Progress®



Use the OpenEdge Command Center

OpenEdge®

Copyright

© 2021 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.

DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Icenium, Inspec, Ipswitch, iMacros, Kendo UI, Kinvey, MessageWay, MOVEit, NativeChat, NativeScript, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), SpeedScript, Stylus Studio, Stylized Design (Arrow/3D Box logo), Styleized 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 Habitat, Chef WorkStation, Corticon.js, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Everywhere, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, JustAssembly, JustDecompile, JustMock, KendoReact, NativeScript Sidekick, 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 Insight, 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. Any other marks contained herein may be trademarks of their respective owners.

July 2021

Updated: 2021/07/16

Table of Contents

Learn about OpenEdge Command Center....7

OpenEdge Command Center console dashboard....9

Install and configure OpenEdge Command Center....13

Launch the OpenEdge Command Center installer....14
Install OpenEdge Command Center in high availability mode....17
Silent installation of OpenEdge Command Center....19
Set up OpenEdge Command Center with MongoDB Atlas on AWS....21
Deploy OpenEdge Command Center on Windows platform using a ZIP package....22
Deploy OpenEdge Command Center on Linux platform using a TAR package....23
Uninstall OpenEdge Command Center....25

Install OpenEdge Command Center Agents....27

Silently install OpenEdge Command Center agents....29
Deploy OpenEdge Command Center agent on Windows platform using a ZIP package....31
Deploy OpenEdge Command Center agent on Unix platform using a TAR package....33
Uninstall OpenEdge Command Center agents....34

How to....35

Log in to OpenEdge Command Center....37
Change or reset passwords....37
Configure new OpenEdge Command Center agents....38
Manage agent services....39
Manage services for OpenEdge Command Center server....40
Change logging level....41
Configure and manage PAS for OpenEdge instances....41
    Configure PAS for OpenEdge instances....42
    Manage PAS for OpenEdge instances....54
Add agent labels....58
Update agent labels....58
Generate new agent keys....59
Search for and filter agents....60
Configure email settings....60
Add a new user....61
Reset the super administrator password....62
Set up TLS....63
    Set up TLS for OpenEdge Command Center server and agent communication....63

Set up TLS for OpenEdge Command Center and MongoDB communication.....64

OpenEdge Command Center reference.....67

Sign in.....67
OpenEdge Command Center 68
OpenEdge Command Center agents.....69
Edit OpenEdge Command Center agents.....70
OpenEdge Command Center agent keys.....70
Application servers.....70
Users.....71
Email settings.....71

