

Copyright (c) 2022, Oracle. All rights reserved. Oracle Confidential.

## Provision a New Oracle E-Business Suite Installation on a Single Node on Oracle Cloud Infrastructure (Doc ID 2764690.1)

---

This knowledge document describes how to use an image hosted in Oracle Cloud Infrastructure (OCI) to provision an Oracle E-Business Suite Release 12.2.11 with Oracle Database 19c demonstration instance on a single virtual machine (VM) on OCI.

The most current version of this document can be obtained in My Oracle Support Knowledge [Document 2764690.1](#).

There is a [change log](#) at the end of this document.

### In This Document

This document is divided into the following sections:

- [Section 1: Before You Begin](#)
- [Section 2: Create Instance Using an Image from the OCI Console Marketplace](#)
- [Section 3: Perform Post-Install Steps](#)
- [Section 4: Take Steps to Further Secure Your Instance](#)
- [Section 5: References](#)

## Section 1: Before You Begin

---

In this 30-minute tutorial, you will use an image hosted in Oracle Cloud Infrastructure (OCI) to provision an Oracle E-Business Suite Release 12.2.11 with Oracle Database 19c instance on a single virtual machine (VM) on OCI.

You can provision a Demo Install Image containing demonstration data. This instance is suitable for conducting demonstrations and exploring new features.

### 1.1 Background

Create an Oracle Cloud Infrastructure Compute instance (virtual machine) containing the Release 12.2.11 database and application tiers from **Oracle E-Business Suite 12.2.11 Demo Install Image**. Use this single-node Vision demonstration instance to evaluate and test standard Oracle E-Business Suite functionality, and demonstrate the standard business flows delivered with the applications. Also use it to become familiar with the technology components of Oracle E-Business Suite Release 12.2 and train your users.

The image can be found in the OCI Console Marketplace and also in the OCI Oracle Images list in your tenancy. Instructions for the OCI Console Marketplace are provided in this document.

The instance you create will have the following embedded technology components:

- Operating System

Component	Version
Oracle Linux 7.9	7.9 64-bit

- Technology Component Versions

Component	Version
RDBMS Oracle Home	Oracle Database 1

Component	Version
Application Code Level	<ul style="list-style-type: none"> <li>○ Oracle E-Business Suite 12.2.11 Release Update Pack (<a href="#">Document 2758</a>)</li> <li>○ R12.AD.C.Delta.13 and R12.TXK.C.Delta.13 (<a href="#">Document 1617461.1</a>)</li> <li>○ Technology consolidated patches for database and middle tier techstack</li> <li>○ Oracle E-Business Suite Person Data Removal Tool (PDRT) patches (<a href="#">Document 2758</a>)</li> </ul>
Oracle Forms and Reports	10.1.2
Oracle WebLogic Server	10.3.6.0.2
Web Tier	11.1.1
JDK	1.7.0_75
Java Client	Java Web Start is enabled by default on your instance. Refer to My Oracle Support Knowledge <a href="#">Document 2517025.1</a> , <i>Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure</i> , for information about the use of Java Web Start.
Critical Patch Update (CPU)	<i>Oracle E-Business Suite Release 12.2 Critical Patch Update Av</i>

**Note:** Alternatively, you can use the Oracle E-Business Suite Cloud Manager to provision Oracle E-Business Suite in Oracle Cloud, migrate Oracle E-Business Suite environments from on-premises to Oracle Cloud, and conduct subsequent lifecycle management of these cloud environments. See My Oracle Support Knowledge [Document 2517025.1](#), *Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure*, to understand the complete range of options.

## 1.2 What Do You Need?

- An understanding of the relevant information in My Oracle Support Knowledge [Document 2517025.1](#), *Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure*.
- An SSH Key Pair which will be used for accessing your instance. See [Generating an SSH Key Pair for Oracle Compute Cloud Service Instances](#).
- An Oracle Cloud Infrastructure (OCI) tenancy, with the following associated resources:
  - A compartment
  - A user who is either a tenancy administrator, or who has privileges to manage all resources in the compartment
  - A Virtual Cloud Network (VCN) and an associated subnet which will be associated with the Oracle E-Business Suite instance

## Section 2: Create Instance Using an Image from the OCI Console Marketplace

Follow these steps to create and connect to your Oracle E-Business Suite instance when using an image from the OCI Console Marketplace.

