: The path to the server data folder. For example, `C:\\OECC_DATA\\data` or `C:/OECC_DATA/data`.
12. Save the changes and close the file.
13. Start the OpenEdge Command Center server from a command shell opened in the **Run as administrator** mode. For example:


```
C:\OECC_SERVER > oeccserver.bat start
```

Deploy OpenEdge Command Center on Linux platform using a TAR package

You can download the installation package, `PROGRESS_OECC_SERVER_1.x.x_LNX_64.tar.gz`, from the Progress Software Download Center and use it to deploy the OpenEdge Command Center server on a Linux 64-bit platform.

Before you deploy OpenEdge Command Center, you must set up MongoDB as the configuration database.

To deploy the OpenEdge Command Center server on a Linux platform, complete the following steps:

1. On your Linux computer, create a folder for OpenEdge Command Center installation files. For example, `/usr/OECC_SERVER`.

Note: Ensure that the folder name does not have any space because the Linux platform does not support spaces in the file path.

2. In the installation folder, create a `conf` folder. For example, `/usr/OECC_SERVER/conf`.
3. On your Linux computer, create a server data folder for the OpenEdge Command Center server data files. For example, `/usr/OECC_DATA/data`.
4. In the server data folder, create another `conf` folder. For example, `/usr/OECC_DATA/data/conf`.
5. Extract the `PROGRESS_OECC_SERVER_1.x.x_LNX_64.tar.gz` file to the installation folder (`/usr/OECC_SERVER`).
6. In the extracted folder, browse to the `orig` folder. Copy the specified files from the `orig` folder, place them in the folders you created, and rename them as follows:

File in the <code>orig</code> folder	New location and file name
<code>db-config.json.orig</code>	<Server data folder>/conf/db-config.json For example, <code>/usr/OECC_DATA/data/conf/db-config.json</code>
<code>firstuser-config.json.orig</code>	<Server data folder>/conf/firstuser-config.json For example, <code>/usr/OECC_DATA/data/conf/firstuser-config.json</code>

File in the orig folder	New location and file name
system-config.json.orig	<Server data folder>/conf/system-config.json For example, /usr/OECC_DATA/data/conf/system-config.json
server-config.json.orig	<Installation folder>/conf/server-config.json For example, /usr/OECC_SERVER/conf/server-config.json

7. Open the <Server data folder>/conf/db-config.json file in an editor and provide the following details of MongoDB:

- **dbHostNameAndPort:** The IP address and port of the MongoDB database. For example, 172.29.16.152:27017.
- **user and password:** The credentials used by the OpenEdge Command Center server to access the MongoDB database.
- **authSource:** Set the value to admin.

An example of the db-config.json file is as follows:

```
{
  "dbHostNameAndPort": "172.29.17.112:27017",
  "srvRecord": false,
  "connectOptions": {
    "useNewUrlParser": true,
    "useCreateIndex": true,
    "useFindAndModify": false,
    "autoIndex": true,
    "poolSize": 10,
    "bufferMaxEntries": 0,
    "connectTimeoutMS": 10000,
    "socketTimeoutMS": 45000,
    "useUnifiedTopology": true,
    "auth": {
      "user": "username",
      "password": "password"
    },
    "authSource": "admin"
  },
  "tls": false
}
```

8. Save the changes and close the file.

9. Open the <Server data folder>/conf/firstuser-config.json file in an editor and provide the following details of the first user:

- **firstName and lastName:** First and last names of the first user.
- **userName:** The username used by the first user to access OpenEdge Command Center.
- **email:** The email address of the first user.
- **password:** The password used by the first user to access OpenEdge Command Center.
- **description:** A description text about the first user.

10. Save the changes and close the file.

11. Open the `<Installation folder>/conf/server-config.json` file in an editor and provide the following details:
 - `port`: The port on which the OpenEdge Command Center server starts.
 - `dataDir`: The path to the server data folder. For example, `/usr/OECC_DATA/data`.
12. Save the changes and close the file.
13. Start the OpenEdge Command Center server from a Linux shell opened with the Super User or **root** privileges. For example:

```
./oeccserver.sh start
```

Uninstall OpenEdge Command Center

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

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

```
prompt> cd /usr/openedge_command_center/uninstall
```

2. Enter the following command:

```
./Uninstall OpenEdge Command Center -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.

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

Upgrade OpenEdge Command Center

You can upgrade an older version OpenEdge Command Center to the latest version using the OpenEdge Command Center installer. You can download the latest version of the installer from the [Progress Software Download Center](#).

It is recommended that you shut down the OpenEdge Command Center server before you start upgrade process.

To upgrade OpenEdge Command Center, complete the following steps:

1. Launch the OpenEdge Command Center installer on the computer with the older version of OpenEdge Command Center.
2. Read the information on the **Introduction** page, verify that all other applications are closed, and click **Next**.
The installer detects the older installation of OpenEdge Command Center on the computer and prompts you to confirm if the upgrade needs to be made.
3. To proceed with the upgrade, click **Continue**.
4. On the **Review** page, the installer displays the following information about the existing installation:
 - **Product Name**—OpenEdge Command Center.
 - **Install Folder**—Path where OpenEdge Command Center is installed.
 - **Link Folder**—Path where the database is installed.
 - **Disk Space Information**—Amount of space available and required by OpenEdge Command Center.

Check the information and click **Install**.

The new version OpenEdge Command Center is installed and configured using the configurations of the existing installation.

If the OpenEdge Command Center server is set up as a service, the OpenEdge Command Center console automatically opens in a web browser after the upgrade is complete.

Revert to the previous installation

When you upgrade the OpenEdge Command Center installation, the `backup` folder is created in the OpenEdge Command Center installation directory. The `backup` folder contains configurations and data of the previous installation.

To revert to the previous installation, complete the following steps:

1. Shut down the OpenEdge Command Center server.
2. Copy the configuration and data files from the `backup` folder and replace the files in the OpenEdge Command Center installation directory.
3. Restart the OpenEdge Command Center server.

Install OpenEdge Command Center Agents

OpenEdge Command Center is an add-on product to OpenEdge. It can be downloaded and installed independently of OpenEdge. After installing OpenEdge Command Center, use the agent installer to install and configure an agent. Download the setup file to your local machine.

Before you install the OpenEdge Command Center agent on a single machine 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 Information Hub](#). You can also refer the document for information on compatibility of OpenEdge Command Center with OpenEdge releases.

Note: OpenEdge Command Center agents are supported only on 64-bit platforms. They are supported on all operating systems that support OpenEdge 12.2.5 and later releases, such as Windows, Linux, AIX, and Solaris. The JDK requirements of agents comply with OpenEdge 12.2.x JDK requirements.

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_1.x.x_WIN_64.exe PROGRESS_OECC_AGENT_1.x.x_WIN_64.zip
Linux	PROGRESS_OECC_AGENT_1.x.x_LNX_64.bin PROGRESS_OECC_AGENT_1.x.x_LNX_64.tar.gz
AIX	PROGRESS_OECC_AGENT_1.x.x_AIX_64.bin
Solaris	PROGRESS_OECC_AGENT_1.x.x_SOL_64.bin

2. Run the installer file. For example:

```
./PROGRESS_OECC_AGENT_1.x.x_LNX_64.bin
```

By default, the installer runs in graphical mode. However, if you are running the installation in VM 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. Read the information on the **Introduction** page, verify that all the other applications are closed, and click **Next**.
4. Read and accept the End User License Agreement (EULA), and click **Next**.
5. On the **Install Configurations** page, enter the following information:
 - a. In **Agent Installation Directory**, you can optionally choose a nondefault directory in which you want to install the agent.
 - b. Check the **Install Agent as a service** option if you want to install the agent as a service. (When this option is enabled, the agent is automatically launched as a service.)
 - c. In **Java Home Directory**, specify the root directory in which the JDK is installed. The directory must match the one that is defined as the `JAVA_HOME` environment variable.
 - d. Click **Next**.
6. On the **Server Connections** page, enter the following information:
 - a. In **Upload OECC Agent Key File**, you can optionally specify an OECC Agent Key JSON file to autofill the fields on this page. If you specify this file, skip to Step d.
 - b. In **Server Host Name**, specify the name of the host machine on which you are installing the agent.
 - c. In **Server Port**, specify:
 - **Server Host Name**
 - **Server Port**

Check the Server Secure Connection to enable agent communication in secure mode using Secure Web Socket. This option is disabled by default.

- **Agent Key Name**
- **Agent Key**

Note: Optionally, you can leave the preceding four fields blank and, after installation, update the agent properties manually to specify these entities.

The agent key name and agent key can be generated on OpenEdge Command Center. For more information, see 'Generate new agent keys' in *Use the OpenEdge Command Center*.

d. Click **Next**.

7. On the **OpenEdge Installation Directories** page, browse to the OpenEdge installation directory and select the instance you want to map with the agent, then click **Next**.

8. Review the information you have provided before completing the installation and click **Next**.

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

9. Click **Done** to complete the agent installation.

For details, see the following topics:

- [Silently install OpenEdge Command Center agents](#)
- [Deploy OpenEdge Command Center agent on Windows platform using a ZIP package](#)
- [Deploy OpenEdge Command Center agent on Unix platform using a TAR package](#)
- [Uninstall OpenEdge Command Center agents](#)
- [Upgrade OpenEdge Command Center agent](#)

Silently install OpenEdge Command Center agents

To silently install an OpenEdge Command Center agent, you create a response file that is based on a template. You then run the response file as a script.

Response file template

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