1

Learn about OpenEdge Command Center

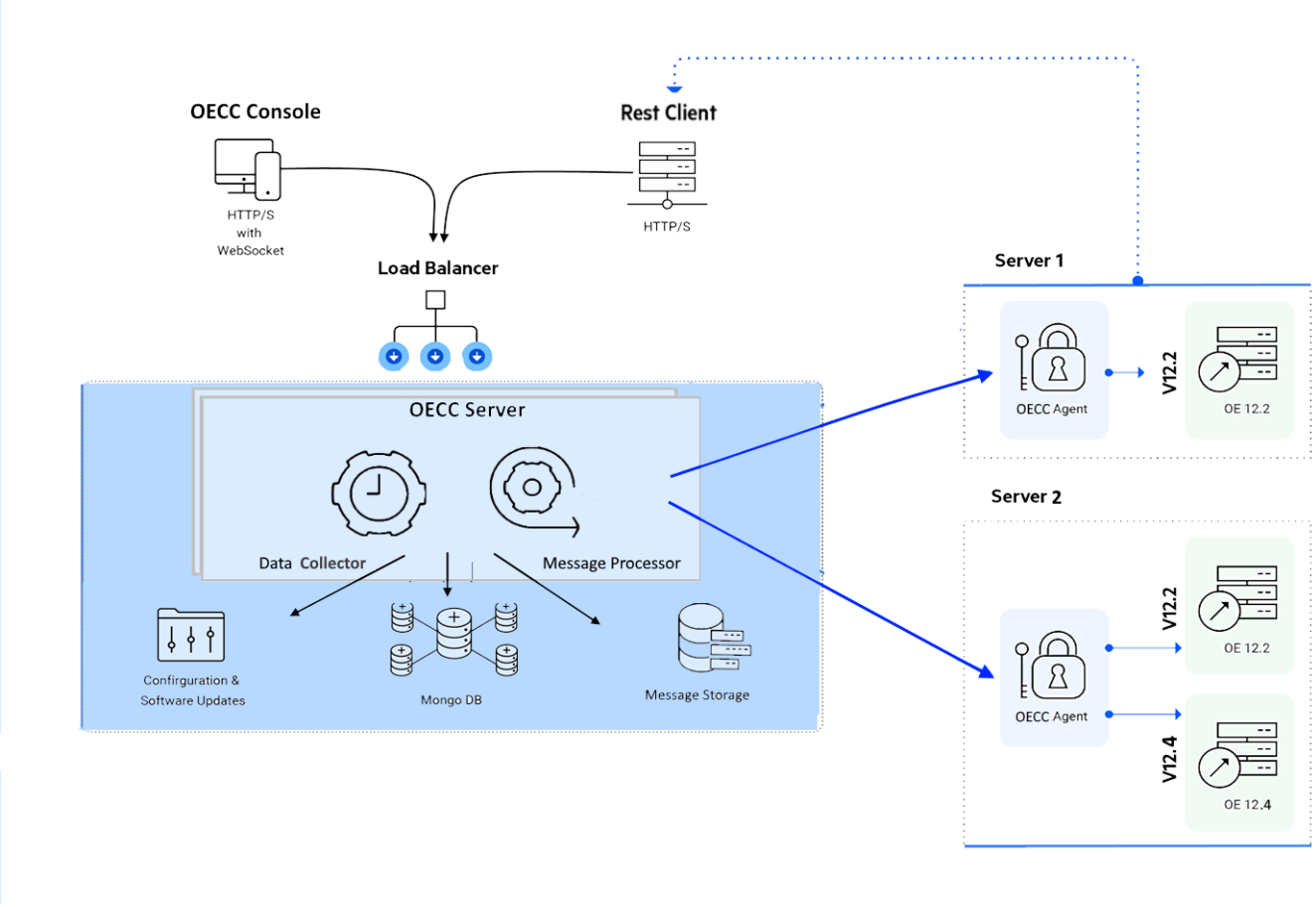
OpenEdge Command Center features the latest UI and UX technologies. In its first release, OpenEdge Command Center is built to effectively manage PAS for OpenEdge instances and, in the future, databases. It aims to incrementally support everything you need to manage instances. It simplifies the administrative 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 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. 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.
	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. For more information about agents, see Configure new OpenEdge Command Center agents on page 38 and Manage agent services on page 39.
	The PAS for OpenEdge instances page, which lists all instances that are available from an agent. You can view the instance details, sich as its name, labels, and status. 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 41.

Click . . .	. . . to display
	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. For more information, see Add a new user on page 61.
	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. For more information, see Generate new agent keys on page 59.
	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.
	Tthe 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. For more information, see Configure email settings on page 60.

2

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

Before you install OpenEdge Command Center, you must download MongoDB and set up it up with basic authentication mode. OpenEdge Command Center supports the following versions and 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 14—Typically used for a complete installation of OpenEdge Command Center server and console components.
- Install OpenEdge Command Center in high availability mode on page 17—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 19—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

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 software download is provided in a bin archive, `PROGRESS_OECC_SERVER_1.0.0_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 programmatically 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:

   ```
   prompt> ./PROGRESS_OECC_SERVER_1.0.0_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:
   1. Enter the installation directory path, for example:`/usr/openedge_command_center`
   2. 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.
   3. Enter the Data Directory path and click **Next**.

      Example: `/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 17.

9. On the **Database Configurations** page:
   1. Enter the **Hostname/IP Address** information.
   2. 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**.

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

- Database authentication

Note: 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 database 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/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. Then when you specify a data directory on the **Install Configurations** page, you 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 installer file `PROGRESS_OECC_SERVER_1.0.0_LNX_64.bin` that was used for the prior OpenEdge Command Center installation.

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. For example:

   ```
   prompt> ./PROGRESS_OECC_SERVER_1.0.0_LNX_64.bin
   ```

   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, for example: `/usr/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 `PROGRESS_OECC_SERVER_1.0.0_LNX_64.bin` file.
2. Enter the following command to record installation choices in the `response.properties` file:

   ```
   PROGRESS_OECC_SERVER_1.0.0_LNX_64.bin -r /response.properties-file
   ```

3. Run the `PROGRESS_OECC_SERVER_1.0.0_LNX_64.bin` file by performing the steps in Launch the OpenEdge Command Center installer on page 14.

   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:

   ```
   ./PROGRESS_OECC_SERVER_1.0.0_LNX_64.bin -i silent -f /response.properties-file
   ```

   After you enter the preceding 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 14, 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 locationl 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_1.0.0_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_1.0.0_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 `orig` folder	New location and file name
`db-config.json.orig`	`<Server data folder>\conf\db-config.json` For example, `C:\OECC_DATA\data\conf\db-config.json`
`firstuser-config.json.orig`	`<Server data folder>\conf\firstuser-config.json` For example, `C:\OECC_DATA\data\conf\firstuser-config.json`
`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`.

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_1.0.0_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_1.0.0_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 `orig` folder	New location and file name
`db-config.json.orig`	`<Server data folder>/conf/db-config.json` For example, `/usr/OECC_DATA/data/conf/db-config.json`
`firstuser-config.json.orig`	`<Server data folder>/conf/firstuser-config.json` For example, `/usr/OECC_DATA/data/conf/firstuser-config.json`
`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`.
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.

3

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_1.0.0_WIN_64.exe` `PROGRESS_OECC_AGENT_1.0.0_WIN_64.zip`
Linux	`PROGRESS_OECC_AGENT_1.0.0_LNX_64.bin` `PROGRESS_OECC_AGENT_1.0.0_LNX_64.tar.gz`
AIX	`PROGRESS_OECC_AGENT_1.0.0_AIX_64.bin`
Solaris	`PROGRESS_OECC_AGENT_1.0.0_SOL_64.bin`

2. Run the installer file. For example:

   ```
   ./PROGRESS_OECC_AGENT_1.0.0_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

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: • 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: • 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_1.0.0_*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_1.0.0_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_1.0.0_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 `orig` folder	File name in the `conf` folder
`installationsInfo.json.orig`	`installationsInfo.json`
`java.properties.orig`	`java.properties`
`serverInfo.json.orig`	`serverInfo.json`

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
    ```

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

You can use installation package, `PROGRESS_OECC_AGENT_1.0.0_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_1.0.0_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 `orig` folder	File name in the `conf` folder
`installationsInfo.json.orig`	`installationsInfo.json`
`java.properties.orig`	`java.properties`
`serverInfo.json.orig`	`serverInfo.json`

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
    ```

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**.

4

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 37
Set your password	Change or reset passwords on page 37
Work with agents	• Configure new OpenEdge Command Center agents on page 38 • Manage agent services on page 39 • Add agent labels on page 58 • Generate new agent keys on page 59 • Search for and filter agents on page 60
Configure PAS for OpenEdge	• Create a PAS for OpenEdge instance on page 54 • Modify PAS for OpenEdge configuration properties on page 42 • #unique_30 • #unique_31

For information how to . . .	. . . see
Manage PAS for OpenEdge	• Start or stop a PAS for OpenEdge instance on page 56 • Delete a PAS for OpenEdge instance on page 57 • Obtain process details on page 57
Set up email	Configure email settings on page 60
Add users	Add a new user on page 61

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
- 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 OpeEdge 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 OpenEge 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.

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

Using the OpenEdge Command Center console, you can perform the following operations to configure PAS for OpenEdge instances:

- Modify PAS for OpenEdge configuration properties on page 42

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 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.
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 `tomcat-certstore.jks` 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 `tomcat-certstore.jks` that holds the root or intermediate CA certificates. These certificates are used to validate the clients using TLS client authentication.

Property	Default value	Description
Encryption Protocol	`TLSv1.2`	Specifies the HTTPS protocol selected for secure communication. If required, you can also edit this value in the `catalina.properties` 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-separted 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.