1. Log in to the OCI Service Console.
2. Select Menu, then Compute on the left hand panel under the heading Core Infrastructure, and then select the compartment where you will create your new instance.

Note: This step is necessary to work around a known issue.

3. Select Menu again, then Marketplace under the heading Solutions and Platforms; then Filter by Type **Image**, Publisher **Oracle**, and Category **Packaged Application**.
4. Click on **Oracle E-Business Suite 12.2.11 Demo Install Image**, and on the resulting screen, do the following:
  - If there are multiple packages, select the latest package version from the dropdown list unless you require an earlier version. Note that the latest version contains Oracle Database 19c.

- Select the compartment or subcompartment where you wish to install Oracle E-Business Suite.
  - Review and accept the Oracle Standard Terms and Restrictions.
  - Click **Launch Instance**.
5. In the Create Compute Instance screen, specify the following:
- Under **Name**, enter your choice of name. For example, `ebs12211-demo`.
  - Under **Create in compartment**, verify your choice of compartment or select another.
  - In the **Placement** region, select from the **Availability domains** shown.
  - In the **Image and Shape** region:
    - Under **Image**, you will see the name of the OCI Console Marketplace image you chose in Step 1.
    - Under **Shape**, you will see a default shape. If you want to specify another shape, click on **Change Shape**.
  - In the **Networking** region:
    - Under **Network**, select an existing virtual cloud network, for example, `my-vcn`.
    - Under **Subnet**, select an existing subnet, for example, `my-subnet`.
- Note:** If the VM is associated with a public subnet and you want to assign a public IP address, then select the **Assign a public IPV4 address** option.
- In the **Add SSH keys** region, select **Choose public key files** to specify the file containing your SSH public key generated previously.
  - In the **Boot volume** region, make no changes to accept the default volume size.
  - Click **Create** to create your Compute Instance.
6. Establish SSH Connectivity.

Review the security lists associated with the subnet to ensure that an ingress rule exists with the following attributes:

- SOURCE TYPE: CIDR
- SOURCE CIDR: Enter the CIDR block of your choice. Note that 0.0.0.0/0 corresponds to the public internet. We recommend restricting this to the CIDR block that corresponds to the IP range you want to give access to.
- IP PROTOCOL: SSH (TCP/22)
- DESTINATION PORT: 22

When the instance is fully provisioned and running, connect to it using SSH as described in [Connecting to an Instance](#).

7. After the instance has been created (provisioned), it will appear in the instance list. To view full details about it, including IP addresses, click the instance name in the list.

## Section 3: Perform Post-Install Steps

After you provision your environment, you must perform the tasks below to configure access and secure the environment.

In addition, the steps in [Section 4: Secure Your Instance](#) should be followed to ensure that environment is secure.

In order to perform the tasks in this section, you must first connect as the `opc` user using `ssh` to the Oracle Cloud Infrastructure instance that hosts your Oracle E-Business Suite environment.

### 3.1 Update Operating System

Switch from the `opc` user to the root user, and then perform an operating system update using the following commands:

```
$ sudo su -  
# yum update  
Is this ok [y/d/N]: y
```

### 3.2 Enable Instance-Level Firewall Access to Port 8000

In order to access the applications, you must enable firewall access to port 8000 on your instance.

While still logged on as the root user, use the following commands to enable port 8000:

```
# firewall-cmd --add-port=8000/tcp --permanent
# systemctl restart firewalld
```

To confirm the change, use the following command:

```
# firewall-cmd --list-all
```

### 3.3 Update Hostname

Your hostname must be updated to reflect the current VCN network configuration. While still logged on as the root user, perform a required hostname update using the following command:

```
# /u01/install/scripts/updatehosts.sh
```

### 3.4 Enable and Change SYSADMIN Password

To ensure your environment is adequately protected, you must change your Oracle E-Business Suite account passwords.

- a. While still logged on to the Oracle Cloud Infrastructure instance that hosts your Oracle E-Business Suite environment, switch from the `opc` user to the `oracle` user using the following command:

```
$ sudo -i -u oracle
```

- b. Start the database:

```
$ /u01/install/APPS/scripts/startdb.sh
```

- c. Start the application tier processes:

```
$ /u01/install/APPS/scripts/startapps.sh
```

- d. Set the environment:

```
$ . /u01/install/APPS/EBSapps.env run
```

- e. To log in through the web interface, you must initially set a password of your choice for the `SYSADMIN` user. After the `SYSADMIN` user is active with the new password, you can create new users or activate existing locked users. To enable the `SYSADMIN` user, run the following commands:

```
$ mkdir -p ~/logs
$ cd ~/logs
$ sh /u01/install/APPS/scripts/enableSYSADMIN.sh
```

When prompted, enter a new password for the `SYSADMIN` user.