```
# Tue Mar 09 02:46:56 EST 2021
# 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=
OECC_AGENT_AS_SERVICE=0
OECC_JAVA_HOME=

#Server Connection
```

```
#-----
AGENT_KEY_FILE=
SERVER_HOST_NAME=
SERVER_PORT=
AGENT_KEY=
AGENT_KEY_NAME=
SERVER_SEC_CONNECTION=0

#OpenEdge Installations
#-----
OE_INSTALL_DIR_1=
OE_INSTALL_DIR_2=
```

When you create the response file based upon the preceding 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"> 0—The agent is not started as a service automatically after installation is complete. 1—The agent is started automatically after installation is complete.
OECC_JAVA_HOME	The directory that contains the JDK, which must be version 11.0.4 or later.
AGENT_KEY_FILE	The fully-qualified path of the JSON file that contains the server information.
SERVER_HOST_NAME	The IP address of the OpenEdge Command Center server. Specify a value if AGENT_KEY_FILE is not specified. (If AGENT_KEY_FILE is already specified, specifying a value here is optional.)
SERVER_PORT	The OpenEdge Command Center server port number. Specify a value if AGENT_KEY_FILE is not specified. (If AGENT_KEY_FILE is already specified, specifying a value here is optional.)
AGENT_KEY	The key assigned to the agent. Specify a value if AGENT_KEY_FILE is not specified. (If AGENT_KEY_FILE is already specified, specifying a value here is optional.)

For the following variable specify the following
SERVER_SEC_CONNECTION	Whether a secure transport is used to communicate with OpenEdge Command Center server. The possible values are: <ul style="list-style-type: none"> 0—Specifies that a secure transport is not used. 1—Specifies that a secure transport is used.
OE_INSTALL_DIR_1	(Optional) A directory that contains an OpenEdge installation.
OE_INSTALL_DIR_2	(Optional) A second directory that contains an OpenEdge installation.

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:

```
PROGRESS_OECC_AGENT_1.x.x_platform -i silent -f /response-file-name
```

In the preceding command:

- *platform* represents the operating system-specific suffix of the installer file name. For example, WIN_64.exe or LNX_64.bin.
- *response-file-name* represents the name of the silent installation response file.

After you enter the preceding command, the agent installation runs without intervention.

A log file of the installation procedure is available in the `logs` subdirectory of the agent installation directory.

Deploy OpenEdge Command Center agent on Windows platform using a ZIP package

You can use installation package, `PROGRESS_OECC_AGENT_1.x.x_WIN_64.zip`, to deploy an OpenEdge Command Center agent on a Windows 64-bit computer with a PAS for OpenEdge installation. The installation package can be deployed on all Windows platforms that support OpenEdge 12.2.5 and later releases. You can download the installation package from the Progress Software Download Center.

To deploy the OpenEdge Command Center agent on a Windows platform, complete the following steps:

1. On the Windows computer that hosts the PAS for OpenEdge installation you want to monitor, create a folder for the OpenEdge Command Center agent installation files. For example, `C:\OECC_AGENT`.
2. Extract the contents of the `PROGRESS_OECC_AGENT_1.x.x_WIN_64.zip` file to the installation folder (`C:\OECC_AGENT`).
3. In the extracted folder, browse to the `orig` folder. For example, `C:\OECC_AGENT\orig`.

4. Copy the following files from the `orig` folder:

- `installationsInfo.json.orig`
- `java.properties.orig`
- `serverInfo.json.orig`

5. Place the copied files in the `conf` folder of the extracted files. For example, `C:\OECC_AGENT\conf`.

6. Rename the copied files in the `conf` folder as follows:

File name in the <code>orig</code> folder	File name in the <code>conf</code> folder
<code>installationsInfo.json.orig</code>	<code>installationsInfo.json</code>
<code>java.properties.orig</code>	<code>java.properties</code>
<code>serverInfo.json.orig</code>	<code>serverInfo.json</code>

7. Open the `\conf\serverInfo.json` file in any text editor and provide the following details:

- `host`: The IP address of the OpenEdge Command Center server.
- `port`: The port number of the OpenEdge Command Center server.
- `agentKey` and `agentKeyName`: Generate agent key and agent key name in the OpenEdge Command Center console and enter the respective values.

For more information, see 'Generate new agent keys' in *Use the OpenEdge Command Center*.

8. Save the changes and close the file.

9. Open the `\conf\java.properties` file in any text editor and provide the path to the root directory in which the JDK is installed. For example, `JAVA_HOME=C:/jdk11.0.4_x64`.

10. Save the changes and close the file.

11. Open the `\conf\installationsInfo.json` file in any text editor. For the `path` field, enter the path to the OpenEdge installation directory that you want to monitor. For example, if the OpenEdge instance you want to monitor is installed at `C:\Progress\OpenEdge` on your computer, enter the value of `path` as `C:\\Progress\\OpenEdge` or `C:/Progress/OpenEdge`.

12. Save the changes and close the file.

13. Start the OpenEdge Command Center agent from a command shell opened in the **Run as Administrator** mode. For example:

```
C:\OECC_AGENT > oeccagent.bat start
```

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

Deploy OpenEdge Command Center agent on Unix platform using a TAR package

You can use installation package, `PROGRESS_OECC_AGENT_1.x.x_LNX_64.tar.gz`, to deploy an OpenEdge Command Center agent on a Unix 64-bit computer with a PAS for OpenEdge installation. The installation package can be deployed on all Unix platforms that support OpenEdge 12.2.5 and later releases. You can download the installation package from the Progress Software Download Center.

To deploy the OpenEdge Command Center agent on a Unix platform, complete the following steps:

1. On the Unix computer that hosts the PAS for OpenEdge installation you want to monitor, create a folder for the OpenEdge Command Center agent installation files. For example, `/usr/OECC_AGENT`.

Note: Ensure that the folder name does not have any space because the Unix platform does not support spaces in the file path.

2. Extract the contents of the `PROGRESS_OECC_AGENT_1.x.x_LNX_64.tar.gz` file to the installation folder (`/usr/OECC_AGENT`).
3. In the extracted folder, browse to the `orig` folder. For example, `/usr/OECC_AGENT/orig`.
4. Copy the following files from the `orig` folder:
 - `installationsInfo.json.orig`
 - `java.properties.orig`
 - `serverInfo.json.orig`
5. Place the copied files in the `conf` folder of the extracted files. For example, `/usr/OECC_AGENT/conf`.
6. Rename the copied files in the `conf` folder as follows:

File name in the <code>orig</code> folder	File name in the <code>conf</code> folder
<code>installationsInfo.json.orig</code>	<code>installationsInfo.json</code>
<code>java.properties.orig</code>	<code>java.properties</code>
<code>serverInfo.json.orig</code>	<code>serverInfo.json</code>

7. Open the `/conf/serverInfo.json` file in any text editor and provide the following details:
 - `host`: The IP address of the OpenEdge Command Center server.
 - `port`: The port number of the OpenEdge Command Center server.
 - `agentKey` and `agentKeyName`: Generate agent key and agent key name in the OpenEdge Command Center console and enter the respective values.

For more information, see 'Generate new agent keys' in *Use the OpenEdge Command Center*.

8. Save the changes and close the file.

9. Open the `/conf/java.properties` file in any text editor and provide the path to the root directory in which the JDK is installed. For example, `JAVA_HOME=/opt/jdk11.0.4_x64`.
10. Save the changes and close the file.
11. Open the `/conf/installationsInfo.json` file in any text editor. For the `path` field, enter the path to the OpenEdge installation directory that you want to monitor. For example, if the OpenEdge instance you want to monitor is installed at `/usr/Progress/OpenEdge` on your computer, enter the value of `path` as `/usr/Progress/OpenEdge`.

If you have multiple OpenEdge installations, add more `path` fields and enter the installation directory path of the other OpenEdge installations on the computer. For example:

```
"installations" : [ {  
  "path" : "/usr/124dlc"  
}, {  
  "path" : "/usr1/122dlc"  
} ]
```

12. Save the changes and close the file.
13. Start the OpenEdge Command Center agent from a Unix shell opened with the Super User or **root** privileges. For example:

```
./oeccagent.sh start
```

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

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.

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

```
prompt> cd C:\Progress\OECC_Agent\uninstall
```

2. Enter the following command:

```
prompt> Uninstall OECC Agent
```

The uninstaller runs in interactive mode, prompting you to confirm your uninstallation choices.

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

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 **OpenEdge Command Center Agent**, then click **Uninstall**.

Upgrade OpenEdge Command Center agent

You can upgrade an older version OpenEdge Command Center agent to the latest version using the agent installer. You can download the latest version of the installer from the [Progress Software Download Center](#). Click the **Open Download Center** link and log in using your Progress SSO credentials. From the product list, select **Progress OpenEdge**, and then select the appropriate OpenEdge version. To download OpenEdge Command Center components, you must select OpenEdge 12.2.x or later. From the **New Release** tab, select the link for OpenEdge Command Center, and then download the required installation files.

It is recommended that you shut down the OpenEdge Command Center agent before you start upgrade process.

To upgrade the OpenEdge Command Center agent, complete the following steps:

1. Launch the OpenEdge Command Center agent installer on the computer with the older version of the agent.
2. Read the information on the **Introduction** page, verify that all other applications are closed, and click **Next**.

The installer detects the older installation of the agent on the computer and prompts you to confirm if the upgrade needs to be made.

3. To proceed with the upgrade, click **Continue**.
4. On the **Review** page, the installer displays the following information about the existing agent installation:

- **Product Name**—OpenEdge Command Center Agent.
- **Install Folder**—Path where the OpenEdge Command Center agent is installed.
- **Link Folder**—Path where the database is installed.
- **Disk Space Information**—Amount of space available and required by the OpenEdge Command Center agent.

Check the information and click **Install**.

The new version OpenEdge Command Center agent is installed and configured using the configurations of the existing installation.

Revert to the previous installation

When you upgrade the OpenEdge Command Center agent installation, the `backup` folder is created in the agent installation directory. The `backup` folder contains configurations and data of the previous installation.

To revert to the previous installation, complete the following steps:

1. Shut down the OpenEdge Command Center agent.
2. Copy the configuration and data files from the `backup` folder and replace the files in the agent installation directory.
3. Restart the OpenEdge Command Center agent.

How to

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

For information how to see
Log in	Log in to OpenEdge Command Center on page 43
Set your password	Change or reset passwords on page 43
Work with agents	<ul style="list-style-type: none">• Configure new OpenEdge Command Center agents on page 44• Manage agent services on page 45• Add agent labels on page 85• Generate new agent keys on page 86• Search for and filter agents on page 87
Configure PAS for OpenEdge	<ul style="list-style-type: none">• Create a PAS for OpenEdge instance on page 61• Modify PAS for OpenEdge configuration properties on page 48

For information how to see
Manage PAS for OpenEdge	<ul style="list-style-type: none"> • Start or stop a PAS for OpenEdge instance on page 63 • Delete a PAS for OpenEdge instance on page 64 • Obtain process details on page 64
Set up email	Configure email settings on page 88
Add users	Add a new user on page 89

For details, see the following topics:

- [Log in to OpenEdge Command Center](#)
- [Change or reset passwords](#)
- [Configure new OpenEdge Command Center agents](#)
- [Manage agent services](#)
- [Manage services for OpenEdge Command Center server](#)
- [Change logging level](#)
- [Configure and manage PAS for OpenEdge instances](#)
- [Manage ABL applications, web applications, and REST services](#)
- [Monitor OpenEdge resources using the OpenEdge Command Center agent](#)
- [Add agent labels](#)
- [Update agent labels](#)
- [Generate new agent keys](#)
- [Search for and filter agents](#)
- [Configure email settings](#)
- [Add a new user](#)
- [Reset the super administrator password](#)
- [Set up TLS](#)

Log in to OpenEdge Command Center

To access OpenEdge Command Center console dashboard from a web browser:

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

The host is the name of a machine 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**.

You can access the OpenEdge Command Center console dashboard from any browser.

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
- Applications Servers
- Command Center Agents
- Users
- Agent Keys
- Console Settings
- Email Settings

Each option provides a list of actions that you can perform.

Note: Your session times out if OpenEdge Command Center detects no activity for more than 30 minutes.

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 new OpenEdge Command Center agents

After you install OpenEdge Command Center, the following configuration files are placed in the installation directory.

- `installationsInfo.json`
- `java.properties`
- `serverInfo.json`

You can modify these files to configure and create new OpenEdge Command Center agents.

To configure a new agent:

1. Open the **oecc-agent** folder from the installation directory.
2. Go to the **conf** folder.
3. Update the `installationsInfo.json` file.

```
{
  "_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": "installation path"
  }]
}
```

Insert the OpenEdge installation path.

4. Update the `serverInfo.json` file

```
"host": "hostname",
"port": "port",
"agentKey": "agentkey",
"agentKeyName": "agentkeyname",
"isServerSecured": false
```

Specify values for the following parameters:

- **Hostname**—Name of the machine where OpenEdge Command Center is hosted.
- **Port**—Port on which the OpenEdge Command Center is running.
- **AgentKey**—Key that is generated from OpenEdge Command Center.
- **AgentKeyName**—Agent key name given while creating the agent key.
- **isServerSecure**—Set to `true` if TLS is enabled.

After you configure the agents, the agent information is available from the OpenEdge Command Center Agents page. The PAS for OpenEdge instances associated with the agent are discovered and are listed on the dashboard as well as on the PAS for OpenEdge instances page.

Manage agent services

After you start an agent, the status of the agent is updated in the **Command Center Agents** page. Note that the status of an agent cannot be updated from the OpenEdge Command Center. You can create the OpenEdge Command Center agent service to start an agent as a system service.

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

To create, start, stop or delete an agent service:

1. From a command window that is set with administrator privileges, change to the `conf` subdirectory of the OpenEdge Command Center agent installation directory.
2. Run the following command:

Windows:

```
OECCAgentService.bat create|start|stop|delete
```

Linux, Solaris, and AIX:

```
OECCAgentService.sh create|start|stop|delete
```

When you run a create command, the agent service is created with different names on these platforms because the service naming conventions differ across the platforms. For example, the length of a service name on the AIX platform cannot be more than 29 characters. The details of services created on different platform are as follows:

Platform	Service Name
Windows	Progress OpenEdge Command Center Agent
Linux and Solaris	Progress-OpenEdge-Command-Center-Agent
AIX	ProgressOECommandCenterAgent

Note: The agent maintains two log files for capturing the following messages:

- Agent-related error messages
- Agent-related standard output messages
- Agent service-related messages regarding agent create, start, stop, and delete operations

These log files are named `oecc-agent.out<timestamp>.log` and `oecc-agent.err<timestamp>.log`. On Windows, AIX, and Linux platforms, these files are maintained in the `agent-install-dir/logs` directory by default.

On Solaris platforms, the log file names and locations for agent-related messages are the same as for Windows, AIX, and Linux. However, agent *service*-related messages (that is, for agent service create, start, stop, and delete operations) are placed in the `/var/svc/log/application-Progress-OpenEdge-Command-Center-Agent:default.log` file.

On Linux platforms with `systemd` version earlier than 236, agent logs are not generated in the `agent-install-dir/logs` directory. This occurs only when the OpenEdge Command Center agent is started as a service. Therefore, on these Linux systems, Progress recommends that you run the following command to generate agent logs:

```
journalctl -u Progress-OpenEdge-Command-Center-Agent
```

Manage services for OpenEdge Command Center server

You can create the OpenEdge Command Center server service on a Linux 64-bit platform to start OpenEdge Command Center as a system service.

To create, start, stop, or delete the OpenEdge Command Center service:

1. From a command window that is set with administrator privileges, change to the conf subdirectory of the OpenEdge Command Center installation directory.
2. Run the following command:

```
oeccservice.sh create|start|stop|delete
```

When you run the create command, the `Progress-OpenEdge-Command-Center-Server` service is created.

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.

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 **Progress Application Servers** 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.

Modify PAS for OpenEdge configuration properties

To modify the configuration of a 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 **Info** section, update values for the following properties:

Field	Description
Instance Name	Name of the PAS for OpenEdge instance.
	Note: 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.
Labels	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
HTTPS Connector	ON	Use the ON/OFF toggle switch to enable or disable the HTTPS connector respectively.
Port	8443	Specifies the HTTPS protocol connector port number.
Connection Timeout	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.
SSL Session Timeout	86400	Specifies the time, in seconds, after which the TLS session ends.
Server Key Alias	test	Specifies the alias name of the keystore entry holding the server's private key and public key certificate.
Server Key Password	password	Specifies the password to use when accessing the TLS keystore.
Store Type	PKCS12	Specifies the type of Java keystore format used by Apache Tomcat keystore.
Max Queue Size	100	Specifies the maximum size of the HTTPS connector message queue.
Max Connections	-1	Specifies the maximum number of TCP socket connections per HTTPS connector.

Property	Default value	Description
Client Authentication	none	Specifies whether to enable or disable TLS client authentication by the HTTPS connector. The options are required , none , and optional . The default is none.
Certificate Trust Type	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.
Certificate Store Password	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.
Encryption Protocol	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.
Enabled Cyphers	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.
Bind On Init	false	Check box to control when to bind the socket used by the connector.
Compression	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
HTTP Connector	ON	Use the ON/OFF toggle switch to enable or disable the HTTP connector respectively.
Port	8090	Specifies the HTTP protocol connector port number.
Connection Timeout	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.

Property	Default value	Description
Max Connections	-1	Specifies the maximum number of TCP socket connections per HTTP connector.
Max Queue Size	100	Specifies the maximum size of HTTP connector message queue.
URI Encoding	ISO-8859-1	<p>Specifies the character encoding used to decode the URI bytes after decoding the URL.</p> <hr/> <p>Note: This value is set to the default value of the Apache Tomcat server, and it affects both the HTTP and HTTPS connectors.</p> <hr/>
Bind On Init	false	Check box to control when to bind the socket used by the connector.
Compression	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
Shutdown Port	—	<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>
Shutdown Password	SHUTDOWN	<p>Specifies a private shutdown port access code to prevent one server instance from being shutdown by anyone.</p> <hr/> <p>Note: If the shutdown port is specified, you must change this value to avoid insecure configuration.</p> <hr/>
Stuck Session Valve	ON	TBD
Stuck Thread Threshold	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.

Property	Default value	Description
Max Threads	300	Specifies the maximum number of OS process threads the PAS for OpeEdge Server can use.
Minimum Spare Threads	10	Specifies the number of spare threads the server reserves for future client operations.
Web Application Directory	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>
Common Library Path	—	<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 (https://tomcat.apache.org/tomcat-9.0-doc/class-loader-howto.html).</p>
Auto Deploy WAR Files	false	<p>Select the checkbox to enable the security settings used by the Apache Tomcat server for deploying web applications.</p> <p>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>.</p>
Unpack WAR Files	true	Select the checkbox to allow unpacking of web archive (<code>.war</code>) files when the PAS for OpenEdge instance is started.
Version Logger	ON	Use the ON/OFF toggle to enable or disable logging the command line arguments passed to Java when the Apache Tomcat server is started.
Log Command Line Arguments	true	Select the checkbox to log the command line arguments passed to Java when the Apache Tomcat server is started.

Property	Default value	Description
Log Environment Variables	false	Select the checkbox to log the current environment variables when the Apache Tomcat server is started.
Log Java System Properties	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
Max POST Request Size	2097152	Specifies the maximum size, in bytes, of a connector's POST message body.
Max Pipeline Requests	100	Specifies the maximum number of pipelined HTTP keepalive requests before the TCP socket to the client is closed.
Message Timeout	10000	Specifies the maximum time, in milliseconds, to wait for asynchronous messages to complete.
Compression Minimum Size	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.
Compression MIME Types	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
Catalina Logging Level	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.
OpenEdge ABL Logging Level	WARN	Sets the log level for ABL application (oeabl.war) Session Manager and Spring Security logging.
Authentication Logging Level	ERROR	Sets the log level for ABL application login event logging.
Authorization Logging Level	ERROR	Sets the log level for ABL application URL access event logging.
OpenEdge STS Logging Level	WARN	Sets the log level for the OpenEdge Authentication Gateway server Security Token Service web application.

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

Provide values for the following properties:

Property	Description
Agent Log entry types	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
Agent Log Level	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 **Agent Log entry types** and **Agent Log Level** properties are applied without restarting the PAS for OpenEdge instance.

Filter PAS for OpenEdge configuration 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 PAS for OpenEdge properties:

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 of the configuration property you want to modify.

For example, enter `SSL session timeout` to modify the HTTPS connection property **SSL Session Timeout**. Only the **SSL Session Timeout** field is displayed on the **Edit PAS For OpenEdge Instance** page.

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 **PASOE Instances**.

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
Instance Name	<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>Note: 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/>
Instance Size	View the size of the cloned PAS for OpenEdge instance. This value is automatically calculated by OpenEdge Command Center.

In the following field do the following
Labels	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_<source></code> is added to the field.
OpenEdge Installation	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. 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 Overwrite duplicate PAS for OpenEdge instance option removes the red color and allows you to proceed with the cloning.
Overwrite duplicate PAS for OpenEdge instance	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.
Start PAS for OpenEdge instance after it is cloned	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 in 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 **PAS for OpenEdge 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.

NAME	STATUS	LABELS	HOST NAME	CATALINA BASE	VERSION
windevmng	OFFLINE		W10X64	C:\OpenEdge\WRK\windevmng	12.4.0
nomngdev	OFFLINE		W10X64	C:\OpenEdge\WRK\nomngdev	12.4.0
prodnomngwin	OFFLINE		W10X64	C:\OpenEdge\WRK\prodnomngwin	12.4.0
prodmgwin	OFFLINE		W10X64	C:\OpenEdge\WRK\prodmgwin	12.4.0
TestPASCentOSMgrProd	RUNNING	TestPA...	localhost.localdomain	/usr/WRK/TestPASCentOSMgrProd	12.4.0
TestPASWin	RUNNING	paswin	W2K16BASE	C:\OpenEdge\WRK\TestPASWin	12.4.0
lindvmng	RUNNING		localhost.localdomain	/usr/WRK/lindvmng	12.4.0
wintestnew	OFFLINE		W10X64	C:\OpenEdge\WRK\wintestnew	12.4.0
TestPASNoMgr	RUNNING		localhost.localdomain	/usr/WRK/TestPASNoMgr	12.4.0
TestPASNoMgr1	RUNNING	TestPA...	localhost.localdomain	/usr/WRK/TestPASNoMgr1	12.4.0
TestPAS2	RUNNING	TestPA2	localhost.localdomain	/usr/WRK/TestPAS2	12.4.0
TestPASNoMgr2	RUNNING	TestPA...	localhost.localdomain	/usr/WRK/TestPASNoMgr2	12.4.0
newmangdep	OFFLINE		W10X64	C:\OpenEdge\WRK\newmangdep	12.4.0
TestPASNoMgr3	RUNNING	TestPA...	localhost.localdomain	/usr/WRK/TestPASNoMgr3	12.4.0

Please select a PAS instance to view ABL applications

2. Click 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, it's deployment path, number of services, and the status the four transports is displayed.

NAME	PATH	SERVICES	TRANSPORTS
TestPASWin	/	1	REST WEB SOAP APSV
TestPASWin	/oeabl	1	REST WEB SOAP APSV

Note: The OpenEdge Command Center release 1.0 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 applications or ABL web applications

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

1. In the OpenEdge Command Center console, click **PAS for OpenEdge 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. Click the check-box next to the instance name on which you want to deploy the ABL application or web application.

3. In the **Applications** window on the lower part of the screen, click **Deploy**.

The **Deploy Applications** dialog box is displayed.

At this point in the procedure you can choose to either deploy a new ABL application or a web application that is associated with an existing ABL application.

4. To deploy a new ABL application:

- a. In the **Deploy Applications** dialog box choose **ABL Application** as the Application Type.

- b. Define the **ABL Application Name**.

- c. In the **Select application file** field, click **Select File** and browse to the location of the ABL application WAR file.

- d. In the **Web Application Name** field, enter the name of the web application that is to be associated with the ABL application.

Note: The name is automatically detected from the WAR file is displayed by default. You can change the application name as desired.

