JD Edwards EnterpriseOne

Deploying JD Edwards EnterpriseOne on Linux Learning Path

1.0

JD Edwards EnterpriseOne
Deploying JD Edwards EnterpriseOne on Linux Learning Path

1.0

Part Number: G36660-01

Contents

Preface

Welcome to the JD Edwards EnterpriseOne documentation.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc* .

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs* if you are hearing impaired.

Related Information

For additional information about JD Edwards EnterpriseOne applications, features, content, and training, visit the JD Edwards EnterpriseOne pages on the JD Edwards Resource Library located at:

http://learnjde.com

Conventions

The following text conventions are used in this document:

Convention	Meaning
Bold	Boldface type indicates graphical user interface elements associated with an action or terms defined in text or the glossary.
Italics	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`Monospace`	Monospace type indicates commands within a paragraph, URLs, code examples, text that appears on a screen, or text that you enter.
> Oracle by Example	Indicates a link to an Oracle by Example (OBE). OBEs provide hands-on, step- by-step instructions, including screen captures that guide you through a process using your own environment. Access to OBEs requires a valid Oracle account.

1 Introduction

Overview

This learning path describes how to deploy JD Edwards EnterpriseOne Release 9.2 using One-Click Provisioning on-premises with Linux using an Oracle Database. It is important to note that this document is primarily concerned with the basic requirements for an installation of JD Edwards EnterpriseOne on-premises. It is not intended as a blueprint for operations in typical environments such as Development, Test, or Production.

Upon completion of this learning path, you will have a working deployment of JD Edwards EnterpriseOne on Linux with an Oracle Database on-premises. This process includes post installation tasks and the administration of your deployment.

Before You Begin

Before you begin using JD Edwards EnterpriseOne One-Click Provisioning, you should be aware of these prerequisites:

- Knowledge and Skills
- Tools and Resources

Knowledge and Skills

You must have a fundamental understanding of JD Edwards EnterpriseOne and the installation process for On Premises.

One-Click Provisioning consolidates, enhances, and simplifies the traditional method of installing JD Edwards EnterpriseOne using standalone installers for the various components which includes:

- Server Manager Console installer
- Server Manager Agent installer
- Deployment Server installer
- Platform Pack installer for the Enterprise Server and Database Server
- Installation Planner (functionality provided by One-Click Provisioning)
- HTML Server (installed using Server Manager)

One-Click Provisioning includes two installation modes:

- Quick Start
- Advanced

The Quick Start mode is designed to direct you through a basic JD Edwards EnterpriseOne installation. This mode is not required. That is, you can choose to use Advanced Mode instead of, or supplemental to, Quick Start mode for add-on functionality. The Advanced Mode enables you to orchestrate and deploy configurations to suit your own requirements. Both mode options are covered in this learning path.

This Learning Path is not a substitute for the database administration manuals provided by your Relational Database Management System (RDBMS) vendor, the network administration manuals provided by your network vendor, or the installation and configuration manuals for third-party products used with JD Edwards EnterpriseOne.

Tools and Resources

The PuTTY tool (*https://www.putty.org*) for generating SSH key pairs on the client machine that you will use to connect to any Linux server deployed by One-Click Provisioning.

Fundamentals

You can deploy JD Edwards EnterpriseOne using the JD Edwards EnterpriseOne One-Click Provisioning Server. This server features a web-based JD Edwards Provisioning Console interface that enables the provisioning of a fully functional suite of interconnected servers. The required core servers are the Database Server, the Enterprise Server, the HTML Web Server, and the Application Interface Service (AIS) Server. The One-Click Provisioning Server includes the JD Edwards Server Manager Console (SMC). One-Click Provisioning will also deploy the required Deployment Server into a Microsoft Windows environment.

For all servers you should use the highest version available that is specified in the Oracle Certifications for JD Edwards EnterpriseOne for One-Click Provisioning.

The following servers can be deployed by One-Click Provisioning:

- One or more Database Servers
- One or more Enterprise Servers
- One or more Standard HTML Servers (as standalone instances within WebLogic, not clustered)
- One or more Dedicated HTML Servers (as standalone instances within WebLogic, not clustered)
- One or more AIS Servers (as standalone instances within WebLogic, not clustered)

Prior to deploying the web components using One-Click, users must separately install their own licensed version of WebLogic Server. This learning path includes the prerequisites for WebLogic setup for use with JD Edwards EnterpriseOne.

One-Click provisioning can only deploy this machine into a Microsoft Windows Server:

- A single Deployment Server

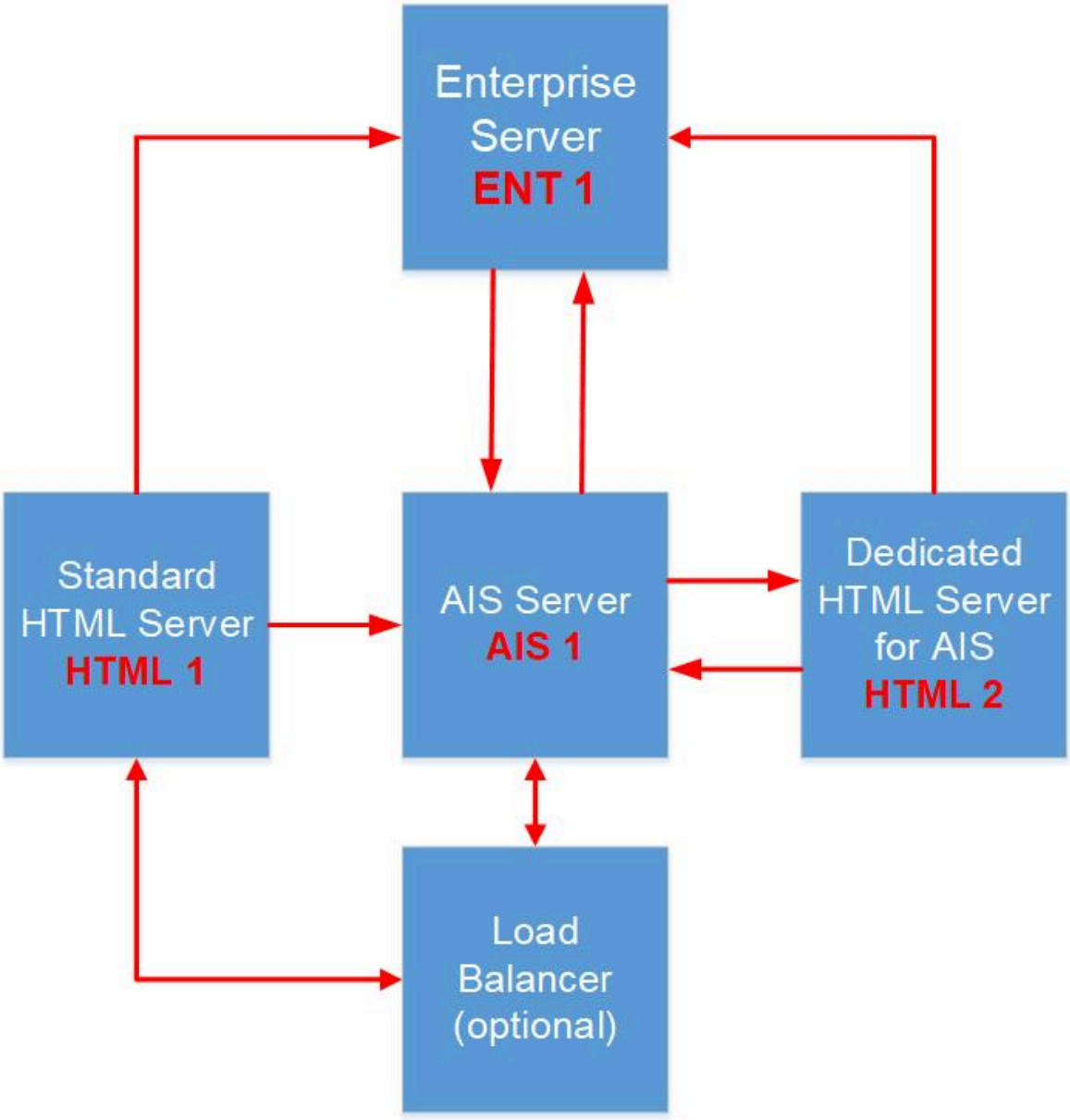
Standalone and Dedicated HTML Servers

Beginning with One-Click Provisioning based on JD Edwards Tools Release 9.2.5, the JD Edwards EnterpriseOne One-Click architecture for HTML and AIS Servers introduces the concept of Standalone and Dedicated HTML Servers.

Using Quick Start Mode, users are required to select a single HTML Server that is dedicated to a specific AIS Server.

Using Advanced Mode, in addition to adding additional Dedicated HTML and AIS server pairs, users can add a Standard HTML Server that is not dedicated to an AIS Server. A Standard HTML Server functions as a traditional HTML Server handling all non-AIS requests. To scale by pathcode, multiple pairs of HTML and AIS servers can be configured. Likewise, multiple Standard HTML Servers can be configured for use with or without load balancers. Using one or more Standard HTML Servers is recommended for Production environments.

The following diagram depicts the architecture and following that is a description of the characteristics of each HTML and AIS server.



Standard HTML Server

Note: The Standard HTML Server can only be deployed using the Advanced Mode.

Referencing the the pod architecture diagram, the Standard HTML Server is **HTML 1** and has these characteristics:

- Can be loaded balanced (using LBaaS or other)
- Configured for one-way communication to a specific Enterprise Server (**ENT 1**)
- Configured for one-way communication to an AIS Server (**AIS 1**)

- Not paired with an AIS Server to perform AIS runtime
- Not configured to communicate with the Dedicated HTML Server for AIS (**HTML 2**)

AIS Server

Referencing the the pod architecture diagram, the AIS Server is **AIS 1** and has these characteristics:

- Can be loaded balanced (using LBaaS or other)
- Paired with a dedicated Dedicated HTML Server for AIS (**AIS 2**)
- Configured for two-way communication with both an Enterprise Server (**ENT 1**) and, for AIS runtime, to the Dedicated HTML Server for AIS (**HTML 2**)

Dedicated HTML Server for AIS

> **Note:** The Quick Start mode can only deploy a single Dedicated HTML Server for AIS. You must use the Advanced Mode to deploy a Standard HTML Server.

- Referencing the the pod architecture diagram, the Dedicated HTML Server for AIS is HTML 2 and has these characteristics:
- Cannot be loaded balanced (using LBaaS or other)
- Paired to a specific AIS Server (**AIS 1**)
- Configured for one-way communication with an Enterprise Server (**ENT 1**)
- Configured for two-way communication with a specific AIS Server (**AIS 1**) for AIS runtime

Standalone Deployment Server

You can use Advanced Mode to install a Standalone Deployment Server, which is usually defined as part of the required workflow during Quick Start mode. Using this optional flow you can provision Deployment Server by itself without having to orchestrate any other server. However, you must ensure that you know the exact host name of the core JD Edwards EnterpriseOne servers that are, or will be, in the same environment as the Standalone Deployment Server. These core servers include the Database Server, Enterprise Server, HTML Server, and AIS Server. It is not necessary that of any of these core JD Edwards EnterpriseOne servers exists at the time of orchestrating the Standalone Deployment Server. At any time prior or subsequent to the deployment of a Standalone Deployment Server, you can can orchestrate the core JD Edwards EnterpriseOne servers. After you have deployed a Standalone Deployment Server, you must ensure that you perform the procedures in the OBE of this Learning Path entitled: ***Performing Post Installation for the Standalone Deployment Server.***

Server Manager Console Centralized Configuration

As part of One-Click Provisioning, Centralized Configuration in the Server Manager Console is enabled automatically. One-Click adds the server group specific INI settings when provisioning individual servers. Post provisioning, the administrator is responsible for applying the group changes on the Centralized Configuration enabled environments.

Supported Software Versions

The following table lists the supported software versions for Oracle and Microsoft components running on Oracle Cloud Infrastructure:

Supported Software Versions	
Operating System	
- Provisioning Server	Oracle Enterprise Linux 9.6
- Oracle Database Server in Compute	Oracle Enterprise Linux 9.6
- Oracle Database Server in DB Systems	Oracle Enterprise Linux 8.10 (Oracle 26ai: current, subject to change)
- Oracle Autonomous Database	Autonomous Transaction Processing on Dedicated Exadata Infrastructure - Version 26ai
- Enterprise Server	Oracle Enterprise Linux 9.6
- Oracle WebLogic Server	Oracle Enterprise Linux 9.6
- Deployment Server	Microsoft Windows Server 2022
Oracle Database	Oracle 19C (Compute Database) Oracle 26ai (Database System, Oracle Autonomous Database)
Oracle WebLogic Server	14.1.1.0
Oracle WebLogic Server Patches for 14.1.1.0	p28186730, p38412913 Tip: You can verify your patch level running this command from the **<OH>/OPatch** location on your WebLogic Server: **./opatch lspatches**
Java Development Kit (JDK) (Required for Oracle WebLogic Server)	Version 1.8.0 up to Update 471
Load Balancer (Optional)	OCI Load Balancer
JD Edwards EnterpriseOne One-Click System	Tools Release 9.2.26.1 64-bit ESU up to JN21495 UDO up to UDO_9.2_10719 + UN26_UDO_Bundle Planner JN21409 Data Pack is DP0289201

2 Upgrading from Prior Releases of EnterpriseOne

Upgrade Considerations

If you are planning an Applications Upgrade to a One-Click installation of JD Edwards EnterpriseOne, you should be aware of important technical considerations.

These considerations are described in the Applications Upgrade Guide which describes an upgrade to the base Applications Release 9.2.

Refer to this section of the upgrade guide:

Technical Considerations for Applications Upgrade to a 64-bit Version of 9.2

3 Planning Your Deployment

Minimum Resource Requirements

The table below specifies the minimum resource requirements to install and run JD Edwards On-Premises using an Oracle database (Linux and Microsoft Windows) or a Microsoft SQL Server database (Microsoft Windows). Your environment may require additional resources based on transaction volumes, number of users, availability requirement, integrations, and business requirements.

Note: For implementation of JD Edwards EnterpriseOne on Oracle Cloud Infrastructure, users can choose any Shape Series that provides:

- x86-compatible processors (such as Intel and AMD). Support for RISC (reduced instruction set) processors (such as ARM) is specifically excluded.
- Minimum of 2 OCPUs
- Minimum of 30 GB memory per OCPU

Note: Within the **Specialty and previous generation** shape series, only these shapes are supported:

- VM.Standard2.2
- VM.Standard2.4
- VM.Standard2.8
- VM.Standard2.16
- VM.Standard2.24

JD Edwards EnterpriseOne Server Type	Minimum Recommended			Notes
	CPU	Memory (GB)	Storage Volume (GB)	
Required JD Edwards Components				
One-Click Provisioning Server	2	30	100	Includes Server Manager
Deployment Server	2	30	210 GB* for all four (4) pathcodes	Using One-Click, customers must install all four (4) path codes. There is no automated way to add additional path codes post deployment.