The `SYSADMIN` user can now connect to Oracle E-Business Suite through the web interface and create new users or activate existing locked users.

### 3.5 Enable Vision Demo Users and Set User Passwords

For a Vision demo environment, you can run another script to unlock a set of 36 application users that are typically used when demonstrating Oracle E-Business using the Vision database. Run this script with the same environment as when running the `enableSYSADMIN.sh` script. To enable the demo users, run the following commands:

```
$ cd ~/logs
$ /u01/install/APPS/scripts/enableDEMOusers.sh
```

When prompted, enter a new password.

Do not run this script on a fresh or production environment.

### 3.6 Enable HTTP Access

From the OCI console, add a security rule to the security list.

- a. Navigate to Networking, then Virtual Cloud Networks.
- b. Select the VCN associated with your instance, such as **my-vcn**.
- c. Identify the subnet associated with your instance, and click on the link for the security list.
- d. Click **Edit All Rules**.
- e. Add an Ingress Rule with the following attributes:
  - o SOURCE TYPE: CIDR
  - o SOURCE CIDR: Enter the CIDR block of your choice. Note that 0.0.0.0/0 corresponds to the public internet. We recommend restricting this to the CIDR block that corresponds to the IP range you want to give access to.
  - o IP PROTOCOL: TCP
  - o DESTINATION PORT: 8000

### 3.7 Configure Web Entry Point (Optional)

As the `oracle` user, use the `configwebentry.sh` script provided in the `/u01/install/scripts` directory to change the webentry point, which is by default set to the physical hostname of the virtual machine. For instance, you could follow the steps in this example to set the webentry point to `myapps.example.com` and access the application using

`http://myapps.example.com:8000/OA_HTML/AppsLogin:`

```
$ /u01/install/scripts/configwebentry.sh
Enter the Web Entry Protocol (Eg: https/http): http
Enter the Web Entry Host Name (Eg: public): myapps
Enter the Web Entry Domain Name (Eg: example.com): example.com
Enter the Web Entry Port (Eg: 443/80): 8000
Enter the ORACLE_SID (Eg: EBSDB): ebsdb

Running AutoConfig to complete the configuration

Enter the APPS user password: apps_password
```

### 3.8 Update Local Hosts File on Your Client Machine (Conditional)

**Note:** If you register your web entry host name and domain from Step 3.6 in your DNS system, you do not need to perform this step.

While logged on to the Compute instance that hosts your Oracle E-Business Suite environment, run the following command to verify your hostname:

```
$ hostname -f
```

Substitute the value that is returned for `hostname` in the instructions below.

- Update the Local Hosts File on Windows:
  - o Find the hosts file you want to modify.
  - o Open the file explorer to open the following directory: `C:\\Windows\\System32\\drivers\\etc`
  - o As you CANNOT edit in this folder, perform the following:
    - Copy this hosts file to your desktop.
    - Edit the hosts file with a text editor.
    - Add one line with the IP address and host name: `<external-IP-address> <hostname>`
  - o Once added, save the file as the hosts file without any extension.
  - o Then, you can copy it back to the original folder.

- Confirm the replacement as an administrator.
- Update the Local Hosts File on Mac:
  - On your Mac, open the Terminal application.
  - Change to the folder where you will find the hosts file.

```
$ cd /etc
```

- Use the following vi command to edit the file:

```
$ sudo vi hosts
```

- Add your host name and save the file.

```
<external-IP-address> <hostname>
```

### 3.9 Log in to Applications

- a. As the Oracle user, start the application tier services. (Conditionally Required)

You need to perform this step only if you have changed the web entry point.

```
# sudo su - oracle
$ /u01/install/APPS/scripts/stopapps.sh
$ /u01/install/APPS/scripts/startapps.sh
```

- b. You can now access the applications using `http://<hostname>:8000/OA_HTML/AppsLogin`

For instance, if your host name is `myapps.example.com`, your login will be:

```
http://myapps.example.com:8000/OA_HTML/AppsLogin
```

### 3.10 Enable Oracle E-Business Suite Integrated SOA Gateway for REST Services (Optional)

Enable Oracle E-Business Suite Integrated SOA Gateway (ISG) for REST services by using the following commands:

```
$ cd ~/log
$ /u01/install/APPS/scripts/enableISG.sh
```

At the start of the script execution, when prompted, enter the APPS Schema password and the WebLogic password.