- e. Enter your Apache Tomcat manager login and password.

Note: OpenEdge Command Center supports live deployment of ABL applications if PAS for OpenEdge is running and the manager application is in an enabled state. There is no restart required to load the context of applications with the PAS for OpenEdge instance. If you enter the incorrect manager login credentials, the application deployment becomes a normal deployment and requires the PAS for OpenEdge instance to restart.

Deploy Applications


PAS Instance
TestLinux

Application Type
☒ ABL Application
☐ Web Application

ABL Application Name
SalesUS

Select Application File

Select files...
Drop files here to upload

 oedbg.war
2.66 KB

Web Application Name
SalesUS

Tomcat Manager Login
jHenderson

Tomcat Manager Password
.....

Cancel
Deploy

5. To deploy a web application:

- a. In the **Deploy Applications** dialog box choose **Web Application** as the Application Type.
- b. In the **Select ABL Application** field, select an ABL application from the drop down list.
- c. In the **Select application file** field, click **Select File** and browse to the location of the ABL application WAR file.
- d. In the **Web Application Name** field, enter the name of the web application that is to be associated with the ABL application.

Note: The name is automatically detected from the WAR file is displayed by default. You can change the application name as desired.

- e. Enter your Apache Tomcat manager login and password.

Note: OpenEdge Command Center supports live deployment of ABL applications if PAS for OpenEdge is running and the manager application is in an enabled state. There is no restart required to load the context of applications with the PAS for OpenEdge instance. If you enter the incorrect manager login credentials, the application deployment becomes a normal deployment and requires the PAS for OpenEdge instance to restart.

Deploy Applications

PAS Instance

TestLinux

Application Type

☐ ABL Application
☒ Web Application


Select ABL Application

TestLinux

Select Application File

Select files...

Drop files here to upload

 oedbg.war
2.66 KB

Web Application Name

SalesUS

Tomcat Manager Login

jHenderson

Tomcat Manager Password

.....

Cancel

Deploy

6. Click **Deploy**.

After you deploy the application, a deployment notification is displayed in the Command Center screen. You can click the bell icon to refresh the notification and obtain status on the deployment operation.

Undeploy ABL applications or ABL web applications

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

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

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

2. Click the check-box next to the instance name on which you want to undeploy the ABL or web application.

The Application window appears below.

3. In the **Applications** window, click the check-box for the ABL application that you want to undeploy.

The web applications associated with the ABL application appear.

4. If you want to undeploy web applications only, select them by clicking the check box next to their name. You can undeploy multiple applications at a time.

5. Click the **Actions** drop down menu and choose either:

- Undeploy ABL Applications** to undeploy the ABL application and any web application associated with it.
- Undeploy WEB Applications** to undeploy the indicated web applications only.

The Undeploy Applications dialog box appears.

6. In the **Undeploy Applications** dialog box, enter your Apache Tomcat manager log in credentials to confirm the undeploy command.

Note: By design, undeploying a running web application leaves it loaded in the OpenEdge Command Center interface until next PAS for OpenEdge restart operation. OpenEdge Command Center supports loading context of the undeployed application when a manager application is enabled and PAS for OpenEdge is running. This is done to assist administrators to manage the availability of other ABL applications until their planned application downtimes.

After you undeploy the application, a deployment notification is displayed in the Command Center screen. You can click the bell icon to refresh the notification and obtain status on the deployment operation.

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

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 **PAS 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. Click **New**.

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

In the following field do the following
Instance Name	Specify a name for the PAS for OpenEdge instance. This is a mandatory field. Note: 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.
OpenEdge Installation	Use the drop-down box to select the OpenEdge installation that corresponds to the PAS for OpenEdge instance that you want to create.
Labels	Use the drop-down box to select one or more labels, or create one or more new labels to assign.

In the following field do the following
Security Model	<p>Specify one of the following security models:</p> <ul style="list-style-type: none"> • Production If you select this model, you can make configuration changes to adjust security settings to ensure your application operates correctly in a production instance. • Developer 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.
Instance Directory	<p>Specify the path of the PAS for OpenEdge instance.</p> <hr/> <p>Note: 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/>
HTTP Port	<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>Note: 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/>
HTTPS Port	<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>Note: 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/>

In the following field do the following
Shutdown Port	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. Note: 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.
Login	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> .
Password	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> .

- 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.
- 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:

- In the OpenEdge Command Center console, click **PAS Instances**.

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

- 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.

- 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 **PAS 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 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 **PAS 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 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 or single pane of glass 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 ABL application across multiple PAS for OpenEdge instances, click the **ABL Applications** tab in the OpenEdge Command Center console. The **ABL Applications** tab has the following panes:

- ABL Applications
- Web Applications
- Services

ABL Applications pane

The **ABL Applications** pane displays a list of ABL applications deployed on the different PAS for OpenEdge instances. The list displays the name of the:

- ABL applications
- PAS for OpenEdge instance where the applications are deployed
- OpenEdge Command Center agents for the PAS for OpenEdge instances

To sort the list, click the required column header and the arrow displayed beside the header.

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

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

You can also deploy additional ABL applications from this pane. For more information, see [Manage ABL applications](#) on page 66.

Web Applications pane

The **Web Applications** pane displays the web applications deployed on the ABL application selected in the ABL Applications pane. 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 68.

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 69.

Manage ABL applications

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

- Deploy ABL applications
- Undeploy ABL applications

Deploy ABL applications

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

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

The **ABL Applications** tab is displayed, showing ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.

2. In the **ABL Applications** pane, click **Actions > Deploy**.

The **Deploy Applications** dialog box is displayed.

3. In the **Select PASOE Instance** list, expand the agent node and then select the PAS for OpenEdge instance where you want to deploy the ABL application.
4. Select the **ABL Application** option.
5. In the **ABL Application Name** field, type the application name .
6. In the **Select Application File** field, click **Select File** and browse to the location of the ABL application WAR file.
7. In the **Web Application Name** field, type the name of the web application that is to be associated with the ABL application.

Note: The 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 as desired.

8. Based on the status of the PAS for OpenEdge instance and deployment of the Manager application, you may have to enter the Apache Tomcat Manager credentials or restart the PAS for OpenEdge instance. The following table lists the different scenarios:

If		Then	
PAS for OpenEdge instance is running	Manager application is enabled	Enter Apache Tomcat Manager credentials	Restart PAS for OpenEdge instance
Yes	Yes	Required	Not required
Yes	No	Not required	Required
No	No	Not required	Required

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

Undeploy ABL applications

To undeploy an ABL application:

1. In the **ABL Applications** pane, select the ABL application you want to undeploy, and click **Actions > Undeploy**.

The **Undeploy ABL Application** dialog box is displayed.

2. Based on the state of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, you perform one of the following steps:

If	Then
The PAS for OpenEdge instance is stopped	Click Undeploy .

If	Then
The PAS for OpenEdge instance is running but the Manager application is not deployed	Review the warning message and click Undeploy & Restart .
The PAS for OpenEdge instance is running and the Manager application is deployed	Enter the Apache Tomcat Manager credentials and click Undeploy .

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

- Optional. Check notifications to confirm if the ABL application was undeployed successfully.

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 applications

To deploy a web application in an existing ABL application:

- In the OpenEdge Command Center console, click **ABL Applications**.
The **ABL Applications** tab is displayed, showing ABL applications, web applications, and services deployed across multiple PAS for OpenEdge instances.
- In the **ABL Applications** pane, click **Actions > Deploy**.
The **Deploy Applications** dialog box is displayed.
- In the **Select PASOE Instance** list, expand the agent node and then select the PAS for OpenEdge instance where you want to deploy the ABL application.
- Select the **Web Application** option.
- In the **Select ABL Application** list, select an existing ABL application.
- In the **Select Application File** field, click **Select File** and browse to the location of the ABL application WAR file.
- In the **Web Application Name** field, type the name of the web application.

Note: The 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 as desired.

- Based on the status of the PAS for OpenEdge instance and deployment of the Manager application, you may have to enter the Apache Tomcat Manager credentials or restart the PAS for OpenEdge instance. The following table lists the different scenarios:

If		Then	
PAS for OpenEdge instance is running	Manager application is enabled	Enter Apache Tomcat Manager credentials	Restart PAS for OpenEdge instance
Yes	Yes	Required	Not required
Yes	No	Not required	Required
No	No	Not required	Required

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

Undeploy web applications

To undeploy a web application:

1. In the **Web Applications** pane, locate the card of the web application you want to undeploy.
2. In the web application card, click **Undeploy**.

The **Undeploy Web Applications** dialog box is displayed.

3. Based on the state of the PAS for OpenEdge instance and deployment of the Apache Tomcat Manager application, you perform one of the following steps:

If	Then
The PAS for OpenEdge instance is stopped	Click Undeploy .
The PAS for OpenEdge instance is running but the Manager application is not deployed	Review the warning message and click Undeploy & Restart .
The PAS for OpenEdge instance is running and the Manager application is deployed	Enter the Apache Tomcat Manager credentials and click Undeploy .

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

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

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 **ABL Applications**.

The **ABL Applications** tab is displayed.

2. In the **ABL Applications** pane, 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.

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.

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.

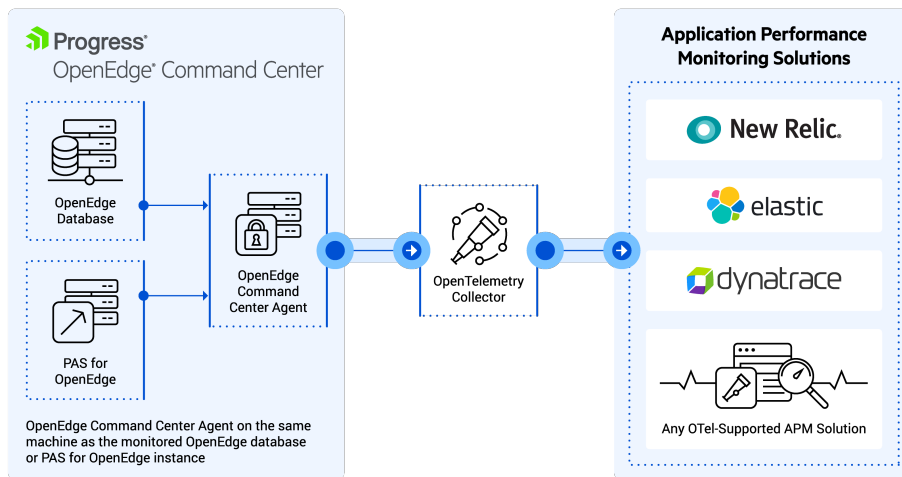
Since OTel is a vendor-agnostic and open-source technology, you can use any market-leading Application Performance Monitoring (APM) vendor solutions, such as Elastic APM, Dynatrace, NewRelic, and so on, to view the performance metrics.

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.

OpenTelemetry metrics for OpenEdge database

The OpenEdge Command Center agent can monitor an OpenEdge database and collect the following performance metrics:

Metrics	Description
Commits	The number of transactions all users have committed.
Undos	The number of transactions rolled back.
Record Updates	The number of records updated.
Record Reads	The number of records read.
Record Creates	The number of records created.
Record Deletes	The number of records deleted.
DB Writes	The number of database blocks written to disk.
DB Reads	The number of database blocks read.
BI Writes	The number of Before-Image (BI) blocks written to disk.
BI Reads	The number of BI blocks read.
AI Writes	The number of After-Image (AI) blocks written to disk.
Record Waits	The number of times users have waited to access a locked record.
Checkpoints	The number of checkpoints that have been performed.
Bufs Flushed	The number of database buffers that have been flushed to disk because they were not written by the time the checkpoint ended.
Rec Lock Waits	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.
BI Buf Waits	The percentage of BI buffer waits, which occur when the database engine must wait to access a BI buffer.
AI Buf Waits	The percentage of AI buffer waits, which occur when the database engine must wait to access an AI buffer.
Writes by APW	The percentage of database blocks written to disk by the Asynchronous Page Writer (APW).
Writes by BIW	The percentage of BI blocks written to disk by the Before-Image Writer (BIW).

Metrics	Description
Writes by AIW	The percentage of AI blocks written to disk by the After-Image Writer (AIW).
Buffer Hits	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	The percentage of buffer hits for the primary buffer pool.
Alternate Hits	The percentage of buffer hits for the alternate buffer pool.

OpenTelemetry metrics for PAS for OpenEdge

The OpenEdge Command Center agent can monitor a PAS for OpenEdge instance and collect the following performance metrics:

Metrics Type	Metrics	Description
REST transport	expressionErrors	The number of expression errors.
	failedRequests	The number of failed requests.
	successfulRunRequests	The number of requests for which response was received successfully.
	successfulRequests	The number of requests successfully sent to the PAS for OpenEdge server.
	connectRequests	The number of connection requests.
	statusRequests	The number of status type requests.
	Requests	The total number of requests.
	successfulConnectRequests	The number of successful connection requests.
	serviceUnavailableRequests	The number of requests for which services were not available.
	runRequests	The number of run requests.
SOAP transport	urlNotFoundErrors	The number of errors because of incorrectly supplied URLs.
	activeRequests	The number of requests that are in the ACTIVE state.
	wSDLRequests	The number of WSDL requests.
	successfulSoapRequests	The number of successful SOAP requests to the PAS for OpenEdge instance.
	soapRequests	The total number of SOAP requests.
	methodNotAllowederrors	The number of errors caused because the requested method is not authorized.
	httpRequestErrors	The number of HTTP requests that resulted in errors.
	httpRequests	The total number of HTTP requests.

Metrics Type	Metrics	Description
	soapProcessorErrors	The number of SOAP processor errors.
APSV transport	forbiddenErrors	The number of requests that failed with the 403 error code.
	disconnectErrors	The number of disconnection errors.
	connectErrors	The number of connection errors.
	disconnectRequests	The number of disconnect requests.
	sessionRequests	The number of session requests.
	sessionErrors	The number of session errors.
WEB transport	headRequests	The number of HEAD requests.
	traceRequests	The number of TRACE requests.
	optionsRequests	The number of OPTIONS requests.
	patchRequests	The number of PATCH requests.
	getRequests	The number of GET requests.
	servletRequests	The number of SERVLET requests.
	deleteRequests	The number of DELETE requests.
	putRequests	The number of PUT requests.
	postRequests	The number of POST requests.
	successfulServletRequests	The number of successful SERVLET requests.
	headErrors	The number of HEAD requests that resulted in errors.
	traceErrors	The number of TRACE requests that resulted in errors.

Metrics Type	Metrics	Description
	optionsErrors	The number of OPTIONS requests that resulted in errors.
	patchErrors	The number of PATCH requests that resulted in errors.
	getErrors	The number of GET requests that resulted in errors.
	deleteErrors	The number of DELETE requests that resulted in errors.
	putErrors	The number of PUT requests that resulted in errors.
	postErrors	The number of POST requests that resulted in errors.
	ablRuntimeErrors	The number of ABL runtime errors.
	ablConnectErrors	The number of ABL connections errors.
	failedServletRequests	The number of SERVLET requests that resulted in errors.
Common	AllRequests	The total number of requests to the PAS for OpenEdge instance.
	AllApps	The total number of applications deployed on the PAS for OpenEdge instance.
	AllAgents	The total number of all agents spawned to execute the server requests.
	AvailableAgents	The number of agents with the AVAILABLE status.
	AllAgentSessions	The total number of sessions including all agents of the PAS for OpenEdge server.
	AllClientConnections	The total number of client connections to the PAS for OpenEdge instance.
	AllClientSessions	The total number of client sessions connected to the PAS for OpenEdge instance.
	InitSessions	The number of initial sessions configured for the PAS for OpenEdge instance.
	IdleSessions	The number of sessions with the IDLE state.

Metrics Type	Metrics	Description
	StartingSessions	The number of starting sessions configured for the PAS for OpenEdge instance.
	AvailableSessions	The number of sessions in the AVAILABLE state.
	ReservedSessions	The number of sessions in the RESERVED state.
	StoppedSessions	The number of sessions in the STOPPED state.

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 84.
 - `schedule`—The time interval at which the agent tries to connect to the OTel Collector in case of a connection failure. This property works in conjunction with the `duration` property.
 - `duration`—The unit of time interval at which the agent tries to connect to the OTel Collector in case of a connection failure. The possible values can be seconds, minutes, hours, or days. This property works in conjunction with the `schedule` property.
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 for the database.

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 for the database.

Note: The password can be in cleartext or encoded using the `genpassword` utility, which is a password encryption utility provided with the OpenEdge database. You can use the `oechl` algorithm to encrypt the password.

- `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 (;).
- `dbconnectionretry`—The number of times the OpenEdge Command Center agent tries to connect to the database in case of a connection failure.
- `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://10.248.0.150:4318"
  protocol: "grpc"
  timeout: 10
  connectionretry: 20
  schedule: 30
  duration: "seconds"

oedbInstances:
- dbname: sports
  host: localhost
  port: 2022
  user: ssl
  password: ssl
  metricsregex:
  otherdbconnparams:
  dbconnectionretry: 5
  dbschedule: 30
  dbduration: SECONDS
- dbname: testdb2
  host: localhost
  port: 3111
  user: admin
  password: xxx
  metricsregex:
  otherdbconnparams:
  dbconnectionretry: 5
  dbschedule: 30
  dbduration: SECONDS
```