				* Storage volume space is in addition to that required by the Windows OS itself, which can be up to 45 GB. Therefore, the minimum recommended storage volume size is 256 GB.
Database Server	2	30	50 GB for a single pathcode and shared data	20 GB is required for each additional pathcode. These numbers are for demo data only and should be adjusted for expected required business data space.
Enterprise Server	2	30	75	
WebLogic Server • HTML Server for Web Client • HTML Server for AIS Server • AIS Server	-	-	30	For the OS and WebLogic Server
	2	30	20	Per Web Instance
	2	30	20	Per Web Instance
	2	30	20	Per Web Instance
Optional JD Edwards Components				
Business Services Server (BSSV)	2	30	50	Per Web Instance
Transaction Server for Real Time Events (RTE)	2	30	50	Per Web Instance
Application Development Framework Server (ADF)	2	30	50	Per Web Instance
One View Reporting (OVR) Server / BI Publisher Server (BIP)	2	30	50 GB is required for a single pathcode	10 GB is required for each additional pathcode
Development Client	2	30	100	Per each Development Client installation

Note: Optional components are not deployed by One-Click. However the Web Components can be manually added through Server Manager and the Development Client can be added in a new Microsoft Windows instance using the traditional on-premise methodology.

Understanding Port Restrictions

This section provides an overview of the restricted ports that cannot be defined or used while creating any web component or server, or both. You should be aware of the restricted ports that cannot be defined or used while creating any web component or server, or both.

The specific port restrictions for any One-Click Provisioning deployment of JD Edwards EnterpriseOne are grouped as follows:

- One-Click Provisioning Console for JD Edwards
- All Internet Browsers
- Google Chrome and Mozilla Firefox Browsers

One-Click Provisioning Console for JD Edwards

- Any port below 1024 is restricted.

All Internet Browsers

The following are restricted ports enforced by the rules of any internet browser:

- 2049
- 4045
- 6000

Google Chrome and Mozilla Firefox Browsers

In addition to the above mentioned restricted ports for any internet browser, the Google Chrome and Mozilla Firefox browsers block specific ports which they deem as unsafe to use on HTTP/HTTPS protocol. These restricted ports are:

- 3659, // apple-sasl / PasswordServer
- 6665, // Alternate IRC [Apple addition]
- 6666, // Alternate IRC [Apple addition]
- 6667, // Standard IRC [Apple addition]
- 6668, // Alternate IRC [Apple addition]
- 6669, // Alternate IRC [Apple addition]

Note: It may be possible to configure Chrome and/or Firefox to change these restrictions.

Generating Secure SHell (SSH) Key Pairs on Your Local System

This section outlines the requirement to generate SSH key pairs on your local system, which can be UNIX or Windows.

Note: All references to UNIX also apply to Linux.

Generating Secure Shell (SSH) Key Pairs on Your Local System

If you already have an SSH key pair, you may use that to connect to your environment whether it is running On-Premises or in Oracle Cloud Infrastructure.

> **Tip:** The best practice is to create at least two SSH keys, a primary and a backup, because if for any reason an SSH Key is no longer valid, access to the instance or machine would be lost with no means to recover the access. A user cannot access an instance or machine without using an SSH Key.

For instances in Oracle Cloud Infrastructure, it is recommended you use the Oracle Cloud Shell to interface with a Oracle Cloud Infrastructure instance. Oracle Cloud Shell is browser-based, does not require installation or configuration of anything on your laptop, and works independently of your network setup. The below referenced Oracle documentation for generating SSH keys provides instructions for these options:

- Oracle Cloud Shell
- Apple MacOS
- Microsoft Windows 10
- Prior Microsoft Windows Versions
- SSH Keys for Linux

Creating a Pre-Installation Worksheet

Machine	**IP Address**
Provisioning Server and Server Manager (same machine)	https://__.__.__.__:3000 where **https** is the only supported browser protocol, and where **3000** is always the port, which you must include as part of the address
Machine	**Hostname**
Database Server in Compute or a DB System	
Autonomous Database (ADB)	ADB Admin User Password: _____ ADB WALLET: _____ Auth Token of User: _____ Tenancy: _____ Username: _____ Region: _____ Bucket: _____
HTML Server	

AIS Server	
Deployment Server	Hostname: _____ Location Name: _____

Note:
Do not use a fully qualified domain name for host names; you should only specify the first node of the domain name.

For the Database, Enterprise, and Deployment Servers, machine names are limited to a maximum of 15 **lower-case** alphanumeric characters as limited by the JD Edwards EnterpriseOne database table and application design.

For all servers, you cannot use special characters in the name, such as an underscore "_". The user interface will enforce this restriction.

User Account	**Password**
oracle	These users do not have a login password. Access is through SSH Keys only, logging in using the username **opc**. Enter SSH Key names here.
jde920	
em_manager_user	
sys, system	
weblogic	
JDE	
jde_admin	
Initial Windows Machine Administrator (temporary)	
Site Key Passphrase	
Server Manager Console	
SQL DB User (SA)	

Note: This is only applicable to Oracle Cloud Infrastructure with Microsoft Windows and On-Premises Microsoft Windows with SQL Server database.

Note: The password for ***any*** Windows user on ***any*** Windows machine must not contain the $ or ! characters; using these characters violates the Oracle password policy and will result in denied access.

4 Configuring the Linux Servers

Obtaining and Using Archive Files for One-Click Provisioning

This section shows you how to obtain and use archive files for One-Click Provisioning for JD Edwards EnterpriseOne.

Prerequisites

- You must have created a VM or a server for the Provisioning Server.
- The Linux instance for the Provisioning Server must be allocated with storage volume space, the amount of which is specified in the ***Before You Begin*** section at the beginning of this Learning Path.
- You must have performed the functions described in the module of this Learning Path entitled: ***All Servers Common Setup.***

Obtain, Unzip, Assemble, and Extract the Provisioning Server Archive Files

Due to file size limitations for files available from the Oracle Software Delivery Cloud (also called OSDC or E-Delivery), the requisite archive cannot be posted as a single entity. Instead you must download a series of files that have been split into allowable sizes and then assemble them into a single archive, and then extract the contents of that archive using the following procedure.

1. Download the files for JD Edwards EnterpriseOne One-Click Provisioning from the Oracle Software Delivery Cloud using **All Categories** and **JD Edwards One-Click Provisioning** as the search criteria. From the displayed list, choose the combination of JD Edwards EnterpriseOne applications and tools releases and proceed to add the items to your cart.
2. Click **Selected Software** and then use the drop-down menu for **JD Edwards One-Click Provisioning** to choose **Linux**.
3. To continue, review and agree to the license agreement.
4. A list of available files is shown.
5. Download the items in your cart. These items have part numbers in the form of `vxxxxxx.zip` and may not be in sequential order.
6. From your download location, unzip all files, which will extract the DiskPart files that need to be reassembled, a rebuild script, and a checksum file.
7. Upload all the unzipped files to any directory on the Provisioning Server.

   > **Note:** At this point it is recommended that, space permitting, you make a copy of these files in case you need to reuse them without re-downloading and re-uploading.

8. Ensure the rebuild.sh script has the proper permissions to execute by using this command:

   ```
   chmod 775 rebuild.sh
   ```

9. Execute the rebuild script with this command:

   ```
   sudo ./rebuild.sh
   ```

   The script performs these operations:

Step 1 - Checks to ensure sufficient space is available on /u01 to complete the extraction

Step 2 - Combines the unzipped pieces of the archive file into a single file

Step 3 - Uses the checksum utility to verify the recombined file size

Step 4 - Moves the JD Edwards packages to the proper location, which is /u01

> **Note:** The extraction and rebuild process can take quite some time, perhaps as long as 10 to 20 minutes.

Once extracted, `/u01` should contain the following components:

```
[root@sqeprov712 u01]# ls -al
total 60
drwxrwx---. 11 root root  4096 Aug  9 21:50 .
dr-xr-xr-x. 18 root root  4096 Aug  7 21:19 ..
drwx------.  3 root root  4096 Jul  7 16:22 app
drwx------.  2 root root  4096 Aug  3 19:46 CertGen
drwxr-xr-x. 12 root root  4096 Aug  3 22:44 E1CloudConsole
drwx------. 22 root root  4096 Jul 28 14:33 E1ProvisionPrime
drwxr-xr-x.  4 root root  4096 Aug  3 23:09 jde920
drwx------.  8 root root  4096 Mar 15 08:35 jdk1.8.0
drwx------.  2 root root 16384 Aug  7 21:16 lost+found
drwxr-x---. 13 root root  4096 Feb  6  2017 OracleSMC
-rwx------.  1 root root   942 Jul 13 05:45 setupPr.sh
drwxrwxr-x. 11 root root  4096 Aug  3  2016 SMConsole
```

Performing Common Setup for All Linux Servers

This section describes these common setup tasks that must be performed on all Linux servers that are deployed by JD Edwards EnterpriseOne One-Click Provisioning:

Prerequisite

You must have a Linux server for all the servers that will be deployed by JD Edwards EnterpriseOne One-Click Provisioning except for the Deployment Server, which must be a Microsoft Windows server. At a minimum, One-Click Provisioning includes the deployment of the Provisioning Server, Database Server, Enterprise Server, and WebLogic Server.

General

The following general prerequisites are required for each Linux server:

1. Ensure that each machine has umask set to 0022.

   To set umask permanently, add below the command to the `bashrc(~/.bashrc)` for ***both*** the **root** and the **opc** users:

   ```
   umask 0022
   ```

2. Ensure that the host name of a Linux server contains only alphanumeric values. For all servers, you cannot use special characters, except a hyphen (-).
3. Log in as the root user.
4. Verify the `/etc/ssh/sshd_config` file contains this setting:

   ```
   ClientAliveInterval 3600
   ```

   Ensure that the setting exists, is set properly to `3600`, and is not commented out.
5. Verify the `/etc/ssh/sshd_config` file has the SSH connection over IPV6 disabled by using this setting:

   ```
   AddressFamily inet
   ```

   Ensure that the setting exists, is set properly to inet (not any), and is not commented out.
6. Verify the `/etc/sudoers` file either does ***not*** contain the following setting or that the setting is disabled in the file:

   ```
   Defaults requiretty
   ```

   > **Tip:** You can use this command to edit the /etc/sudoers file: sudo visudo

7. Also in the `/etc/sudoers` file, set the **opc** user to have passwordless sudo access by adding this entry:

   ```
   opc ALL=(ALL) NOPASSWD: ALL
   ```
8. You must disable IPV6 using the following command:

   ```
   sudo vi /etc/sysctl.conf
   ```

   Ensure that these settings within the /etc/sysctl.conf file are set in order to disable IPV6 protocol:

   ```
   net.ipv6.conf.default.disable_ipv6=1
   ```

   ```
   net.ipv6.conf.all.disable_ipv6=1
   ```
9. You must ensure that the fully qualified domain name (FQDN) in the `/etc/hostname` file does **not** include the **localdomain** suffix. For example, if the following setting exists in your `/etc/hostname` file:

   ```
   sqeweb111.localdomain
   ```

   For example, if the setting `sqeweb111.localdomain` exists in your `/etc/hostname` file, remove the `.localdomain` suffix.

Enable Inbound Ports in the Firewall for Compute Instances

You must enable inbound ports in the firewall service for each Linux server to enable the functionality of the Provisioning Server to provision each Linux server.

1. For each JD Edwards EnterpriseOne server, repeat this command as necessary to specify open ports in the firewall:

   sudo firewall-cmd --zone=public --add-port=*<PORT>*/tcp --permanent

   In the preceding command, *<PORT>* is the number of the port that must be open. The ports that must be open are listed in the following table.

Linux Server Firewall Port List	
Component	**Inbound Ports to Open**
Provisioning Server	22 445 3000 5150 8998 8999 7000-7001 14501-14502
Oracle Database	22 5150 <DB_PORT> 14502-14510
Enterprise Server	22 5150 6017-6022 14502-14510

Linux Server Firewall Port List	
Web Server	22 5150 <WLS_ADMIN_PORT> See Note 1 <SSL_ACCESS_PORT> See Note 2 <SSL_ACCESS_PORT-1> See Note 3 14502-14520

Note: 1 This is the Admin Port on which the Admin Server is running. This value is set by the user while creating a WebLogic domain.

Note: 2 This SSL port must be opened to enable the Server Manager Console to complete the tasks.

Note: 3 This port number is equal to the value of the SSL port minus one. This port must be opened to enable the Server Manager to complete the provisioning tasks. For example, if you have specified the port value as 8081 in the One-Click Provisioning Console, you must open 8080 port (8081-1).

Also, you must open a port for each of the WebLogic Servers. For example, if you have the following environment and server combinations, you should open eight ports: four SSL ports for the port numbers specified by using the Provisioning Console, and four non-SSL ports. The value of each non-SSL port must be the value of the SSL port minus one.

- DV HTML
- PD HTML
- DV AIS
- PD AIS

2. After all the ports are opened in the firewall for each server, use these commands to reload the firewall:

```
systemctl stop firewalld

systemctl start firewalld
```

Disable SELINUX and Reboot Machines

After you have configured the firewall, use this procedure to disable SELINUX and reboot the machine for the changes to take effect.

1. Use this command to check the status of Security Enhanced Linux (SELINUX):

   ```
   sudo getenforce
   ```

   If the returned status is either **Enforcing** or **Permissive**, you must temporarily disable the extra security restriction provided by SELINUX by modifying this file:

   ```
   /etc/selinux/config
   ```

   Edit the `/etc/selinux/config` file to change the `SELINUX=` setting to this value:

   ```
   SELINUX=disabled
   ```
2. When you change any security settings, such as disabling SELINUX as described in the preceding step, you must reboot the machine using this command:

   ```
   shutdown -r now
   ```
3. If you reboot to enable security settings, after the reboot is complete, run `sudo getenforce` to confirm that the status of SELINUX is **Disabled**.

Set Up Users and Groups

Perform these tasks to set up additional users and groups on each Linux server:

1. Create the **opc** user using this command:

   sudo useradd -d /home/opc -m -s /bin/bash opc
2. If the /u01 mount point does not exist, create it using this command:

   sudo mkdir /u01
3. Use this command to ensure that the /u01 mount point has proper permissions to allow the One-Click Provisioning process to subsequently create requisite folders:

   ```
   sudo chmod 770 /u01
   ```
4. Create the **dba**, **oracle**, and **opc** groups using these commands:

   sudo groupadd -g nnnn dba

   sudo groupadd -g nnnn oracle

   sudo groupadd -g nnnn opc

   In the above commands, nnnn is the ID with which the group will be created. You must use a free value which ideally should be above 1000. You can determine used group IDs> with the id command.
5. Create the **oracle** user and add it to the **oracle** group using this command:

   ```
   sudo useradd -d /home/oracle -m -s /bin/bash oracle
   ```
6. Add the **opc** user to the **oracle** group and the **oracle** user to the **dba** group and the **oracle** group using these commands:

   sudo usermod -a -G oracle opc

sudo usermod -a -G oracle oracle

sudo usermod -a -G dba oracle

7. Set /u01 as owned by the **oracle** group using this command:

   sudo chgrp oracle /u01

Install Requisite YUM Packages

You must install a specific set of packages from the YUM repository onto the One-Click Provisioning Server and each additional Linux-based Server in the JD Edwards EnterpriseOne environment which include:

- Provisioning Server
- Compute Oracle Database Server
- Enterprise Server
- WebLogic Server

> **Note:** Ensure that you have enabled your YUM repository. This functionality is required to install YUM packages that are prerequisites to set up each JD Edwards EnterpriseOne server. If you had not enabled your YUM repository before you ran One-Click to set up the JD Edwards EnterpriseOne servers, then you must enable it and manually install and update all required YUM packages as listed below.