**Note:** The required setup tasks for enabling Oracle E-Business Suite REST services provided through Oracle E-Business Suite Integrated SOA Gateway are already preconfigured in this instance. This means that Oracle E-Business Suite integration interface definitions published in Oracle Integration Repository, a component in Oracle E-Business Suite Integrated SOA Gateway, are available for REST service deployment.

Interface types enabled for REST services are PL/SQL APIs, Java Bean Services, Application Module Services, Concurrent Programs, Business Service Objects, and Open Interface Tables and Views.

For more information on deploying and configuring Oracle E-Business Suite REST services, see:

- Installing Oracle E-Business Suite Integrated SOA Gateway, Release 12.2, My Oracle Support Knowledge [Document 1311068.1](#).
- [Administering REST Web Services](#), *Oracle E-Business Suite Integrated SOA Gateway Implementation Guide*

For more information on supported interfaces for REST services and on REST service invocations, see:

- [Oracle E-Business Suite Integrated SOA Gateway User's Guide](#)
- [Oracle E-Business Suite Integrated SOA Gateway Developer's Guide](#)

### 3.11 Configure Enterprise Command Center Dashboards (Optional)

Oracle Enterprise Command Center Framework V7 is installed in this instance. To learn more about Enterprise Command Centers and available discovery dashboards, refer to [Oracle E-Business Suite Enterprise Command Centers \(ECC\) - Quick Start Guide](#).

To use Enterprise Command Centers in this environment, perform the following configuration steps.

- Update the source system URL.
  - Log in to your Oracle E-Business Suite environment as the `sysadmin` user, and select the ECC Developer responsibility.
  - Select Source System in the navigation pane of the Oracle Enterprise Command Center Framework administration UI.
  - In the Source System Definition page, enter your Oracle E-Business Suite login URL in the Source System URL field. The login URL for this instance was derived in Step 8.
- Initially, the Oracle Enterprise Command Center Framework installation includes data only for the Oracle Assets Command Center (FA). Before you can access an Enterprise Command Center dashboard for any other products, you must perform a full load of the product-specific data into the Oracle Enterprise Command Center Framework installation.
  - Run the data load concurrent program for your product as listed in Loading Product Data to Enterprise Command Centers, My Oracle Support Knowledge [Document 2495053.1](#), *Installing Oracle Enterprise Command Center Framework, Release 12.2*. For more details about each data load program, see your product-specific Enterprise Command Center documentation.

## Section 4: Take Steps to Further Secure Your Instance

Taking these additional steps will ensure that your Oracle E-Business Suite instance in Oracle Cloud Infrastructure is secure.

### 4.1 Change Database Passwords for Base Product Schemas

While logged on to your instance, switch from the `opc` user to the `oracle` user using the following command:

```
$ sudo su - oracle
```

Then change the database passwords for the base product schemas:

```
$ sh /u01/install/APPS/scripts/changeDBpasswords.sh
```

When the script prompts you to provide the password for the SYSTEM user, enter 'manager'.

**Note:** Once you have completed the setup tasks described in this document, you can change the passwords for APPLSYSPUB, APPLSYS, APPS, and APPS\_NE schemas. See Appendix B, Database Schemas Found in Oracle E-Business Suite, [Oracle E-Business Suite Security Guide](#) for details.

### 4.2 Add IP Restriction to Database TNS Listener

Add the IP restriction to the database TNS listener using the following command after setting the environment for database ORACLE\_HOME:

```
$ . /u01/install/APPS/19.0.0/ebscdb_apps.env
```

```
$ cd $TNS_ADMIN/EBSDB_apps
$ cat > sqlnet_ifile.ora <<EOF
tcp.validnode_checking = YES
tcp.invited_nodes = ( apps.example.com )
EOF
$ lsnrctl stop EBSCDB
```

```
$ lsnrctl start EBSCDB
```

Now the database listener will only accept connection requests from this host `apps.example.com`.