5. 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.
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`	Specifies the character encoding used to decode the URI bytes after decoding the URL. **Note:** This value is set to the default value of the Tomcat server, and it affects both the HTTP and HTTPS connectors.

Property	Default value	Description
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	—	Specifies the port number to shutdown the server that is running. The values can range from `1024` to `65535`. To disable the shutdown port, set the value to `-1`. You must specify a value in Windows, but this property is optional in UNIX.
Shutdown Password	`SHUTDOWN`	Specifies a private shutdown port access code to prevent one server instance from being shutdown by anyone. **Note:** If the shutdown port is specified, you must change this value to avoid insecure configuration.
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.
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.

Property	Default value	Description
Web Application Directory	`webapps`	Specifies the location of the directory where the web applications are to be deployed. If not specified, then the default directory of the Tomcat server, `webapps` is used. 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.
Common Library Path	—	Specifies a comma-delimited list of library paths. For example, `local/server/common/*jar,local/server/common/x.jar`. The delimiter is platform dependent, and the format of the path must conform to the common library path format of the Tomcat server (`https://tomcat.apache.org/tomcat-9.0-doc/class-loader-howto.html`).
Auto Deploy WAR Files	`false`	Select the checkbox to enable the security settings used by the Tomcat server for deploying web applications. The default value depends on whether the PAS instance is created as a development or a production security configuration. In a production configuration, the default is `false`. In a development configuration, the default is `true`.
Unpack WAR Files	`true`	Select the checkbox to allow unpacking of web archive (`.war`) 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 Tomcat server is started.
Log Command Line Arguments	`true`	Select the checkbox to log the command line arguments passed to Java when the Tomcat server is started.
Log Environment Variables	`false`	Select the checkbox to log the current environment variables when the Tomcat server is started.
Log Java System Properties	`false`	Select the checkbox to log the current Java system properties when the 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 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.

Property	Recommended setting	Description
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 `allowRuntimeUpdate` is set to `true`, 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 `allowRuntimeUpdate` is set to `true`, 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.

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.

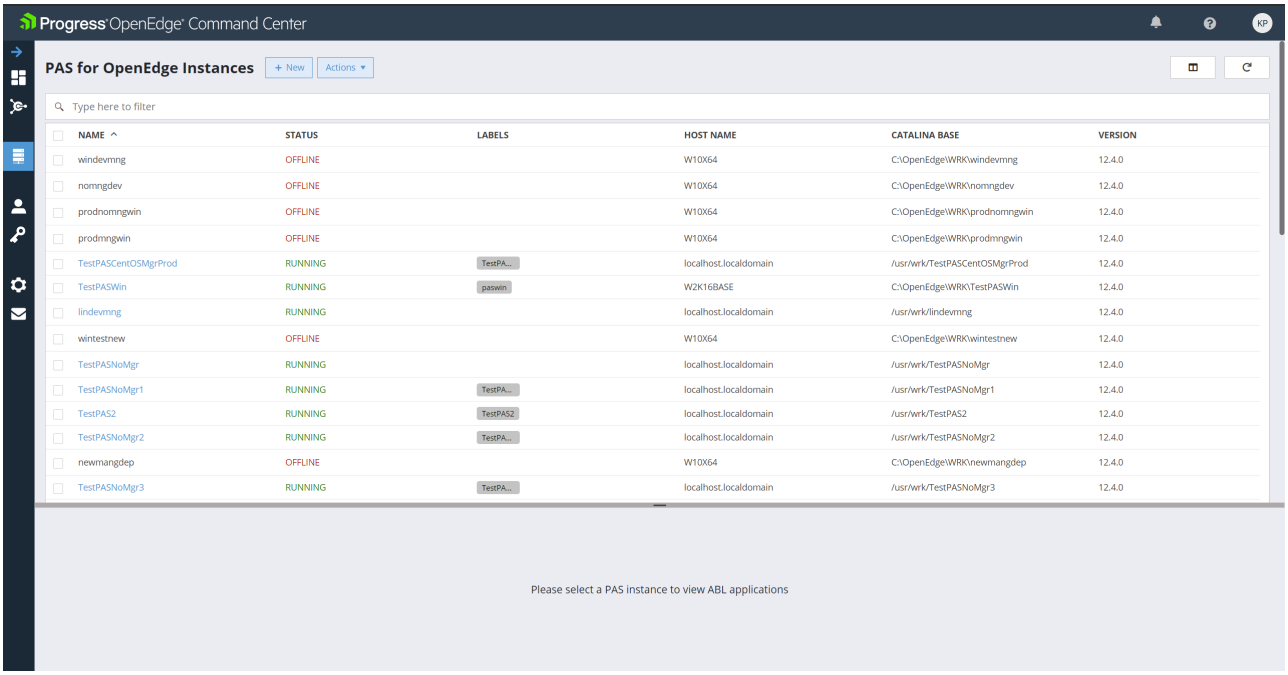
Access your ABL applications or ABL web applications