The following lists are the required packages sorted sorted in an alphabetic order. You can create a script to install the packages one at a time, or all at once. In either case, confirm that when each command runs, it returns either of these results:

```
Complete
```

or

```
Nothing to do
```

> **Note:** If you run all the YUM packages at once, using a single command, you may encounter error conditions where a package may not install as expected due to dependency or other technical issues with the package or library. Further, this behavior is unpredictable and can vary according to system conditions. The resolution of such error conditions is the responsibility of your system administrator and is beyond the scope of this document. If you need help resolving YUM issues, your Linux administrator should open a service request with the Oracle Linux support team. Additionally, various Linux OS images may be delivered with some of the packages that are installed by default. You can use the following commands to cross-check which packages are already installed and those that you need to manually install.

> **Note:** It is recommended that you run YUM install commands as the root user. For example: `sudo su yum install -y bind-utils`

Provisioning Server

Ensure the VM instance for the Provisioning Server contains these YUM packages:

```
bind-utils
```

```
gcc.x86_64

gcc-c++.x86_64

ksh.x86_64

unzip.x86_64

zip.x86_64

zlib-devel.x86_64

openssl-devel
```

Tip: The following is an example of the commands to include the above package list.

Note: The Samba install is a separate command.

```
yum install -y zip.x86_64 unzip.x86_64 bind-utils ksh.x86_64 gcc-c++.x86_64 gcc.x86_64 zlib-devel.x86_64
openssl-devel

yum install 4.18.6-3.0.3.el8_9 -y
```

The following library must be added using the command:

```
sudo dnf install --enablerepo=ol8_codeready_builder libyaml-devel -y
```

Compute Oracle Database Server

Ensure the VM instance for the Compute Oracle Database Server contains these YUM packages:

Note: For users who have previously set up servers using a previous version of the Oracle database, the package names below with strikethrough are not required for the currently supported version.

```
bind-utils

compat-libcap1.x86_64

compat-libstdc++-33.x86_64

compat-openssl10.x86_64

gcc.x86_64

gcc-c++.x86_64

~~glibc.i686~~

glibc.x86_64

glibc-devel.x86_64

ksh.x86_64

libaio.x86_64
```

libaio-devel.x86_64

libgcc.x86_64

libstdc++.x86_64

libstdc++-devel.x86_64

libX11.x86_64

libXau.x86_64

libxcb.x86_64

libXext.x86_64

libXi.x86_64

libXtst.x86_64

make.x86_64

sysstat.x86_64

unzip.x86_64

zip.x86_64

Enterprise Server

> **Note:** Usually, the order in which you run YUM updates is not a factor. However, there is a known dependency on the installation order for certain packages so you should install packages in the order shown below. If other dependencies arise, they should be resolved by your Linux administrator.

Ensure the VM instance for the Enterprise Server contains these YUM packages:

> **Note:** For users who have previously set up servers using a previous version of Linux, the package names below with strikethrough are not required for OL8, while the names in bold are new requirements.

~~**compat-libcap1.x86_64**~~

~~**compat-libstdc++-33.i686**~~

~~**compat-libstdc++-33.x86_64**~~

elfutils-libelf-devel.x86_64

file

gcc.x86_64

gcc-c++.x86_64

~~**glibc.i686**~~

glibc.x86_64

~~glibc-devel.i686~~

glibc-devel.x86_64

ksh.x86_64

~~libaio.i686~~

libaio.x86_64

~~libaio-devel.i686~~

libaio-devel.x86_64

~~libgcc.i686~~

libgcc.x86_64

~~libnsl.x86_64~~

~~libstdc++.i686~~

libstdc++.x86_64

libstdc++-devel.x86_64

~~libX11.i686~~

libX11.x86_64

~~libXau.i686~~

libXau.x86_64

~~libxcb.i686~~

libxcb.x86_64

~~libXext.i686~~

libXext.x86_64

~~libXi.i686~~

libXi.x86_64

~~libXtst.i686~~

libXtst.x86_64

make.x86_64

ncompress

oracle-database-preinstall-19c.x86_64

sysstat.x86_64

unixODBC.x86_64

unixODBC-devel.x86_64

unzip.x86_64

~~**zlib.i686**~~

zlib.x86_64

zip.x86_64

~~**zlib-devel.i686**~~

zlib-devel.x86_64

nss-softokn-freebl.x86_64

~~**nss-softokn-freebl.i686**~~

WebLogic Server

Ensure the VM instance for the WebLogic Server contains these YUM packages:

> **Note:** For users who have previously set up servers using a previous version of WebLogic Server, the package names below with strikethrough are not required for the currently supported version, while the names in bold are new requirements.

bind-utils

~~**glibc.i686**~~

glibc.x86_64

glibc-devel.x86_64

ksh.x86_64

~~**libnsl.x86_64**~~

net-tools

unzip.x86_64

zip.x86_64

zlib-devel.x86_64

Setting Up the Provisioning Server

This section shows you how to set up the Provisioning Server.

Prerequisites

- You must have obtained the archive files for One-Click Provisioning as described in the preceding OBE "Obtaining and Using Archive Files for One-Click Provisioning" of this Learning Path.
- You must have performed the tasks described in the OBE "Performing Common Setup for All Linux Servers" of this Learning Path.

General

Ensure that you have performed all the tasks described in the OBE "All Linux Servers Common Setup" including the steps to create groups and users as well as assigning proper permissions to /u01.

Ensure that there is sufficient storage available on the Provisioning Server for the YUM packages, and the Provisioning Server archive (compressed and extracted).

Install and Compile Ruby

The Ruby program is required to run the functions of JD Edwards One-Click Provisioning. You must use this procedure to install and compile Ruby on the Provisioning Server. This procedure also includes the command to install the gem package for the winrm program.

1. Log in to the Provisioning Server as the **opc** user.
2. Navigate to the home directory using this command:

   ```
   cd ~
   ```
3. Log in as **root** user.
4. Install and compile Ruby using these commands:

   ```
   wget https://cache.ruby-lang.org/pub/ruby/3.3/ruby-3.3.4.tar.gz

   tar -xzf ruby-*.tar.gz

   chmod 755 -R ruby-*

   cd ruby-*

   ./configure --prefix=/usr --disable-dtrace

   make

   make install
   ```
5. Log in as the **opc** user.
6. Install the **gem** package and **uri** as the **opc** user:

   ```
   echo "GEM_HOME=$HOME/gems" >> $HOME/.bash_profile

   echo "export GEM_HOME" >> $HOME/.bash_profile

   source $HOME/.bash_profile

   gem install -v 2.3.6 -r winrm
   ```
7. Log in as the **root** user.
8. Install the **winrm** program using this command as the **root** user:

   ```
   gem install -v 2.3.6 -r winrm
   ```

Run the setupPr.sh Script as the Root User

As the root user, you must run the `setupPr.sh` script that was delivered when you extracted the Provisioning Server archive as described in the preceding section. This script automates the remaining required configuration of the Provisioning Server and performs these requisite tasks:

- Sets up permission and ownership of the extracted content
- Adds system files such as `jdedwards`, `chkPort`, and `chkDNS`
- Configures the Samba service
- Adds the Server Manager Console service
- Adds the Provisioning Console service
- Creates and configures self-signed certificates
- Disables IPv6 on the Provisioning Server

From the script location on `/u01`, run this command as the **root user**:

```
./setupPr.sh
```

> **Note:** If you attempt to run this script as any user other than root, the script will immediately report an error condition: **Script must be run as root.**

After the command runs successfully, the Provisioning Console should be up and running. You can access the Provisioning Console using a URL with the following syntax:

```
https://<Public Ip Address>:3000
```

Setting Up the Oracle Database Server

This section describes these setup tasks that must be performed on the Oracle Database Server:

Prerequisite

You must have performed the functions described in the module of this Learning Path entitled: ***Performing Common Setup for All Linux Servers*** .

General

The following general prerequisites are required for the Oracle Database Server:

1. The database must be installed under the `/u01` directory.

   > **Note:** Installing the database on any mount point other than `/u01` is not supported; provisioning cannot occur.

2. You must configure the semaphore parameter in the `/etc/sysctl.conf` file using this command:
   ```
   sudo vi /etc/sysctl.conf
   ```
   Ensure that this setting exists:

```
kernel.sem = 1024 32000 100 1024
```

3. Ensure that sufficient available storage is available on `/u01` for the Database Server.

   Use this command to view your available storage space on `/u01`:

   ```
   df -h
   ```

4. From SQL prompt, use these commands to allocate recovery space for archive logging:

   - Log in as the **oracle** user:

     ```
     $ sudo su - oracle
     ```

   - Log in to the database:

     ```
     sqlplus '/as sysdba';
     ```

   - Set the recovery space using this command:

     ```
     sql> ALTER SYSTEM SET db_recovery_file_dest_size=50G SCOPE=BOTH;
     ```

   - Verify the available and used recovery space using this command:

     ```
     sql> SELECT * FROM V$RECOVERY_FILE_DEST;
     ```

     For example, if you set the recovery space to 50 GB and installed a full complement of pathcodes (SHARED, PS, DV, PY), issuing this command returns these results where the space limit is approximately 54 GB with 48 GB in use.

     ```
     NAME

     ----------------------------------------------------------------------

     SPACE_LIMIT SPACE_USED SPACE_RECLAIMABLE NUMBER_OF_FILES CON_ID

     ----------- ---------- ----------------- --------------- ----------

     +RECO

     5.3687E+10 4.7264E+10 0 53 0
     ```

Prerequisite Configuration for the Oracle Database Server

The JD Edwards EnterpriseOne One-Click deployment of the Oracle database supports both Oracle Enterprise Edition and Standard Edition 2 for the current supported release of Oracle Database.

> **Note:** You should have an Oracle DBA monitor the database relative to subsequent JD Edwards functions, such as Package Build. Database aspects such as Archive Logging can adversely affect disk space usage and could potentially cause database failures.

The following prerequisite configuration settings are applicable to a customer-installed Oracle database. These prerequisites must be met before the One-Click Provisioning Server can install a JD Edwards EnterpriseOne Database Server:

- Customer must have an Oracle Database Server instance installed.

  > **Note:** The password for the database users of an Oracle database can only include these special characters:_ # -

- Customer must make TNS entry of the pluggable database in the tnsnames.ora file on the Database Server instance (do not use a variable for **ORACLE_HOME**; it must be an absolute value). The hostname field should be updated with the hostname of the Database Server machine.

  > **Note:** For the shared schema, the TNS Alias must be **JDEORCL** and for non-shared schema it must be an alias value *other than* **JDEORCL**.

- You must install the Oracle database as the **oracle** user -- ***not*** as any other user such as **opc**.
- Customer must set the database character set to **AL32UTF8**
- Customer must set the database national character set for the Unicode page setting to **AL16UTF16**

  > **Note:** The character set parameters are critical and must be set when the database is installed; they cannot be changed after installation.

- Minimum storage requirement for JD Edwards Shared Database is 10 GB
- Minimum storage requirement per pathcode is 20GB (Including demo data)
- Above mentioned storage should be made available for:
  - OraDB install directory
  - OraDB index directory
  - OraDB table directory

  These are the directories that you will specify during Orchestration.

  > **Note:** Best practice is to use ***different*** mount points for creating these directories. Otherwise you may encounter database deployment issues.

- Customer must set the minimum required DB processes to provision the JD Edwards EnterpriseOne Database Server to a minimum value of 1500
- Customer must ensure the Files System IO option is **SETALL**
- Database must be running with PDB (JDEORCL) set to **OPEN_MODE**
- Set environment variables for the Oracle Database because by default environment variables for the oracle user are not set

The following is a detailed list of commands necessary to set up the prerequisites for the Oracle Database for use with JD Edwards EnterpriseOne One-Click Provisioning.

1. Use this command to ensure that the /u01 mount point has proper permissions to allow the One-Click Provisioning process to subsequently create requisite folders:

   sudo chmod 775 /u01

   > **Note:** This permission is required for the Database Server or else One-Click Provisioning will fail.

2. Sudo to the **oracle** user from the **opc** user using this command:

   ```
   sudo su - oracle
   ```

3. Make a TNS entry of the pluggable database in the listener.ora and tnsnames.ora files of the Database Server machine. Ensure the same **port** is also specified in each file. For example:

---

listener.ora

LISTENER_ORCL =

(ADDRESS = (PROTOCOL = TCP)(HOST = **hostname**)(PORT = **1521**))

ORCL =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = **hostname**)(PORT = **1521**))

(CONNECT_DATA =

(SERVER = DEDICATED)

(SERVICE_NAME = **jdeorcl**)

)

)

---

tnsnames.ora

JDEORCL =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = **hostname**)(PORT = **1521**))

(CONNECT_DATA =

(SERVER = DEDICATED)

(SERVICE_NAME = **jdeorcl**)

)

)

4. Use this procedure to set the environment variables because by default environment variables for the oracle user are not set.
   - Switch to the **oracle** user using this command:

     ```
     sudo su - oracle
     ```
   - Edit the bash_profile using this command:

     ```
     vi .bash_profile
     ```
   - Add the following lines in the .bash_profile

     ```
     export ORACLE_HOME=path
     export ORACLE_SID=ORCL
     PATH=path
     export PATH
     ```

     > **Note:** You cannot use an environment variable when defining ORACLE_HOME, such as $ORACLE_HOME. You must use the absolute value.