### 4.3 Set New Passwords for SYS and SYSTEM Users

With the database environment variables that are set, set the new passwords for the `SYS` and the `SYSTEM` users.

```
$ sqlplus / as sysdba
SQL> alter user SYSTEM identified by <NEW_PASSWORD> ;
SQL> alter user SYS identified by <NEW_PASSWORD> ;
SQL> exit
```

### 4.4 Change Default Password for Weblogic (WLS) Administrator User

Change the password for the Oracle WebLogic Server (WLS) administrator user `weblogic` by using the following steps:

- a. Source the run file system with the `oracle` user:

```
$ . /u01/install/APPS/EBSapps.env run
```

- b. Stop most of the application tier processes, but leave the Node Manager and Admin server running:

```
$ adstpall.sh -skipNM -skipAdmin
```

When prompted, enter APPS user name (`apps`), APPS password, and current WebLogic Server password (`welcome1`).

- c. Change password for the Oracle WebLogic Server administrator user `weblogic`:

```
$ perl $FND_TOP/patch/115/bin/txkUpdateEBSDomain.pl -action=updateAdminPassword
```

Accept the default `apps` context file path when prompted, enter the current WebLogic Admin password, new WebLogic Admin password, and APPS password.

- d. Start all the application tier processes again on the run edition file system.

```
$ adstrtal.sh
```

When prompted, enter APPS user name, APPS password, and WebLogic Server password.

- e. Replace `<NEW_PASSWORD>` with the password you just changed earlier for the `weblogic` user in the following command:

```
$ cd /u01/install/APPS/scripts/
$ chmod 700 st*apps.sh
$ for f in st*apps.sh ;do sed -i 's/welcome1/<NEW_PASSWORD>/' $f ;done
```

### 4.5 Manually Enable TLS

We highly recommend that you perform the following steps to encrypt the traffic between the client and the Oracle HTTP Server. After the encryption setup is complete, you must configure the Oracle E-Business Suite web entry point.

- a. Prepare the environment by applying the prerequisites. See My Oracle Support Knowledge [Document 1367293.1](#), *Enabling TLS in Oracle E-Business Suite Release 12.2*, Section 5.1: Apply Required Updates and Patches.
- b. Encrypt the traffic from the client to the Oracle HTTP Server by performing the configuration for inbound connections for your Oracle E-Business Suite release. See My Oracle Support Knowledge [Document 1367293.1](#), *Enabling TLS in Oracle E-Business Suite Release 12.2*, Section 5.2: Configure Inbound Connections.

## 4.6 Manually Configure Firewall to Limit Client Access

Perform the steps in this section to configure the required firewall rules.

- a. First, on your application tier node, create firewall rules that allow inbound communication to the web entry point from the clients from which you will access the Oracle E-Business Suite URL. To do so, while still logged on to the instance via `ssh`, switch to the root user:

```
$ sudo su -
```

Run the following commands to create the required firewall rules:

```
# firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=<source_CIDR_range>
port port=<web_entry_point> protocol=tcp accept' --permanent
# firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=<source_CIDR_range>
port port=<web_entry_point> protocol=tcp accept'
```

In these commands, replace `<source_CIDR_range>` with the set of IP addresses from which you will access the Oracle E-Business Suite URL. Replace `<web_entry_port>` with the appropriate port, for example `4443`.

- b. Next, update the security list for the subnet that contains the application tier nodes by adding a security rule that allows inbound communication on the web entry point from the clients from which you will access the Oracle E-Business Suite URL. See [Working with Security Lists](#).

In the Oracle Cloud Infrastructure console, open the security list for the application tier subnet and add a new entry under **Allow rules for ingress** with the following properties:

- **Source CIDR** - The CIDR block for your on-premises network that includes the relevant clients, as specified in your firewall rules
- **Protocol** - TCP
- **Destination Port Range** - The web entry port, for example `443`

## 4.7 Configure Security and Firewall Rules for Secure Access to Fusion Middleware and Weblogic Server Administration Console

Administration of the Oracle Fusion Middleware 11g components delivered with Oracle E-Business Suite Release 12.2, including Oracle HTTP Server and Oracle WebLogic Server, requires secure access to the WebLogic Server administration ports running on the Oracle E-Business Suite primary application tier node. Ports 7001 and 7002 are the default WebLogic Server administration ports for the dual file system with Oracle E-Business Suite Release 12.2. The examples in this section use these default ports. If you have configured different port numbers, change the port numbers in the instructions to match the port numbers for your environment.