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.

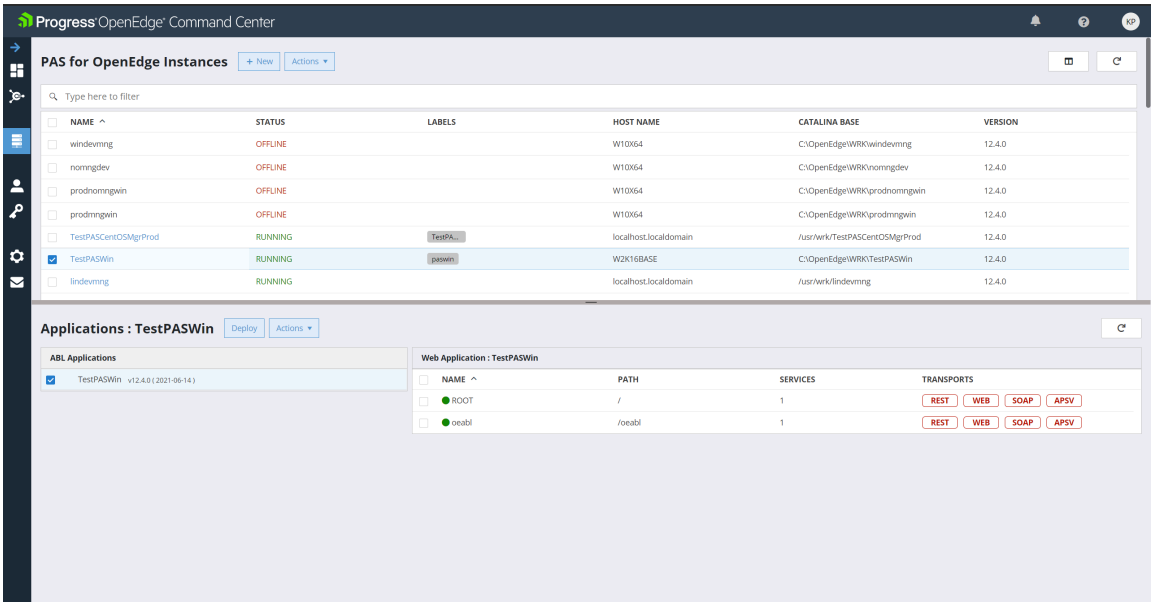


2. Click the check-box next to the instance that hosts the ABL application or web application.

   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.



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 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.