     For example, a properly completed .bash_profile might look like this:

     ```
     export ORACLE_HOME=/u01/app/oracle/product/12.1.0.2/dbhome_1
     export ORACLE_SID=orcl
     PATH=$ORACLE_HOME/bin:$PATH
     export PATH
     ```
   - Save and close the .bash_profile file.
   - Execute the .bash_profile file for the variables to take effect.
5. Connect to the database using this command:

   ```
   sqlplus '/as sysdba';
   ```
6. Verify the code page setting of the Oracle database using this command:
   SELECT VALUE FROM NLS_DATABASE_PARAMETERS WHERE PARAMETER = 'NLS_CHARACTERSET';
7. If the character set is not **AL32UTF8**, you will have to reinstall the database using the correct parameter to set it.
8. Verify the Unicode code page setting of the Oracle database by executing this command:
   SELECT VALUE FROM NLS_DATABASE_PARAMETERS WHERE PARAMETER = 'NLS_NCHAR_CHARACTERSET';
9. If the setting is not **AL16UTF16**, you will have to reinstall the database using the correct parameter to set it.
10. Determine the number of DB processes available using this command:

    ```
    select limit_value from v$resource_limit where resource_name='processes';
    ```
11. If the value is less than 1500 (which is the minimum recommended for use with JD Edwards EnterpriseOne, run this command to set to the minimum recommended value:

    ```
    alter system set processes=1500 scope=spfile;
    ```
12. Check the value of the **filesystemio_option** parameter using this command:

    ```
    show parameter filesystemio_options;
    ```

13. If the value of the **filesystemio_option** parameter is not SETALL (which is required), use this command to set it:

    ```
    alter system set filesystemio_options=setall scope=spfile;
    ```

14. Shutdown the database using this command:

    ```
    shutdown immediate;
    ```

15. Start the database using this command:

    ```
    startup;
    ```

16. Verify the databaset is open using this command:

    ```
    select OPEN_MODE from v$pdbs where NAME = 'JDEORCL';
    ```

    If the pluggable database you want to use is not named **JDEORCL**, you can issue this command to find the name of available PDBs (ignore PDF$SEED) and substitute that name for **JDEORCL** in the command above):

    ```
    NAME, OPEN_MODE from v$pdbs;
    ```

17. If the **OPEN_MODE** is set to **READ WRITE** then the PDB is ready to be provisioned by the JD Edwards EnterpriseOne One-Click Provisioning Server.
18. If the **OPEN_MODE** is not **READ WRITE** then the PDB is not open. Open the PDB using this command:

    ```
    alter pluggable database JDEORCL open;
    ```

    The PDB is ready to be provisioned by the JD Edwards EnterpriseOne One-Click Provisioning Server.
19. Use this procedure to set the environment variables for the Oracle Database because by default environment variables for the oracle user are not set.
    - Switch to the **oracle** user using this command:

      ```
      sudo su – oracle
      ```

    - Edit the bash_profile using this command:

      ```
      vi .bash_profile
      ```

    - Add the following lines in the .bash_profile:

      ```
      export ORACLE_HOME=path

      export ORACLE_SID=ORCL

      PATH=path

      export PATH
      ```

      > **Note:** You cannot use an environment variable when defining ORACLE_HOME, such as $ORACLE_HOME. You must use the absolute value.

      For example, a properly completed .bash_profile might look like this:

      ```
      export ORACLE_HOME=/u01/app/oracle/product/12.1.0/dbhome_1

      export ORACLE_SID=orcl

      PATH=$ORACLE_HOME/bin:$PATH:$HOME/.local/bin:$HOME/bin

      export PATH
      ```

- Save and close the .bash_profile file.
- Execute the .bash_profile file for the variables to take effect.

Setting Up the Enterprise Server

This section shows you how to set up the Enterprise Server for JD Edwards EnterpriseOne with Linux.

Prerequisite

You must have performed the functions described in the module of this Learning Path entitled: **All Servers Common Setup**.

Setting Up the Enterprise Server

This section describes the setup tasks that must be performed on the Enterprise Server.

1. Ensure you have performed all the tasks described in the module of this Learning Path entitled: ***All Linux Servers Common Setup*** including the steps to create groups and users as well as assigning proper permissions to /u01.
2. Create the **oneworld** group using this command:

   ```
   sudo groupadd -g nnnn oneworld
   ```

   where `nnnn` is the id value with which the group will be created. You must use a free value which ideally should be above 1000. You can determine used group ids with the `id` command.

   > **Note:** You must reboot the machine any time you add groups in order for the changes to take affect.

3. Create the **jde920** user and make the KornShell the default shell (using the -s switch with /bin/ksh), using this command:

   ```
   sudo useradd -d /home/jde920 -m -s /bin/ksh jde920
   ```

   > **Note:** This specific user, with access to ksh, is required in order to start and stop the Enterprise Server.

4. Add the **jde920** user to the **oracle** and **oneworld** group using these commands:

   ```
   sudo usermod -a -G oracle jde920
   ```

   ```
   sudo usermod -a -G oneworld jde920
   ```

5. Ensure there is at least 35 GB free space on /u01.
6. Update `.bash_profile` of the **>root**, **opc**, and **oracle** users with below export values.

   > **Note:** This setting is required on the Oracle database target machine, which is the Enterprise Server, in order to enable the installation of the Oracle database client.

   ```
   sudo vi /root/.bash_profile
   ```

   ```
   export CV_ASSUME_DISTID=OL7
   ```

   ```
   sudo vi /home/opc/.bash_profile
   ```

```
export CV_ASSUME_DISTID=OL7

sudo vi /home/oracle/.bash_profile

export CV_ASSUME_DISTID=OL7
```

Setting Up the WebLogic Server

This section shows you how to set up the WebLogic Server for JD Edwards EnterpriseOne.

Prerequisite

You must have performed the functions described in the module "All Servers Common Setup" of this Learning Path.

General

> **Note:** The deployment of the JDK using One-Click Provisioning Console removes the string **anon, NULL** from the property **jdk.tls.disabledAlgorithms** in the file `\jre\lib\security`.

These are the prerequisites for Oracle WebLogic Server:

1. Ensure that you have performed all the tasks described in module "All Linux Servers Common Setup" of this Learning Path including the steps to create groups and users as well as assigning proper permissions to `/u01`.
2. Use this command to ensure that the `/u01` mount point has proper permissions to allow the One-Click Provisioning process to subsequently create the requisite folders:

   ```
   sudo chmod 770 /u01
   ```
3. Ensure the user with which Oracle WebLogic Server was installed is part of the **oracle** group. Use this command to verify:

   ```
   groups username
   ```

Install Oracle WebLogic Server and a JDK

You must manually pre-install Oracle WebLogic Server (WebLogic Server) and a JDK for use by WebLogic Server.

> **Note:** You must ensure that the JDK is installed under the /u01 mount point. Further you must ensure that the JDK is installed by the same user that has been or will be used to install the WebLogic Server. For example, if you use the **oracle** user to install the JDK, you must use the **oracle** user to install the WebLogic Server, or vice versa depending on the order you install these products.

You can then use JD Edwards One-Click Provisioning to deploy the JD Edwards EnterpriseOne web components into the pre-installed WebLogic Server domain. Refer to the Oracle Certifications for JD Edwards EnterpriseOne One-Click Provisioning for details on the supported versions of WebLogic Server.

The complete list of prerequisites is provided below:

- A supported version of WebLogic Server must be pre-installed.

The password must be 8 to 30 characters long, must contain at least one number, and optionally any number of either the Pound Sign (#) or Underscore (_) special characters.

> **Note:** The password for any WebLogic Server user *cannot* contain these special characters:Dollar Sign ($) Exclamation Mark (!) Ampersand (&) Using any of the above special characters violates the Oracle Cloud password policy and will result in denied access.

- A supported JDK version must be installed.
- WebLogic Server must be defined with at least one domain.
- WebLogic Server must be in a running state and able to connect to the Admin Console.
- WebLogic Server must have a running Node Manager process for the existing domain.
- WebLogic Server must be installed as a user that is part of the **oracle** group.

Post Installation Tasks for WebLogic Server

After you have installed the WebLogic Server, prior to using the Provisioning Console for JD Edwards EnterpriseOne, you must manually configure WebLogic Node Manager to disable SSL. Otherwise the provisioning will fail.

1. Locate the nodemanager.property file which is typically found in this location:

   ```
   <ORACLE_HOME>/user_projects/domains/<DOMAINNAME>/nodemanager/nodemanager.properties
   ```

2. Edit the nodemanager.property file to set this property to disable SSL:

   ```
   SecureListener=false
   ```

3. Save the nodemanager.property file.
4. You must set the listen address must be set exactly same as value of **ListenAddress** property of nodemanager.properties file. You must set the listen port 5556, which is non-secure (instead of 5557, which is secure) in both Node Manager properties file and in node manager using the WebLogic Server user interface. For instructions refer to this procedure: *Changing the Oracle HTTP Server Listen Ports.*
5. Restart the WebLogic Node Manager for the setting to take effect.

Ensure WebLogic Server is Patch Current

Refer to the Oracle Certifications for One-Click for WebLogic Server to verify that the latest available patches are applied. Such patches can affect the ability of One-Click Provisioning to deploy web components into the WebLogic Server.

5 Configuring the Microsoft Windows Deployment Server

Running Commands to Change Microsoft Windows Settings

This section shows you how to run commands to change Microsoft Windows settings.

Prerequisites

- You must have access to a physical or virtual Windows machine dedicated for use as a JD Edwards EnterpriseOne Deployment Server.
- You must be able to connect to the Microsoft Windows machine using a Remote Desktop Protocol (RDP) session from a Microsoft Windows client machine.

Enable Remote Command Execution Through Microsoft PowerShell

From Microsoft PowerShell, use this command to enable remote command execution:

```
winrm quickconfig -q
```

Enable Inbound Ports in the Firewall

If you have the Microsoft Windows firewall enabled for any profile (public, private, default), which is recommended, in order for One-Click Provisioning to deploy to the Deployment Server and for JD Edwards EnterpriseOne runtime to function properly, you will need to explicitly open Inbound and Outbound ports.

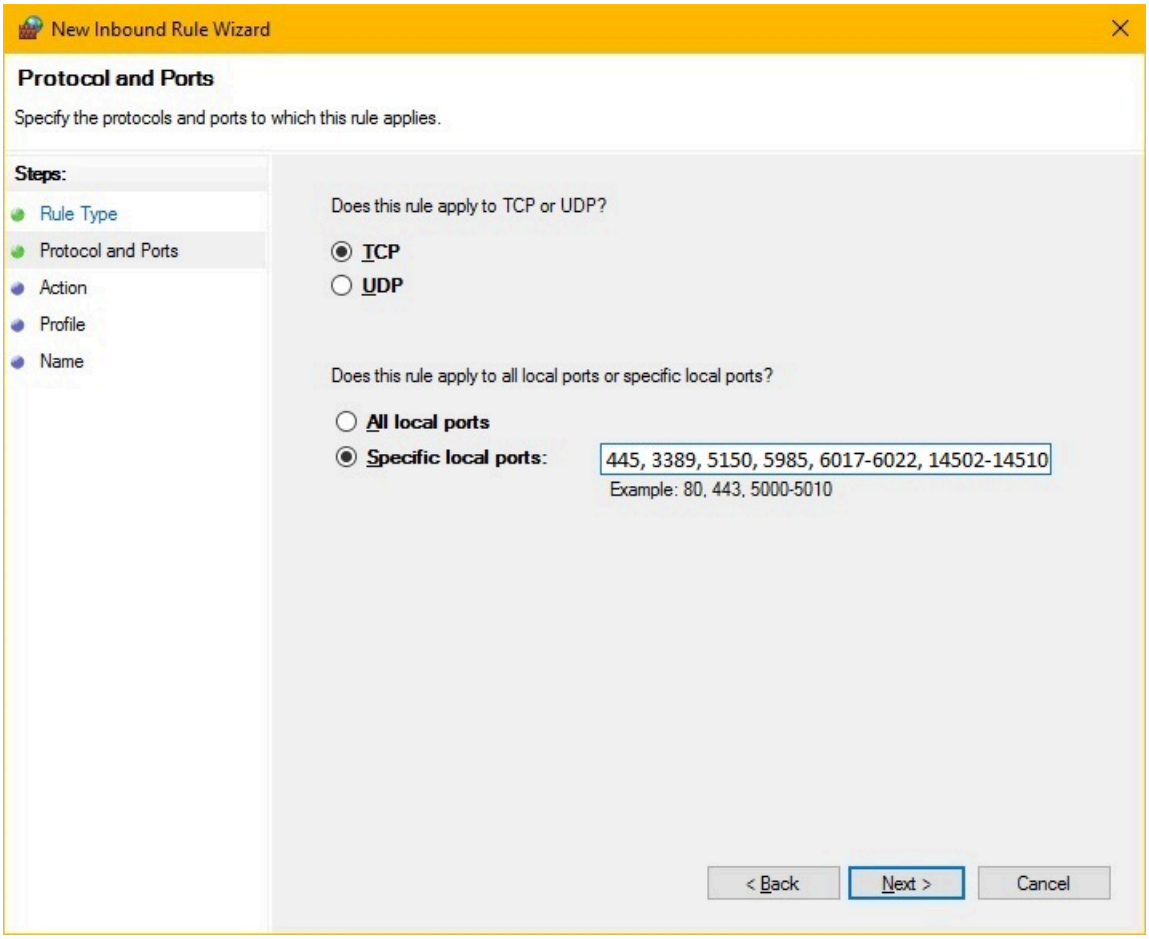
Use this procedure to open the Inbound ports for **each** Microsoft Windows instance.

1. Go to Administrative Tools > Windows Firewall with Advanced Security.
2. In the left pane, highlight **Inbound Rules**.
3. In the right pane, Actions, Inbound Rules, click **New Rule** ...
4. On Rule Type, select the **Port** radio button as the type of rule to create.
5. Click the **Next** button.
6. On Protocol and Ports:
    - You can accept the default value of **TCP** for the protocol to which this rule applies.
    - Choose the radio button for **Specific local ports** and, for ***each*** Windows Server, enter each of the ports shown in the following table, separated by a comma.

Windows Server Firewall Port List	
Component	**Inbound Ports to Open**
Deployment Server	445 3389

	5150 5985 6017-6022 14502-14510

The following example shows the ports you should specify for the Deployment Server.