When you create an Oracle E-Business Suite Release 12.2 environment on Oracle Cloud Infrastructure, you should create a security rule and firewall rules that allow inbound communication on the WebLogic Server administration ports on the primary application tier node. These rules are required as a prerequisite so that a system administrator can securely access the administration ports and the Fusion Middleware Control and WebLogic Server Administration Console. See [Access the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure](#).

Perform the following steps to configure the required security rule and firewall rules:

- a. Update the security list for the primary application tier node by adding a security rule that allows inbound communication on ports 7001 and 7002. See [Working with Security Lists](#).

In the Oracle Cloud Infrastructure console, open the security list for the Oracle E-Business Suite application tier subnet and add a new entry under **Allow rules for ingress** with the following properties:

- **Source CIDR** - The CIDR block corresponding to the source machines.
- **Protocol** - TCP

- **Destination Port Range** - 7001-7002

- Create firewall rules on the primary application tier node that allow inbound communication on ports 7001 and 7002 from the subnet that contains the source machines you would like to connect from. First, log in to the Oracle Cloud Infrastructure instance that hosts your Oracle E-Business Suite environment, using SSH. See [Connecting to an Instance](#).

Then switch to the `root` user:

```
$ sudo su -
```

Run the following commands to create the required firewall rules:

```
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=<source_machines_CIDR>
port port=7001 protocol=tcp accept' --permanent ;
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=<source_machines_CIDR>
port port=7002 protocol=tcp accept' --permanent ;
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=<source_machines_CIDR>
port port=7001 protocol=tcp accept';
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=<source_machines_CIDR>
port port=7002 protocol=tcp accept';
```

## 4.8 Acknowledge the Secure Configuration Recommendations

Access to the environment will be restricted until the system administrator configures or acknowledges the secure configuration recommendations.

To access the Secure Configuration Console, a user must have a responsibility that includes the Applications System (OAM\_APP\_SYSTEM) function privilege, such as the seeded System Administration or System Administrator responsibilities, and must be registered as a local user with Oracle E-Business Suite. The administrator must log in to Oracle E-Business Suite using the local login page (`http(s)://[host]:[port]/OA_HTML/ApsLocalLogin.jsp`) to navigate to the console and unlock the system. If a user with local system administrator privileges is not available, you can access the Secure Configuration Console through a command line utility. For more information, see [Secure Configuration Console](#) in the *Oracle E-Business Suite Security Guide*.

**Note:** Once the system is "Unlocked" for normal usage, the Secure Configuration Console is still available for administrators under the 'Functional Administrator' responsibility.

## Section 5: References

For further information about using this component as part of a larger Oracle E-Business Suite deployment, refer to the following documentation:

- [Oracle Cloud Infrastructure Documentation - Welcome to Oracle Cloud Infrastructure](#)
- [Oracle Cloud Infrastructure Documentation - Developer Tools and Resources](#)

## Change Log

Date	Description
2022-04-26	<ul style="list-style-type: none"> <li>• Changed the release of Oracle E-Business Suite from Release 12.2.10 to 12.2.11 throughout document.</li> <li>• Updated technology component information, such as version levels, in Section 1.1.</li> <li>• Removed former Step 3.5 for CVE-2021-44228.</li> <li>• Updated title for the Quick Start Guide for Oracle E-Business Suite Enterprise Command Centers.</li> </ul>

2021-12-23	<ul style="list-style-type: none"><li>• Added step in Section 3 to apply patches to address Apache log4j vulnerabilities in Oracle E-Business Suite.</li></ul>
2021-11-30	<ul style="list-style-type: none"><li>• Changed the version of Oracle Enterprise Command Center Framework from V6 to V7 in Section 3.11.</li><li>• Changed "EBSCDB_apps.env" to "ebscdb_apps.env" in Section 4.2.</li></ul>
2021-10-12	<ul style="list-style-type: none"><li>• Added Section 3.2 to enable instance-level firewall access.</li></ul>
2021-07-29	<ul style="list-style-type: none"><li>• Changed the version of Oracle Enterprise Command Center Framework from V5 to V6 in Section 3.10.</li></ul>
2021-05-27	<ul style="list-style-type: none"><li>• Initial publication on My Oracle Support. An earlier version of this document was published as an Oracle By Example (OBE) tutorial on Oracle Help Center.</li></ul>

My Oracle Support Knowledge [Document 2764690.1](#) by Oracle E-Business Suite Development.

[Copyright © 2018, 2022, Oracle and/or its affiliates.](#)

Didn't find what you are looking for?