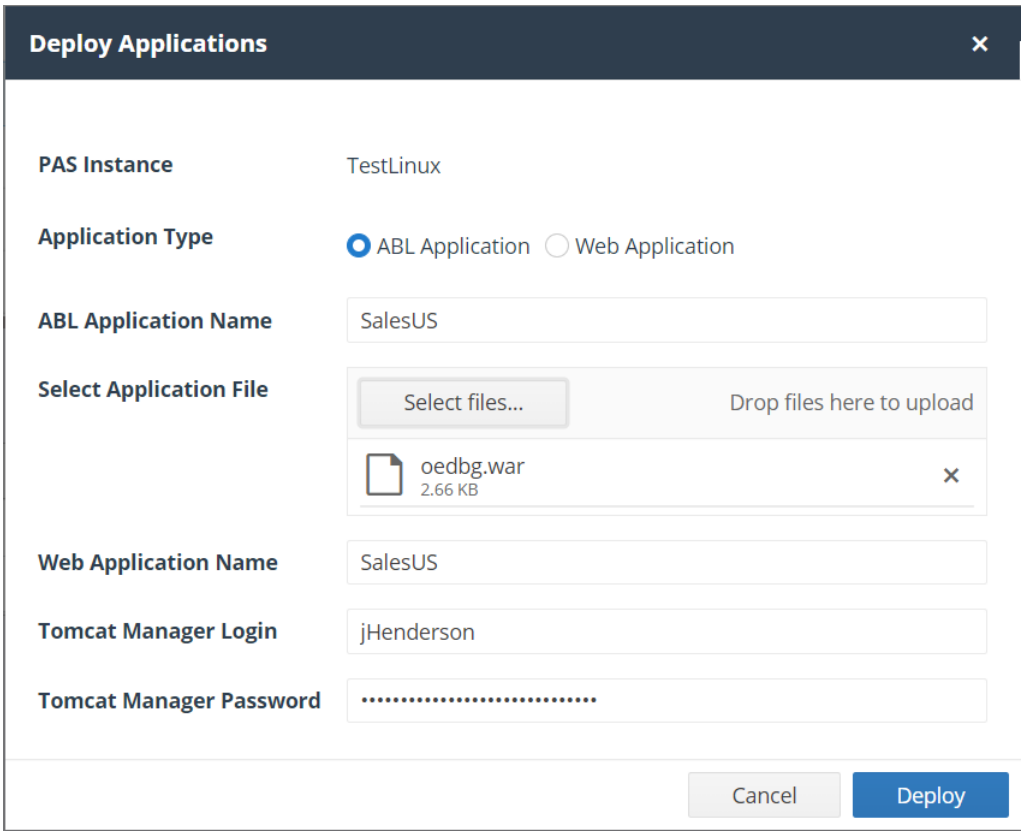
   At this point in the procedure you can choose to either deploy a new ABL application or a web application that is associated with an existing ABL application.

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 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.