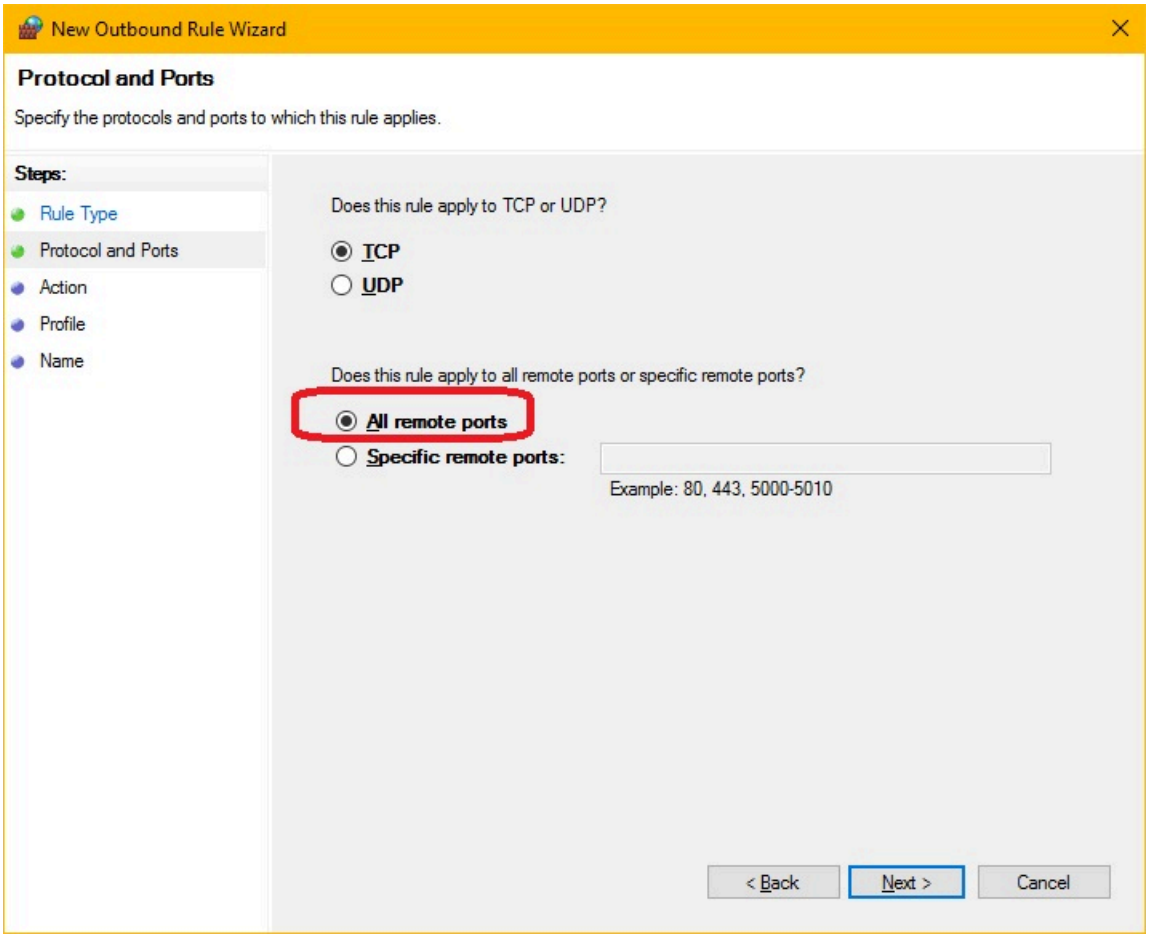
7. Click the **Next** button.
8. On Action, you can accept the default value which is **Allow the connection**.
9. Click the **Next** button.
10. On Profile, select all firewall profile options **(Domain, Private, Public)**.
11. Specify a name for the rule. For example, **JDESMC_RDP**.
12. Click the **Finish** button to save the rule and exit the wizard.

Enable Outbound Ports in the Firewall

If you have the Microsoft Windows firewall enabled for any profile (public, private, default), which is recommended, in order for One-Click Provisioning to deploy to the Deployment Server and for JD Edwards EnterpriseOne run-time to function properly, you will need to explicitly open Inbound and Outbound ports.

Use this procedure to open the Outbound ports in your Microsoft Windows instance.

1. Go to Administrative Tools > Windows Firewall with Advanced Security.
2. In the left pane, highlight **Outbound Rules**.
3. In the right pane, Actions, click **New Rule** ...
4. On Rule Type, select the **Port** option as the type of rule to create.
5. Click the **Next** button.
6. On Protocol and Ports:
    - You can accept the default value of **TCP** for the protocol to which this rule applies.
    - Choose the option for **All remote ports**.



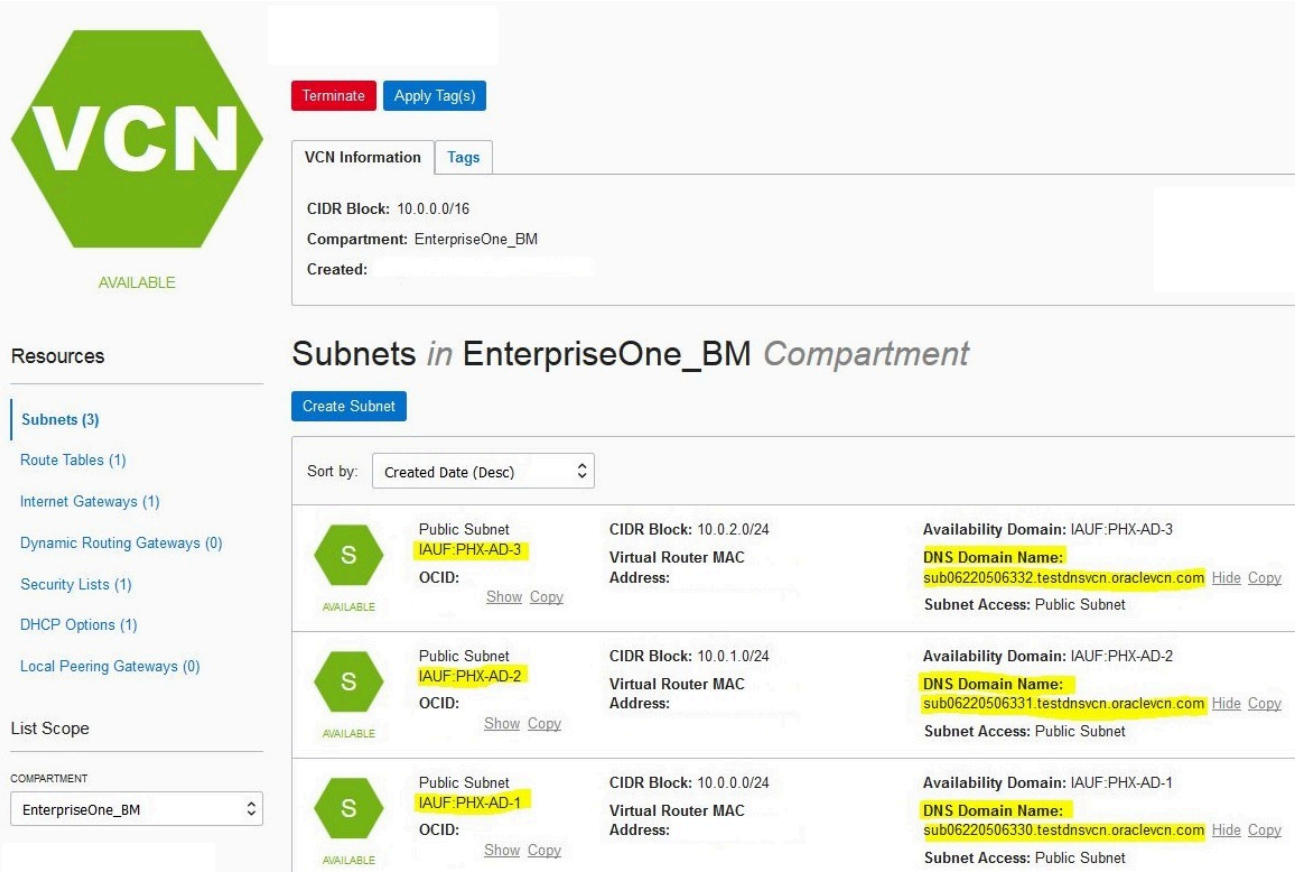
7. On Action, you can accept the default value which is **Allow the connection**.
8. Click the **Next** button.
9. On Profile, select all firewall profile options **(Domain, Private, Public)**.
10. Specify a name for the rule.

11. Click the **Finish** button to save the rule and exit the wizard.

Configure Settings for Ethernet Connections

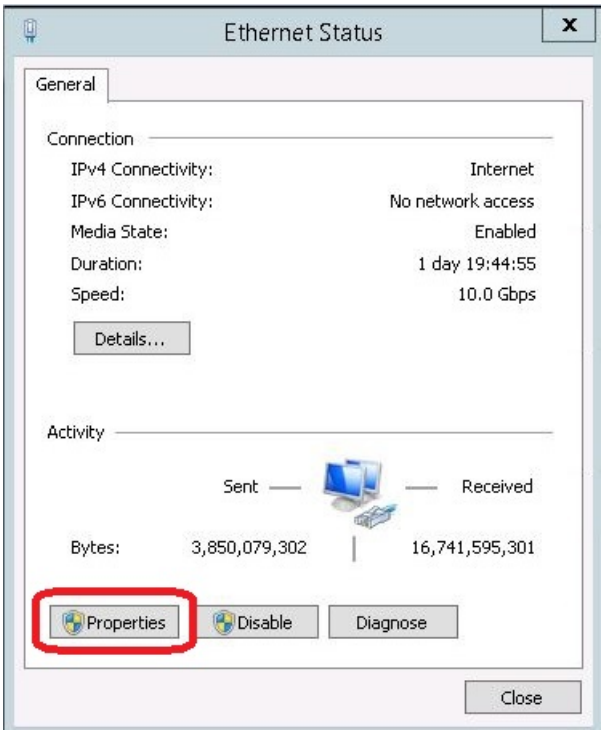
You must configure settings for Ethernet connection to specify the domain name of the Domain Name System (DNS) for the Availability Domain to which all JD Edwards EnterpriseOne servers belong.

For example, if your subnets look like that shown in the example below, you must configure your Network Settings using this procedure:



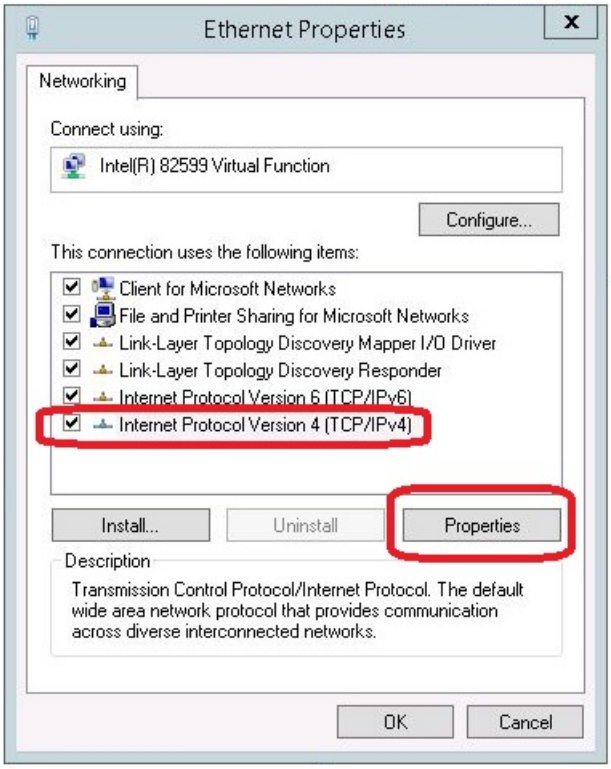
1. Open **Network and Sharing Center**.

2. On Ethernet settings, in Network > Connections, click **Ethernet** to open **Ethernet Status**.

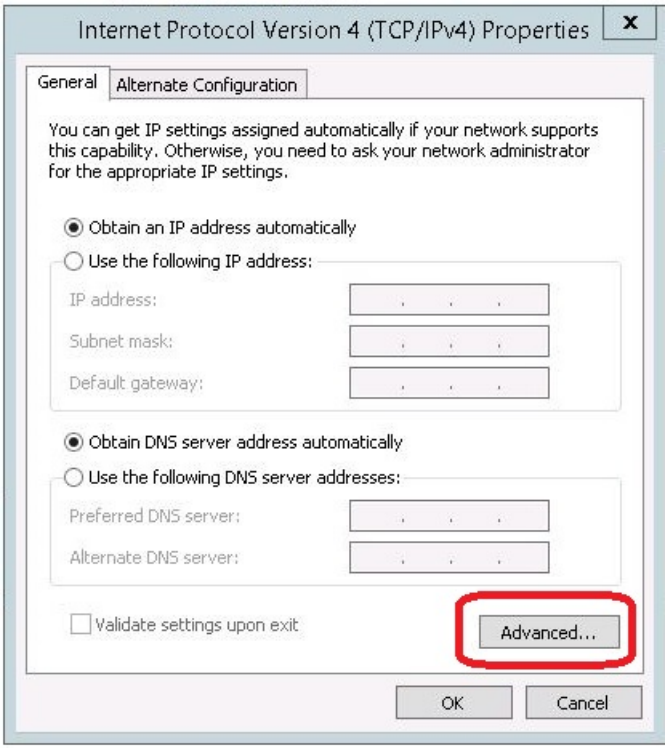


3. On Ethernet Status, click the **Properties** button.

4. On Ethernet Properties, highlight this line: **Internet Protocol Version 4 (TCP/IPv4)** and click the **Properties** button.



5. On Internet Protocol Version 4 (TCP/IPv4) Properties, click the **Advanced** button.

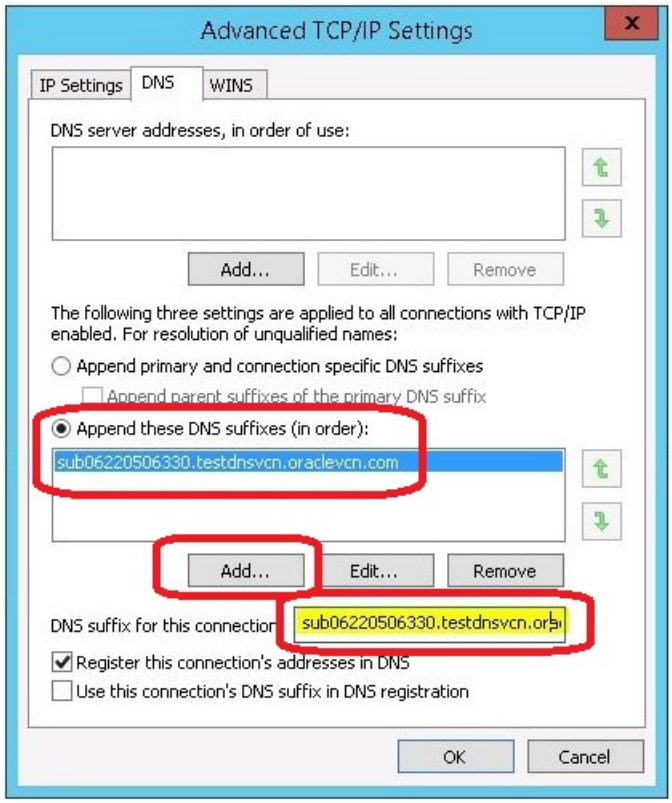


6. On Advanced TCP/IP Settings, click to enable this option: **Append these DNS suffixes (in order):** and click the **Add** button.
7. On the TCP/IP Domain Suffix dialog, enter the value of the DNS Domain Name for your Availability Domain. For example, assuming your subnets were as shown in the preceding screen showing the subnets for each Availability Domain and all servers are created in **sub0622506330.testdnsvcn.oraclevcn.com** subnet, you would enter this value for the suffix:

   ```
   sub0622506330.testdnsvcn.oraclevcn.com
   ```

8. Click the **Add** button to add the DNS suffix.

9. Add this same subnet (in this example, **sub0622506330.testdnsvcn.oraclevcn.com**) in the field labelled **DNS suffix for this connection**.



10. Click the **OK** button to accept the values and exit the **Network and Sharing Center**.

Change Security Option

If you chose a user other than **opc** when for the One-Click Provisioning deployment of your Deployment Server, use this procedure to change the Microsoft Windows security option so that user will be recognized by JD Edwards EnterpriseOne.