After updating the `otagentoedb.yaml` file, restart the OpenEdge Command Center agent.

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 84.
 - `schedule`—The time interval at which the agent tries to connect to the OTel Collector in case of a connection failure. This property works in conjunction with the `duration` property.
 - `duration`—The unit of time interval at which the agent tries to connect to the OTel Collector in case of a connection failure. The possible values can be seconds, minutes, hours, or days. This property works in conjunction with the `schedule` property.

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 database performance metrics whose names match the pattern you have configured are collected. For example, if you specify the value as `/Component/PASOE/*ablapp*/*webapp*/REST/*`, REST transport performance metrics are collected for ABL applications and web applications where the ABL application name contains `ablapp` and the web application name contains `webapp`. When left blank, the agent captures all the defined metrics.

Note: You can use only the `*` quantifier to create a regular expression.

- `agentname`—The name of the PAS for OpenEdge metrics agent.

Note: You can provide details of multiple PAS for OpenEdge instances on your machine under the `pasInstances` node and collect their metrics data using a single OpenEdge Command Center agent.

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
  schedule: 30
  duration: "seconds"

pasInstances:
  - pasdir: "C:/OpenEdge/WRK/oepas5"
    passchedule: 30
    pasduration: SECONDS
    metricsregex:
    agentname:
  - pasdir: "C:/OpenEdge/WRK/oepas2"
    passchedule: 30
    pasduration: SECONDS
    metricsregex:
    agentname:
```

After updating the `otagentpasoe.yaml` file, restart the OpenEdge Command Center agent.

Set up OpenTelemetry Collector

Before setting up the OTel Collector, you must download OTel Collector for your platform and install it. You can install the OTel Collector on a machine different from the one that has the OpenEdge Command Center agent. You can also configure multiple agents to share performance metrics data to the same OTel Collector.

Download the appropriate version of OTel Collector and install it. The minimum supported version of OTel Collector is 0.31 and the last certified version is 0.54. For more information about installing OTel Collector, see the [OpenTelemetry Collector documentation](#).

Note: To avoid any performance impact on the monitored OpenEdge resource, Progress recommends installing OTel Collector on a machine different from the one that has the OpenEdge resource and the OpenEdge Command Center agent.

Perform the following steps to set up the OTel Collector:

1. Open the `config.yaml` file of the OTel Collector installation directory in an editor. For Windows, the `config.yaml` 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 the OTel Collector can get data from the OpenEdge Command Center agent.
 - `processors`—Provide details about what the OTel Collector does with the received data.
 - `exporters`—Provide details about where the OTel Collector sends data for the Application Performance Monitoring (APM) tools.
2. In the `receivers` node, ensure that the value of the `endpoint` property is the same as specified for the `exporter.endpoint` property in the `otagentoedb.yml` or `otagentpasoe.yml` files.
 3. 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 the 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`.
 4. Edit other properties listed in the `config.yml` file per your requirements. To know more about these properties, see the [OpenTelemetry Collector documentation](#).
 5. 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]
```

After updating the `config.yml` file, start the OTel Collector by completing the following steps:

1. Open a Command window and browse to the OTel Collector installation folder.
2. Start the 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-0.31.0-windows_amd64.exe --config config.yml
```

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 `otagentoedb.yml` file.
- When monitoring a PAS for OpenEdge instance, increase the value of the `paschedule` property in the `otagentpasoe.yml` 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 either the OpenEdge resource or the OpenEdge Command Center agent stops. If the monitored OpenEdge resource stops and then restarts, the collection of metrics data resumes if the OpenEdge Command Center agent is 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 values configured for the `connectionretry`, `schedule`, and `duration` properties in the `otagentoedb.yml` or `otagentpasoe.yml` files. If the connection is restored, the Command Center agent sends the performance data for the interrupted duration to the OTel Collector.

However, if the connection is not restored, the Command Center agent does not send the performance data and stops collecting the data from the OpenEdge resource. You need to restart the OpenEdge Command Center agent to start collecting the performance data again.

Set up the APM tool

You can set up any market-leading Application Performance Monitoring (APM) vendor solutions, such as Elastic APM, Dynatrace, NewRelic, and so on, to view the performance metrics of OpenEdge resources. You need to install the APM solution and configure it to use the data exported by the OTel Collector. Because the procedure to install and configure the APM solutions may differ, refer to the documentation for the respective products to configure them.

A possible APM solution that you can consider is to use the following components:

- Elastic APM
- Elasticsearch
- Kibana

However, before you start setting up the APM solution, make sure that both the OpenEdge Command Center agent and the OTel Collector are running.

Set up Elastic APM server

Elastic APM is a popular APM system that enables you to monitor software services and applications in real-time, by collecting detailed performance information. You can download Elastic APM for your platform from www.elastic.co/downloads/apm.

After installing the APM server, ensure that the installation listens to the endpoint where the OTel Collector exports the metrics data. To make this configuration, review the value of the `host` property in the `apm-server.yml` file, available in the Elastic APM installation. To know more about configuring Elastic APM, see [Elastic Documentation](#).

Set up Elasticsearch

Elasticsearch is a NoSQL database that enables you to store, search, and analyze huge volumes of data quickly and in near real-time. You can download Elasticsearch for your platform from www.elastic.co/downloads/elasticsearch.

After installing Elasticsearch, ensure that the Elasticsearch installation listens to the endpoint where the Elastic APM server exports the metrics data. To make this configuration, review the value of the `http.port` property in the `elasticsearch.yml` file, available in the Elasticsearch installation. To know more about configuring Elasticsearch, see [Elastic Documentation](#).

Set up Kibana

Kibana is a free and open-source front-end application that provides search and data visualization capabilities for data indexed in Elasticsearch. You can create different kinds of charts to analyze performance metrics data. You can download Kibana for your platform from www.elastic.co/downloads/kibana.

Install Kibana on a separate machine and then configure the installation to listen to the Elasticsearch data. To make this configuration, edit the `elasticsearch.hosts` property in the `kibana.yml` file, available in the Kibana installation. To know more about configuring Kibana, see [Elastic Documentation](#).

After configuring Kibana to receive metrics data from Elasticsearch, you can view the performance data in Kibana. You can customize the charts and data to view them based on your requirements.

Add agent labels

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 **Command Center 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 labels

To update OpenEdge Command Center agent labels:

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

You can view agent labels on the **Command Center Agents** page.

Generate new agent keys

You must generate an agent key to complete the configuration of an agent in OpenEdge Command Center. Agent keys can be leveraged for agent communication and registration on OpenEdge Command Center. You can generate agent keys from the OpenEdge Command Center console. Note that you need super administrator or administrator privileges to generate agent keys.

To generate new agent keys:

1. Go to **Agent Keys**.
2. Click **Generate Agent Keys**.

A dialog box with the **Key Name** and the **Generated Key** is displayed.

Note: The generated key is encrypted to ensure security of your OpenEdge environment.

3. Click **Save**.
4. On the **New Agent Key** page, the following information is displayed:

- **Key Name**
- **Generated Key**— The key is hidden by default. Use the **Show** option to view the key.

Note: This is the only time that the agent key can be viewed or downloaded.

You cannot recover the agent key later. However, you can generate a new agent key at any time.

5. Click **Download Key**.
6. A populated `serverInfo.json` file is downloaded that contains the agent key. You can edit this file or copy the agent key and use it in your original `serverInfo.json` file.

After a new key is generated, you can view the following information on the **Agent Keys** menu: **Key Name**, **Agents Count**, and **Created At**.

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 **Command Center 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**
 - **Agent Key Name**
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.

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.

Add 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 88.

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 in 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 a user is created, you can update or edit the user information at any time.

To modify a user:

1. On the dashboard, go to **Users** and select a user.
2. On the **Edit User** page, you can update any of the following fields:
 - **First Name**
 - **Last Name**
 - **Email**
 - **Username**
 - **Description**
 - **Role**
3. Click **Save** to update the user information.

Reset the super administrator password

OpenEdge Command Center provides the `resetsuperadmin` utility for modifying the super administrator password. This utility consumes the settings that exist in the configuration file `firstuser-config.json`, which is located in the `/data/conf` directory. In addition to using this utility to change the password, you can also modify any of the following settings for the super administrator:

- First name
- Last name
- User name
- Email address
- Description

To reset the super administrator password:

1. Open a command window as `root`.
2. Change to the `/data/conf` directory
3. Open the `firstuser-config.json` file in an editor, modify the super administrator password as appropriate, and save your changes.
4. Change to the `utils` subdirectory of the OpenEdge Command Center installation directory.
5. Run the following command:

```
prompt> ./resetsuperadmin
```

Note: When using the `resetsuperadmin` utility:

- If a new user is created, then the role that corresponds to the previous super administrator is automatically changed to `no access`.
 - If an existing user is updated to super administrator, then the role that corresponds to the previous super administrator is automatically changed to `no access`.
-

Set up TLS

Enable TLS to establish a secure network channel for communication between the components of OpenEdge Command Center. You can enable TLS for the following communication channels:

- Communication between the OpenEdge Command Center server and agents.
 - Communication between the OpenEdge Command Center server and the MongoDB configuration database.
-

Note: It is recommended that you configure OpenEdge Command Center in TLS mode for your production environments.

Set up TLS for OpenEdge Command Center server and agent communication

To establish a secure network channel for communication between the OpenEdge Command Center server and an agent, you can enable TLS.

To set up a TLS connection between the OpenEdge Command Center server and an agent:

1. Open a command window and change to the OpenEdge Command Center installation directory.
2. Open the file `conf/server-config.json` in an editor.
3. Make the following changes:
 - For `key`, enter the path of the private key that is used for encryption.
 - For `certificate`, enter the path of the public certificate of the CA that has signed the server's TLS certificate. Also known as the root certificate.
 - Set `isServerSecured` to `true`.
4. Save your changes to `conf/server-config.json`.
5. Start the OpenEdge Command Center server (notice that the console is started on the HTTPS transport).
6. In a command window on the agent host machine, change to the OpenEdge Command Center agent installation directory.
7. Open the `conf/serverInfo.json` file in an editor, set `isServerSecured` to `true`, and save your changes.
8. On the agent host machine, import the OpenEdge Command Center server public certificate into the Java keystore.
9. Start the agent.

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

For information about how to generate a self-signed certificate, see the following Knowledge Base articles:

- <https://knowledgebase.progress.com/articles/Knowledge/000027719>
- <https://knowledgebase.progress.com/articles/Article/P150008>

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/>

OpenEdge Command Center reference

For details, see the following topics:

- [Sign in](#)
- [OpenEdge Command Center](#)
- [OpenEdge Command Center agents](#)
- [Edit OpenEdge Command Center agents](#)
- [OpenEdge Command Center agent keys](#)
- [Application servers](#)
- [Users](#)
- [Email settings](#)

Sign in

Use this page to access OpenEdge Command Center from a web browser.

Table 1: Fields

Name	Description
Username	Name of the user logging in.

Name	Description
Password	Password of the user.
Forgot Password	Option to generate a new password in case of a forgotten password.

OpenEdge Command Center

The OpenEdge Command Center consists of several tabs. Each tab provides access to a list of the relevant actions you can perform.

Table 2: Tabs

Name	Description
Dashboard	
Application Servers	Use this tab to list all PAS for OpenEdge instances that are available on an agent; that is, an OpenEdge machine that is configured on OpenEdge Command Center
ABL Applications and Web Applications	Use this tab to deploy and disable ABL applications.
Command Center Agents	Use this tab to create and manage the agents across all of your OpenEdge deployments, as well as generate agent keys for your agents.
Users	Use this tab to create and manage users and user information, such as name, email, and role for your OpenEdge Command Center instances.
Agent Keys	Use this tab to generate new agent keys, or disable or delete ones that are no longer needed.
Console Settings	Use this tab to manage database settings, update settings, agent settings, general settings, and repository settings
Email Settings	Use this tab to manage email notification and configuration settings.

Progress Application Servers—The Application Servers option lists all the Progress Application Servers available on an agent, that is an OpenEdge machine that is configured on OpenEdge Command Center. You can view the name (instance), labels (if any assigned), status (running or down), host name, install path, version, connection configuration, HTTP/HTTPS configuration, server options, request options, PAS for OpenEdge Java environment settings.

ABL Applications and Web Applications—This tab allows you to deploy and disable ABL applications.

Command Center Agents— You can create and manage the agents across all of your OpenEdge deployments as well as generate agent keys for your agents. Additionally, you can monitor the status of your agents (running or stopped) and manage the labels associated with specific agents.

Users—OpenEdge Command Center administrators can create and manage users and user information, such as name, email, and role for your OpenEdge Command Center instances.

Agent Keys—Use the **Agent Keys** tab to generate new agent key, or disable or delete keys that are no longer needed. After an agent key is created, you can associate it with a specific agent to authorize that agent to be used with the OpenEdge Command Center.

Console Settings—Console Settings refers to the general setting for the OpenEdge Command Center itself. On this tab you can manage database settings, update settings, agent settings, general settings, and repository settings.

Email Settings—You can use the **Email Settings** tab to manage email notification and configuration settings. On this tab you can set the mail server host name, port, and authentication credentials.

OpenEdge Command Center agents

Use this page to display all the OpenEdge Command Center agents that are running in your environment. You can create new agents, as well as manage existing agents and generate security keys for agents from this page.

Table 3: Buttons

Name	Description
Generate Agent Keys	Generate new agent keys.
Actions	Delete agent keys.

Table 4: Attributes

Name	Description
Name	Name assigned to an agent.
Labels	Agent labels, if any assigned.
Host name	Host name of the agent configured.
OS	Agent's operating system information.
OS Version	Version of the agent's operating system.
OS Family	Operating system family that the agent belongs to.
Version	Version of the agent.
Status	Status of the agent: running or inactive.

Edit OpenEdge Command Center agents

Table 5: Fields

Name	Description
Name	Name assigned to an agent.
Agent IP Address	IP address of the agent being updated.
Agent Status	Status of the agent: running or inactive.
Labels	Agent labels, if any.

OpenEdge Command Center agent keys

This page displays all the OpenEdge Command Center agent keys used by agents. You can create new agent keys, as well as manage existing agent keys.

Table 6: Buttons

Name	Description
Generate Agent Keys	Generate new agent keys.
Actions	Delete agent keys.

Table 7: Column Names

Name	Description
Key Name	Name assigned to the key generated.
Agents Count	Number of agents configured using that agent key.
Created At	Date and time information of when the agent key was generated.

Application servers

Application servers

Use this page to display all the PAS for OpenEdge instances that are running in your environment. You can configure and manage existing instances from this page.

Table 8: Attributes

Name	
Name	Name of the PAS for OpenEdge instance.
Label	Application server labels, if any.
Status	Status of the application server: running or inactive.
Host Name	Host name of the application server.
Install Path	Installation directory of the application server.
Version	Version of the application server.

Users

OpenEdge Command Center administrators can create and manage users and user information, such as name, email, and role for your OpenEdge Command Center instances.

Table 9: User information

Name	
First name	The first name of the user. For example: Tom.
Last name	The last name of the user. For example: Hanks.
Username	The first and last name of the user. For example: Tom Hanks.
Role	The role of the user, whether a super administrator or an administrator.
Email	Email address of the user.
Description	Details about the user.
Created at	Date and time when the user was created.
Last Login	Date and time when the user was last active.

Email settings

Email Settings

Use this page to display all PAS for OpenEdge instances that are running in your environment. You can configure and manage existing server instances.

Table 10: Attributes

Name	
SMTP Host Name	Host name of the simple mail transfer protocol.
SMTP Port	Port number of the mail server.
Secure connection	TLS port number.
Allow Only Trusted Certificates	Reject untrusted certificates.
STARTTLS Options	Transport Layer Security (TLS) options.
Enable SMTP Authentication	Authentication using the simple mail transfer protocol.
Mail Server (SMTP) Username	Username registered on the mail server.
Mail Server (SMTP) Password	Password assigned to the username registered on the mail server.
Default Email Sender	Email address of the sender.