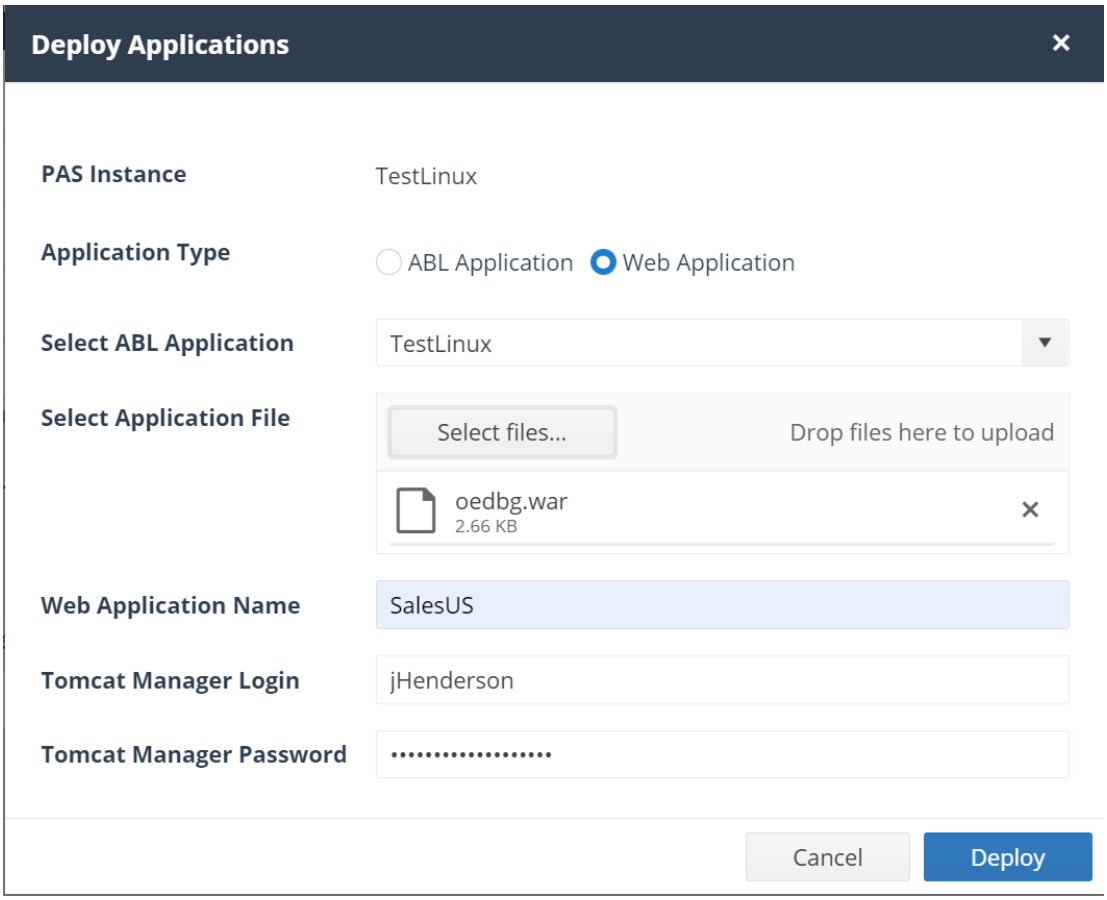


5. To deploy a web application:
   a. In the **Deploy Applications** dialog box choose **Web Application** as the Application Type.
   b. In the **Select ABL Application** field, select an ABL application from the drop down list.
   c. In the **Select application file** field, click **Select File** and 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 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.



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:

   a. **Undeploy ABL Applications** to undeploy the ABL application and any web application associated with it.

   b. **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 Tomcat manager log in credentials to confirm the undepoly 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

Using the OpenEdge Command Center, you can perform the following operations to manage PAS for OpenEdge instances:

- Create a PAS for OpenEdge instance on page 54
- Start or stop a PAS for OpenEdge instance on page 56
- Obtain process details on page 57

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.

In the following field . . .	. . . do the following
Labels	Use the drop-down box to select one or more labels, or create one or more new labels to assign.
Security Model	Specify one of the following security models: • **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	Specify the path of the PAS for OpenEdge instance. **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).
HTTP Port	Specify an unused port number to be associated with the PAS for OpenEdge instance HTTP port. By default, this is set to 8080. **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.

In the following field . . .	. . . do the following
HTTPS Port	Specify an unused port number associated with the PAS for OpenEdge instance HTTPS port. By default, this is set to 8443. **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.
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.
Tomcat Manager login	Enter the login ID of the Tomcat Manager web application that hosts the PAS for OpenEdge instance. If you are using the Tomcat Web server shipped with OpenEdge, then the default login ID is `tomcat`.
Tomcat Manager password	Enter the password of the Tomcat Manager web application that hosts the PAS for OpenEdge instance. If you are using the Tomcat Web server shipped with OpenEdge, then the default password is `tomcat`.

3. 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.
4. To enable online deployment of ABL applications for your PAS for OpenEdge instance, select the '**Deploy Manager application to enable online deployment**' option. If you select the option for a developer instance of PAS for OpenEdge, all web applications, such as `manager` and `oemanager`, are deployed. If you select the option for a production instance of PAS for OpenEdge, only the Manager web application is deployed. OpenEdge Command Center uses the Manager application to load the application deployment status in PAS for OpenEdge.
5. Click **Create PAS Instance**.

Start or stop a PAS for OpenEdge instance

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

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

1. In the OpenEdge Command Center console, click **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 start or stop.

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

3. From the **Actions** menu, select **Start** or **Stop**, as appropriate.

   A notification popup is displayed that shows the start or stop operation in progress.

4. Click the **Refresh** button to view the change in status of the corresponding PAS for OpenEdge instance.

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

Delete a PAS for OpenEdge instance

To delete one or more PAS for OpenEdge instances:

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

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 adiministrator or administrator priviliges 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 60.

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 adminstrator 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
`mode`	Set value to `requireTLS` or `preferTLS`.
`certificateKeyFile`	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
`mode`	Set value to `requireTLS` or `preferTLS`.
`certificateKeyFile`	Path of the public certificate of the MongoDB server that is signed by the CA.
`CAFile`	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
`sslCA`	Path of the public certificate of the CA that is used to validate the certificates presented by the MongoDB server.
`sslKey`	The private key used for encryption.
`sslCert`	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/

5

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 confiure 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.