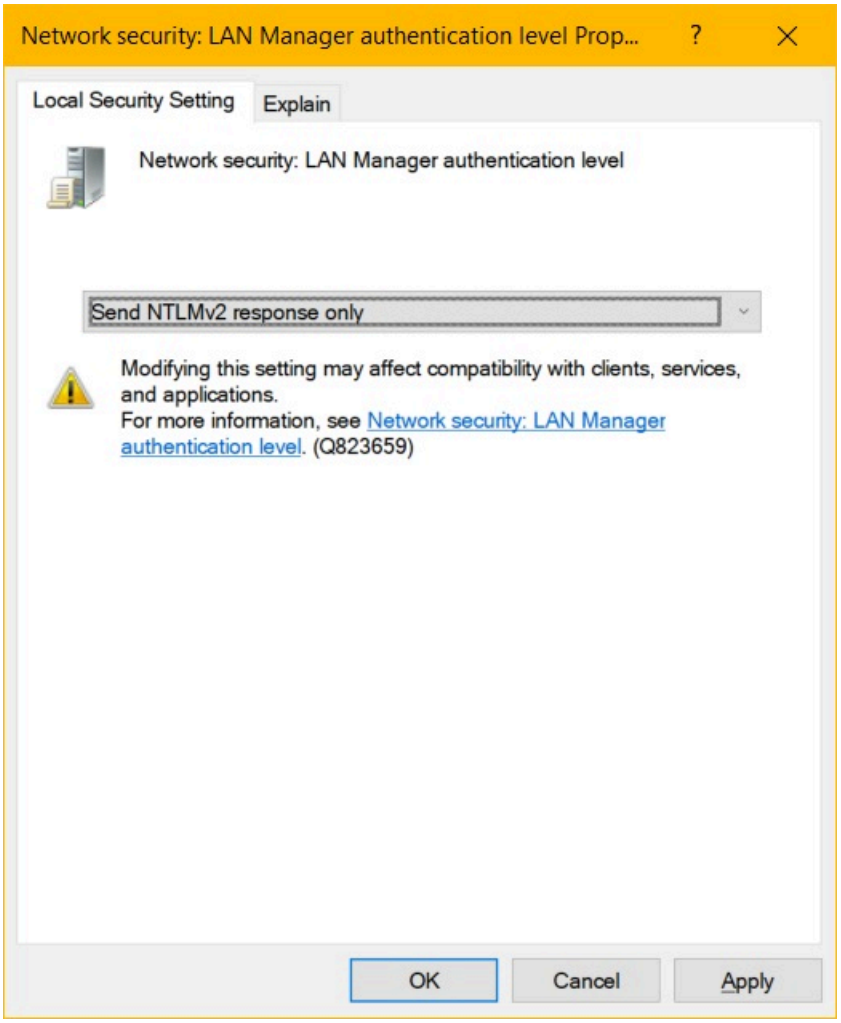
1. Log in to the Deployment Server as the user you configured, which is other than the **opc** user.
2. Open the Microsoft Windows **Local Security Policy** program from Start > Run, or from a Command Prompt:

   ```
   secpol.msc
   ```
3. On Local Security Policy, navigate to Local Policies > Security Options.
4. Locate and edit this setting:

   Network Security: LAN Manager authentication level

5. Use the pulldown to select this setting:

   Send NTLM V2 response only



6. Click the **Apply** button to save the setting.

Change the Maximum Transmission Unit (MTU) Setting

The recommended MTU setting is 1500. Use this procedure to check, and if necessary, change the current MTU setting.

1. Open Windows PowerShell as Administrator and run the following command (as a single contiguous line) to check the current value of the MTU setting:

```
Get-NetIPInterface | where {($_.InterfaceAlias -eq "Ethernet") -and ($_.AddressFamily -eq "IPv4") -and
($_.NlMtu -Gt 0)}
```

2. If the returned value is not set to 1500, run this command (as a single contiguous line) to set the MTU value to 1500:

```
Get-NetIPInterface | where {($_.InterfaceAlias -eq "Ethernet") -and ($_.AddressFamily -eq "IPv4") -and
($_.NlMtu -Gt 0)} | Set-NetIPInterface -NlMtuBytes 1500
```

Allocating Disk Space

You must ensure that the disk space you allocate for the Deployment Server is allocated to a single drive, which can only be one of these:

- **C:**
- **D:**
- **Z:**

6 Using the One-Click Provisioning Server

Configuring CA Certificates for One-Click UI (Optional)

This section shows you how to configure CA Certificates for the One-Click User Interface. This task is optional.

JD Edwards EnterpriseOne One-Click Provisioning can be configured with a supplied CA certificate. However, after initial installation you must obtain your own CA certificates. These must be certificates that are verified by a verified CA authority such as Entrust and Symantec Corporation.

Prerequisite

You must obtain CA certificates and their chain of deliverables.

Configuring CA Certificates for One-Click UI (Optional)

Use this procedure to configure CA certificates for the One-Click Provisioning user interface. This step is not required for initial installation but is required for subsequent usage of JD Edwards EnterpriseOne in Oracle Cloud Infrastructure.

1. Combine the the contents of `rootca.pem` and `intermediateca.pem` certificates to a file named `ca-cert.pem` file as per order from the CA authority.
2. Rename `.net.key` to `key.pem`.
3. Rename `<variable>.crt` to `cert.pem`.
4. Copy `ca-cert.pem`, `key.pem` and `cert.pem` to this directory:

   ```
   /E1CloudConsole/keys
   ```
5. Restart the Provisioning Server:
   - **Linux-based Provisioning Server**

     Restart the E1CloudConsole.service using following command:

     ```
     sudo systemctl stop E1CloudConsole.service sudo systemctl start E1CloudConsole.service
     ```
   - **Microsoft Windows-based Provisioning Server**

     Use these steps to restart the user interface:

     - Navigate to this directory:

       ```
       \JDE\bin
       ```
     - Open Powershell with Administrator rights.
     - Run this script:

       ```
       .\E1CloudConsoleWin.ps1
       ```

Accessing the JD Edwards Provisioning Console

This section shows you how to access the JD Edwards Provisioning Console.

As described in the subsequent OBEs in this Learning Path, you will use the JD Edwards One-Click Provisioning Console to set up a completely functional EnterpriseOne environment by performing these three steps:

1. Configure – Provide the Server Manager details.
2. Orchestrate – Create the deployment plan.
3. Deploy – Initiate the scripts for the automated provisioning of the EnterpriseOne system.

Prerequisite

To access the Provisioning Console, you must use a supported browser.

The recommended browsers for accessing the One-Click Provisioning Console are:

- Google Chrome
- Mozilla Firefox

Open the browser and connect to the URL using this syntax:

```
https://XXX.XXX.XXX.XXX:3000
```

Where:

- **https** is the only supported browser protocol.
- **XXX.XXX.XXX.XXX** is the public IP address for the One-Click Provisioning Server instance.
- **3000** is the port on which the One-Click Provisioning Server is running, and which you must include as part of the address.

> **Note:** Should you exit the Provisioning Console or experience a timeout, the next time you enter the Provisioning Console, it displays the point where you left off. When you click the **Configure** icon, you will be prompted for the same credentials that you entered during your first access to the One-Click Provisioning Console.

Configuring the Server Manager Account

This tutorial shows how to configure the Server Manager account in JD Edwards One-Click Provisioning Console.

Configuring the Server Manager Account

Configuring the Server Manager Account

This section shows how to configure the Server Manager account in JD Edwards One-Click Provisioning Console.

If you are a new user, you are required to change the administrator passwords for WebLogic Server and Server Manager Console. Remember the Server Manager password you entered in the Change Password window for future logins.

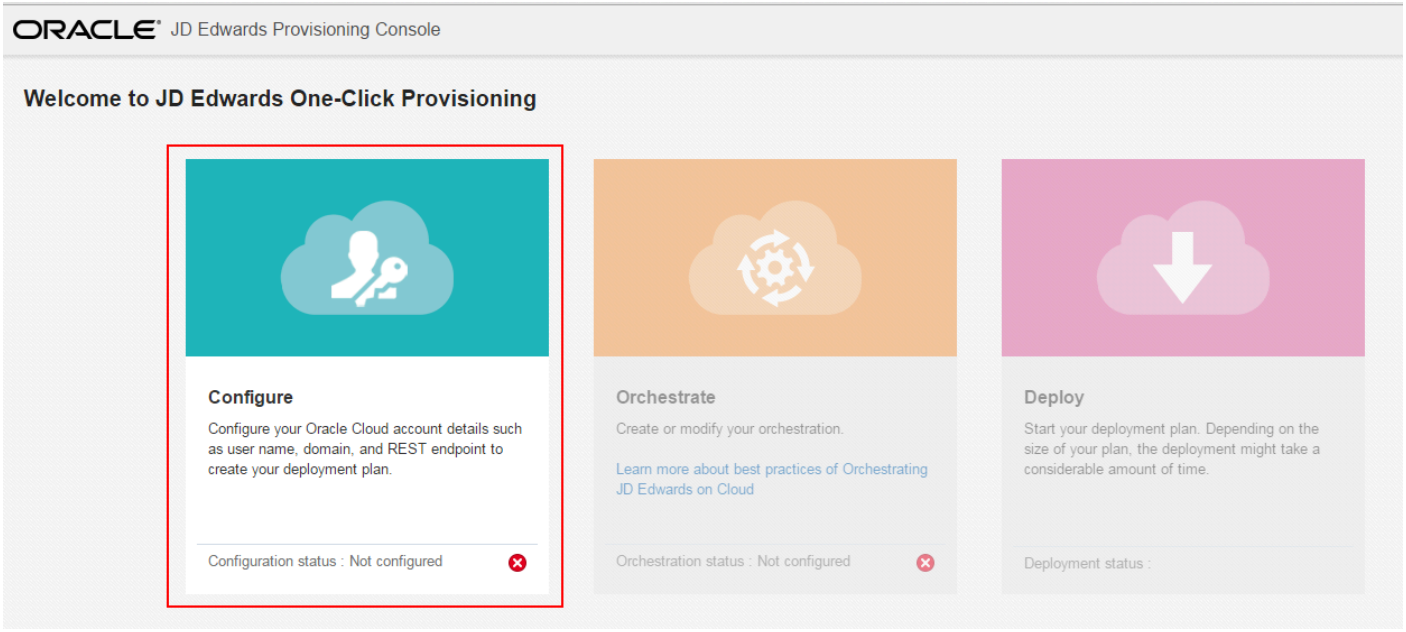
Prerequisite

Downloaded the One-Click archive files from the Oracle Software Delivery Cloud (also called OSDC or E-Delivery). For more information see the section entitled: ***Setting Up the Provisioning Server*** .

Configure the Server Manager Account

Use this procedure to provide the account information.

1. On Welcome to the JD Edwards Provisioning Console, click the **Configure** icon.



2. If you are a new user, as prompted by the JD Edwards Provisioning Console, you are also required to change the administrator passwords for WebLogic Server and Server Manager Console.

   On Change Password, enter the passwords for the Server Manager Administrator. The password must only have numbers, alphabets, and special characters (@,!,$,_,#), and is between 8 and 30 characters long.

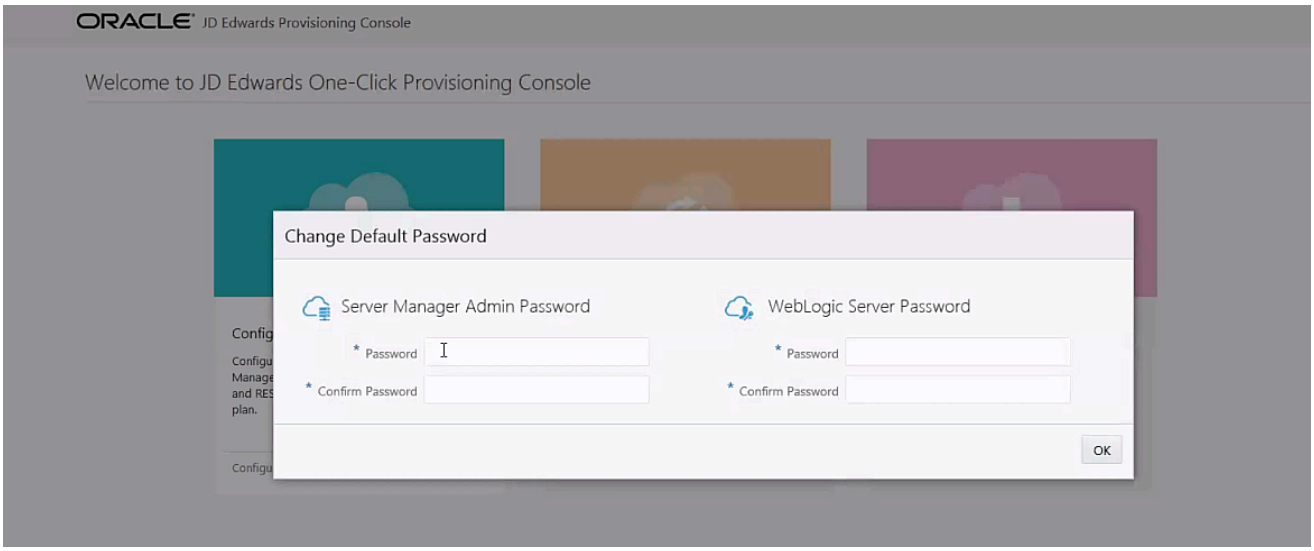
   Also, enter the password for the WebLogic Server. The password must start with a letter, is between 8 and 30 characters long, contains at least one number, and optionally, any number of special characters (#,_). For example, Ach1z0#d

   > **Note:** The password for any WebLogic Server user cannot contain the $ or ! character. Using either of these characters violates the Oracle password policy and will result in denied access.

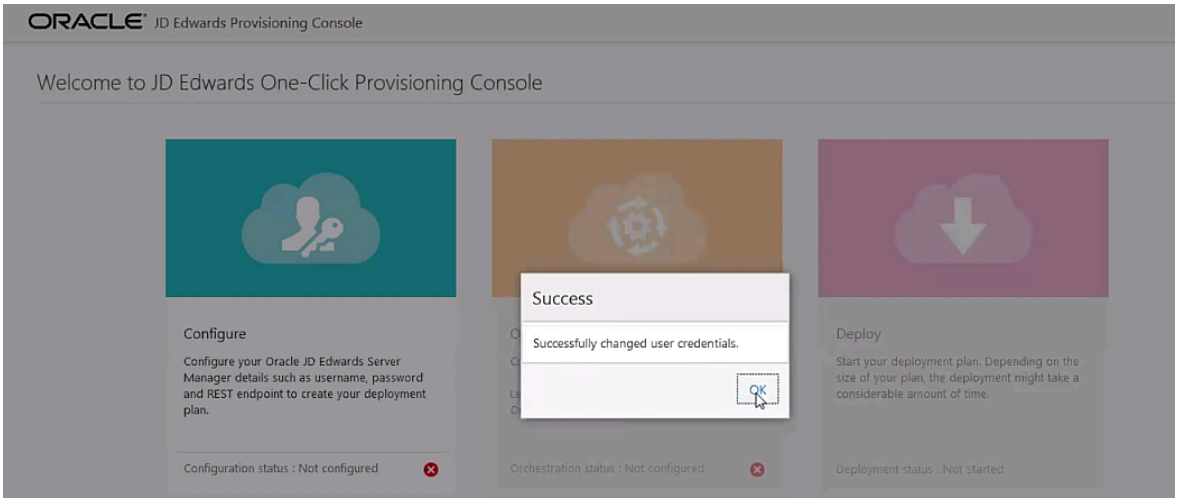
   > **Tip:** Valid values for the passwords are displayed in the tooltip when you click the field.

   Click the **OK** button.

   > **Note:** The system displays a message indicating that is changing default passwords; this may take a few minutes to complete before the next screen is displayed.

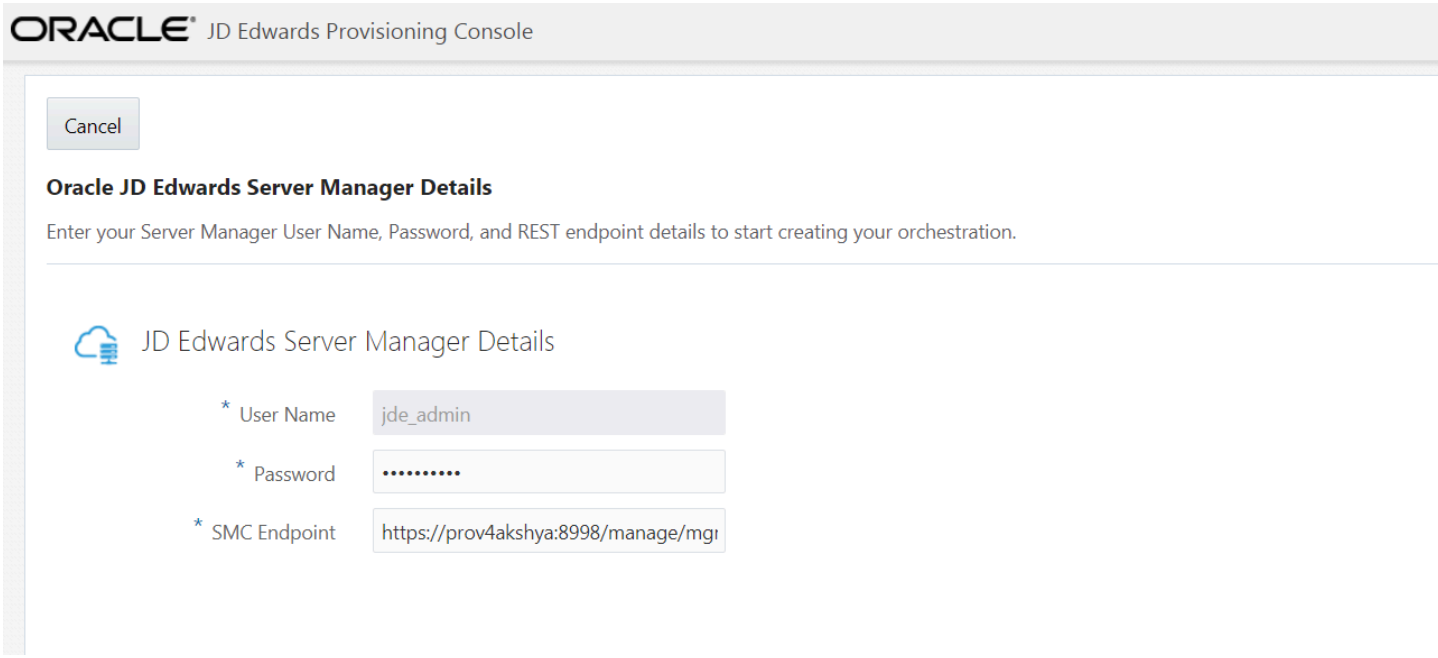


3. On the Success window, click the **OK** button.



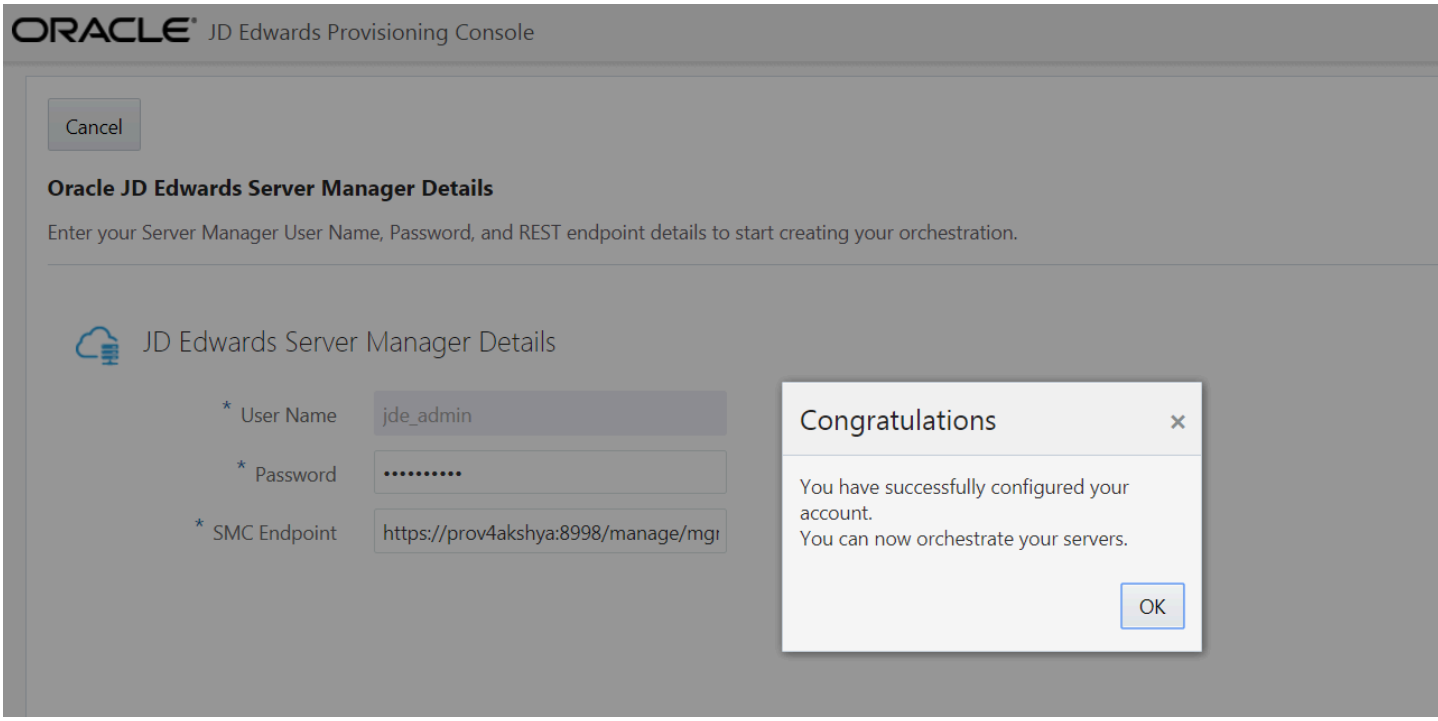
4. On Oracle JD Edwards Server Manager Details, reenter the Admin password for the Server Manager Console. The SMC Endpoint is pre-populated automatically.

> **Note:** It is recommended that you record this value on the Pre-Install Worksheet, which you created as described in the companion document to this tutorial in the section entitled: Create the **Pre-Install Worksheet**.



5. Click the **Save Configuration** button.

   The system will take some time to authenticate the Server Manager Endpoint and Credentials. When the authentication is verified, click the **OK** button on the **Congratulations** box.


ORACLE JD Edwards Provisioning Console
Cancel
Oracle JD Edwards Server Manager Details
Enter your Server Manager User Name, Password, and REST endpoint details to start creating your orchestration.
JD Edwards Server Manager Details
* User Name
jde_admin
* Password
* SMC Endpoint
https://prov4akshya:8998/manage/mgr
Congratulations
You have successfully configured your account.
You can now orchestrate your servers.
OK

7 Creating a Deployment Plan

Orchestrating a Quick Start Deployment Plan

This tutorial

Orchestrating Using Quick Start Mode

This section shows you how to orchestrate a basic Deployment Plan using the Quick Start mode. For performance reasons, an orchestration using the Quick Start mode alone is not recommended for Production environments.

Use the Quick Start mode in the JD Edwards One-Click Provisioning Console to create a deployment plan that includes all the core components of JD Edwards EnterpriseOne, which will be deployed exclusively on Oracle Cloud Infrastructure.

Refer to the OBE "Fundamentals" of this Learning Path for a description of the various servers that can be deployed by One-Click Provisioning.

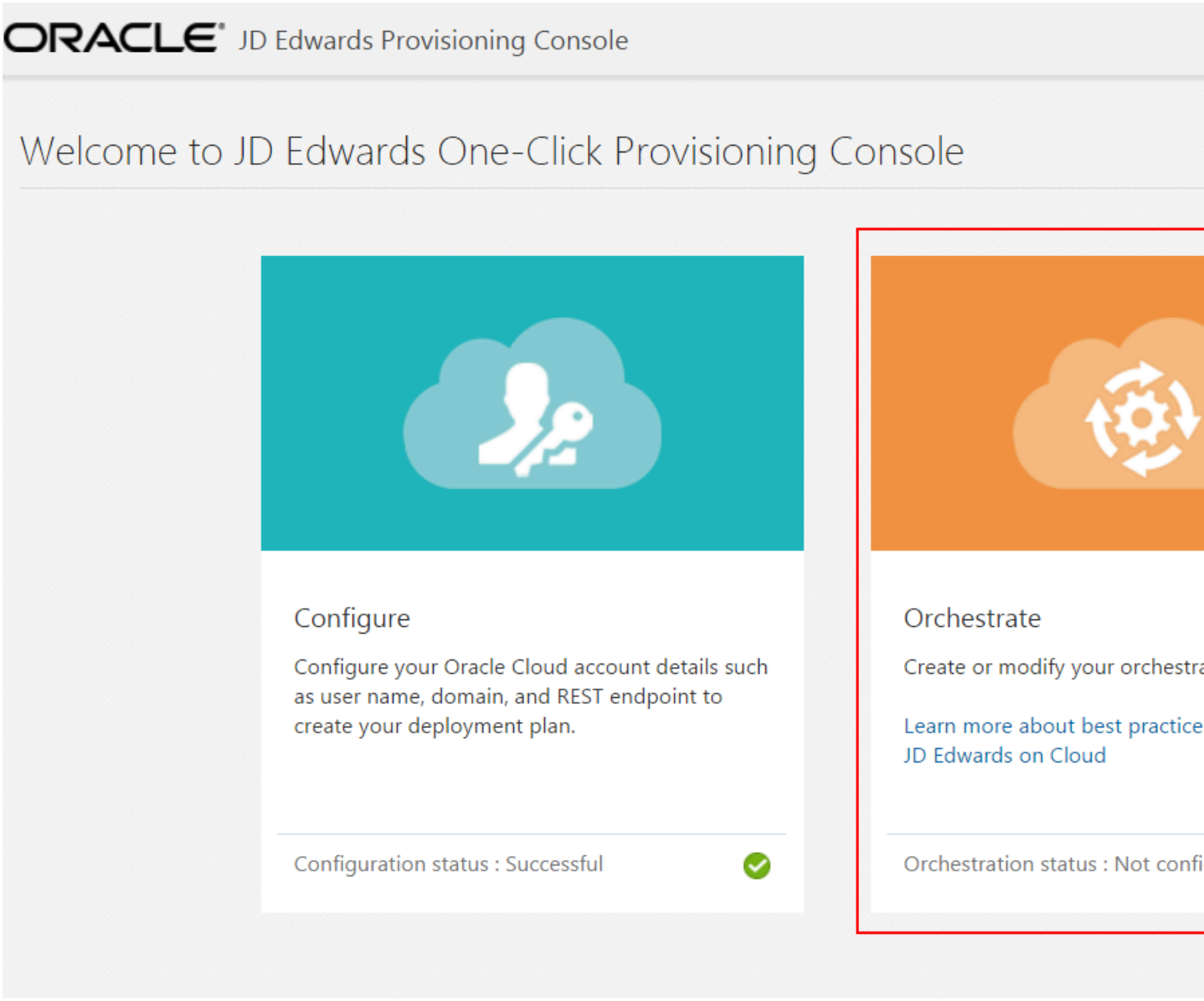
Prerequisite

You must have configured the administrator passwords for the WebLogic Server and the Server Manager Console in the Configure section of the JD Edwards One-Click Provisioning Console.

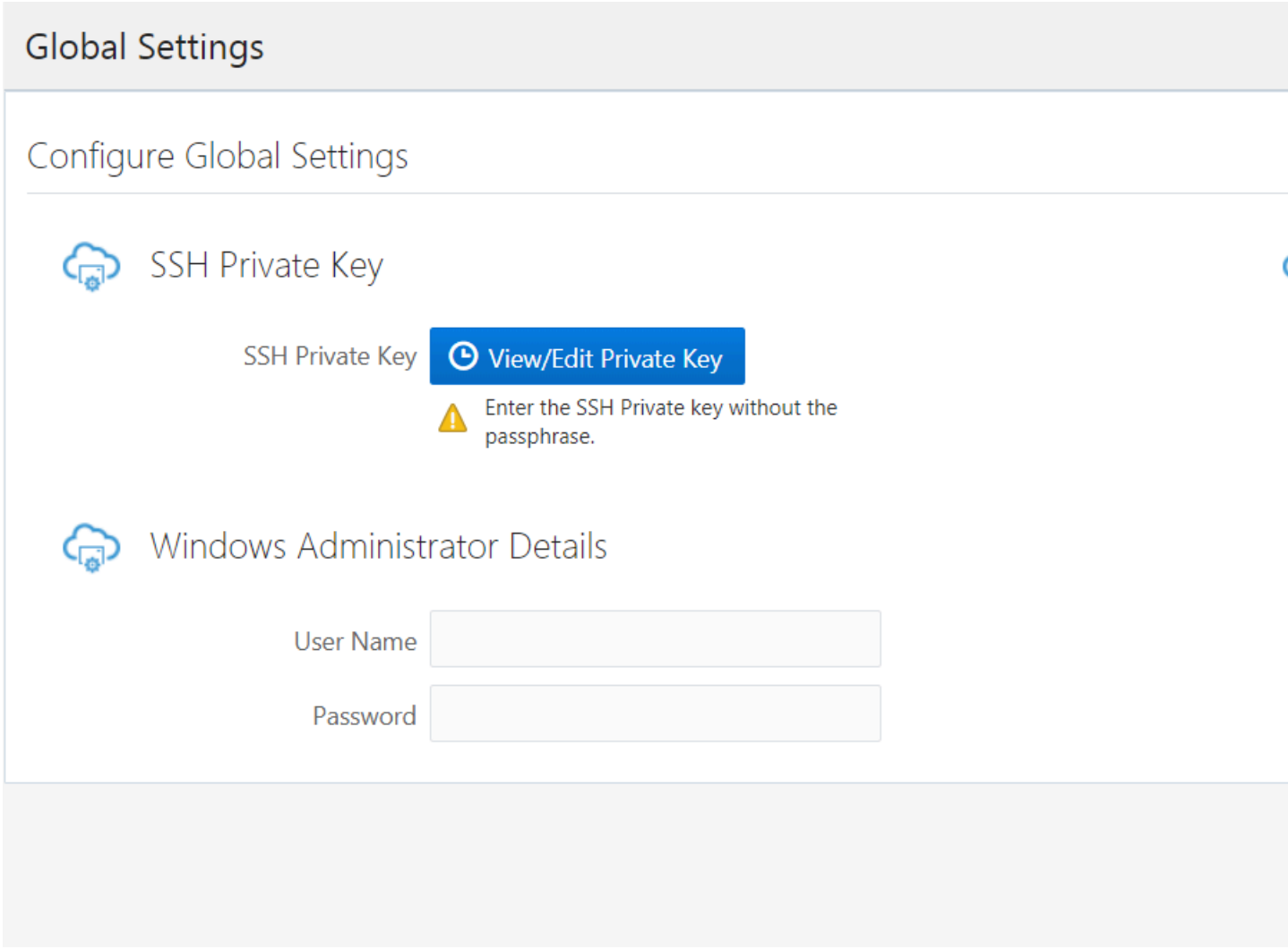
Orchestrating a Quick Start Deployment Plan

To orchestrate a Quick Start deployment plan:

1. On Welcome to the JD Edwards Provisioning Console, click the **Orchestrate** icon.



2. If this is the first pass through a JD Edwards One-Click Provisioning orchestration, the following Global Settings screen will appear first. In the **SSH Private Key** section, click the **View/Edit Private Key** button.



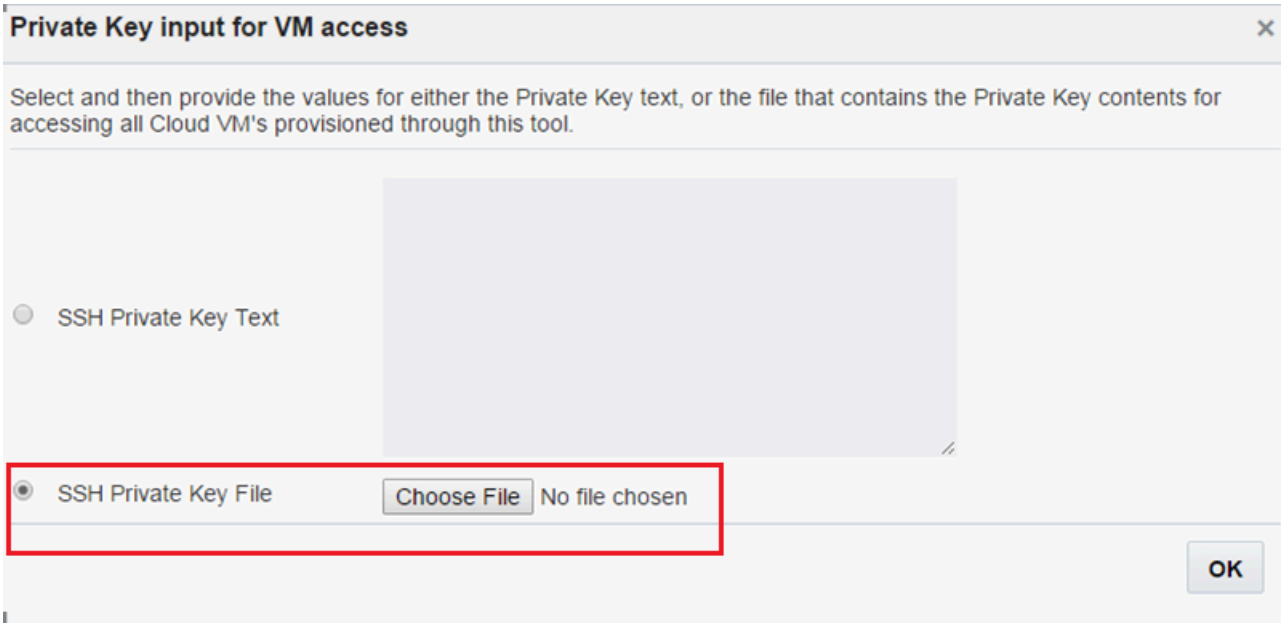
3. On the **Private Key input for VM access** dialog box, you must either specify the SSH private key text, or browse and select the file that contains the SSH private key contents for accessing all the instances that are provisioned using this tool.

> **Note:** Ensure the uploaded file is in the legacy `.openssh` format which is supported in One-Click Provisioning. For Example: `oci_Instance.openssh`.

> **Note:** The private key in the legacy `.openssh` format starts with `-----BEGIN RSA PRIVATE KEY-----` and ends with `-----END RSA PRIVATE KEY-----`. While the new format starts with `-----BEGIN OPENSSH PRIVATE KEY-----` and ends with `-----END OPENSSH PRIVATE KEY-----`.

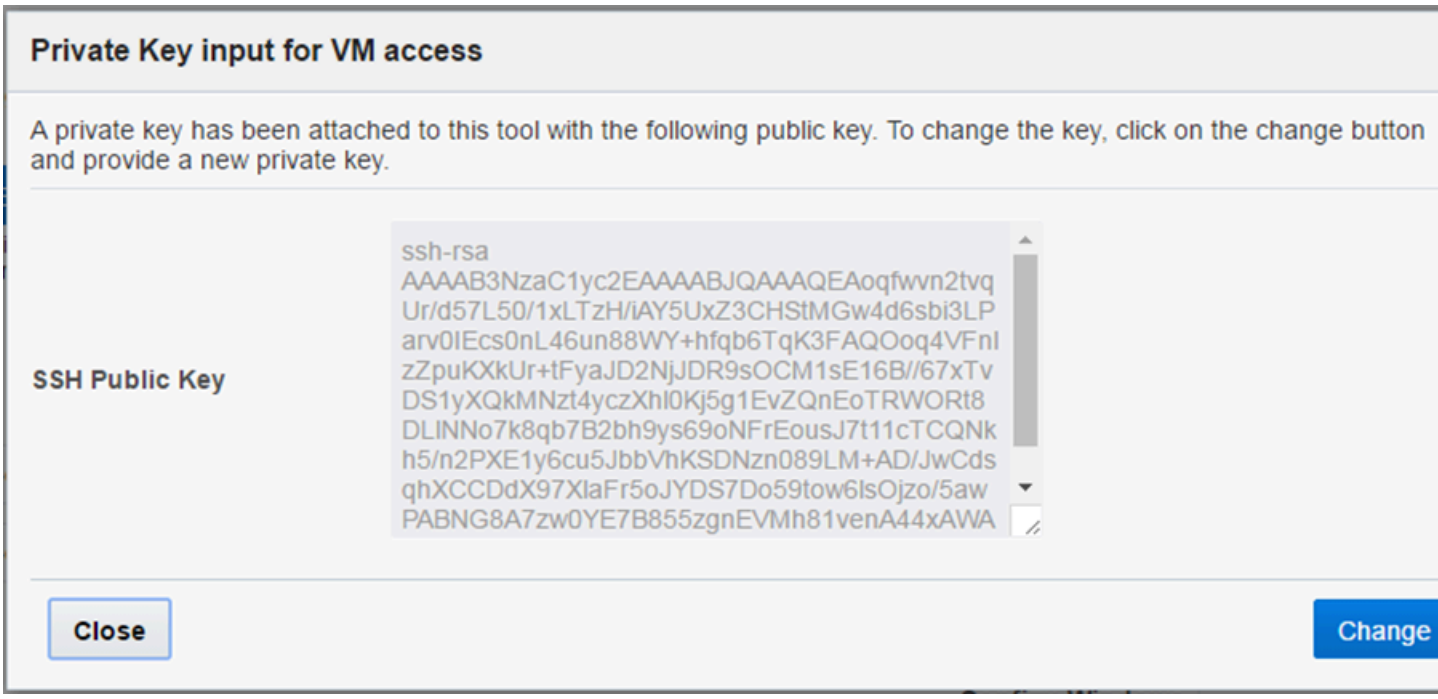
To browse and select the file, select the **SSH Private Key File** option and then click the **Choose File** button. For more information regarding SSH Keys, refer to the section "*Generating Secure SHell (SSH) Key Pairs*."

> **Note:** Ensure that the SSH Private Key Text field is not blank. The One-Click Provisioning Console validates the private keys and you cannot save the Global Settings if this field is blank.



4. Browse and select the appropriate file, and then click OK.

> **Note:** If you click the **View/Edit Private Key** button again, you can see the **Public Key for VM access** window with the SSH Public Key value in the **SSH Public Key** text field. To change the private key, click the **Change** button and provide the new value.



5. Click the **Close** button.
6. In the Windows Administrator Details section, enter the Windows user name and password. Ensure that the user name is entered as `opc` and that this user has the administrative privileges.

> **Note:** You must enter the same password for this Windows Server that you previously specified in the section "*Logging in to the Windows VM*" of this Learning Path.

7. In the Set EnterpriseOne Passwords section, enter and then confirm these passwords:
    - **JDE User Password**

      Create the password for JD Edwards EnterpriseOne. In support of the long password functionality, the password must be between 12 and 30 characters. It can contain only alphanumeric characters, and can only include this special character: _ (underscore).
    - **Site Key Passphrase**

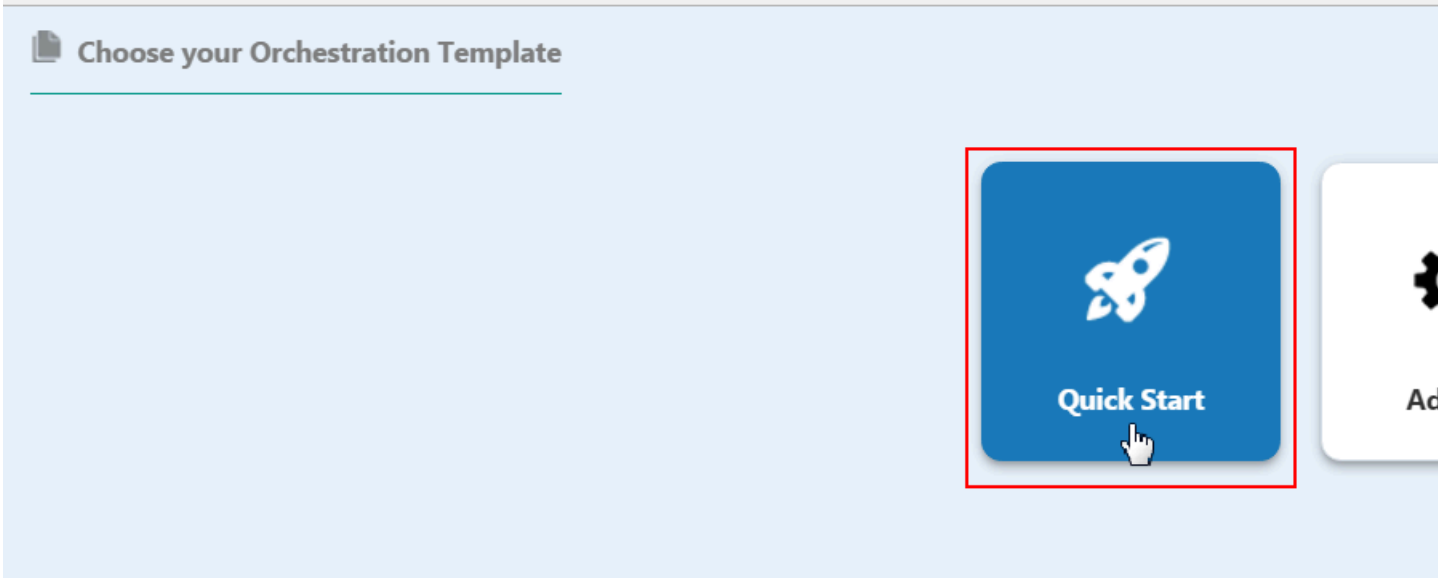
      Enter the passphrase for generating the site key. The passphrase must start with a letter, end with an alphanumeric character, must be between 8 and 40 characters, and contain at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 underscore characters.

> **Tip:** The conditions to set the passwords appear in a tooltip when you click the fields.

> **Note:** It is highly recommended that you keep a record of these critical passwords. If you have not already done so, you should record these values in the Preinstallation Worksheet.

8. Click the **Save** button to exit the Global Settings screen.
9. On the Choose your Orchestration Template window, click the **Quick Start** icon to create your Quick Start JD Edwards Deployment Plan.

> **Note:** Refer to the applicable OBEs of this Learning Path for instructions on using the Advanced mode, and Export and Import orchestration functions.



10. On Database Server Instance page, complete these fields to create and configure the Database Server instance.

Server Configuration

- *Database Server Type*

  The Database Server Type is populated by default as Oracle Database.
- *ATP-D*

  You should only enable the ATP-D option if you are using an Oracle Autonomous Database Dedicated; this database is only supported in Oracle Cloud Infrastructure. This functionality is described in the

Learning Path "Deploying JD Edwards EnterpriseOne on Oracle Cloud Infrastructure on Linux with Autonomous Database."

- *Platform*

  This field is disabled and it is automatically populated as Linux.
- *Instance Name*

  Create an instance name for your database instance.
- *Host Name*

  Enter the host name.

Database Configuration

- *DB Install Path*

  Enter the DB installation path.
- *DB Admin Password*

  Enter the password of the database administrator.
- *Net Service Name*

  Enter the net service name.

JD Edwards Database Configuration

- *Use ASM feature*

  Enable this option if you are using RAC DB as your Database Server.

  If you disable ASM in your Orchestration, you must enter valid values for the install, table, and index directories for your Oracle database. For example:

  - `/u01/DataDB`
  - `/u01/ORATABLE`
  - `/u01/ORAINDEX`

  If you enable ASM in your Orchestration, you must enter valid values for your DISK group. By default the values for are assumed to be DATA. Otherwise, you can enter any other name that you have created. An example screen is shown below as Database Server Instance - ASM Enabled.
- *JDE DB Install Directory*

  Enter the installation path.

  Path Rules: All directories in the specified path must preexist, ***except*** the last directory in the path. Therefore you must manually create the directory structure except for the last directory, which the Provisioning Server deployment process creates. For example, if you specify /u01/ORCL/INSTALL,

the /u01/ORCL directory must preexist and the Provisioning Server deployment creates the /INSTALL directory.

- *JDE DB Table Directory*

  Enter the path to install the table data.

  Path Rules: All directories in the specified path must preexist, ***except*** the last directory in the path. Therefore you must manually create the directory structure except for the last directory, which the Provisioning Server deployment process creates. For example, if you specify /u02/ORCL/TABLE, the /u02/ORCL directory must preexist and the Provisioning Server deployment creates the /TABLE directory.

- *JDE DB Index Directory*

  Enter the path to install the indexes.

  Path Rules: All directories in the specified path must preexist, ***except*** the last directory in the path. Therefore you must manually create the directory structure except for the last directory, which the

Provisioning Server deployment process creates. For example, if you specify /u03/ORCL/INDEX, the /u03/ORCL directory must preexist and the Provisioning Server deployment creates the /INDEX directory.

- *Schemas*

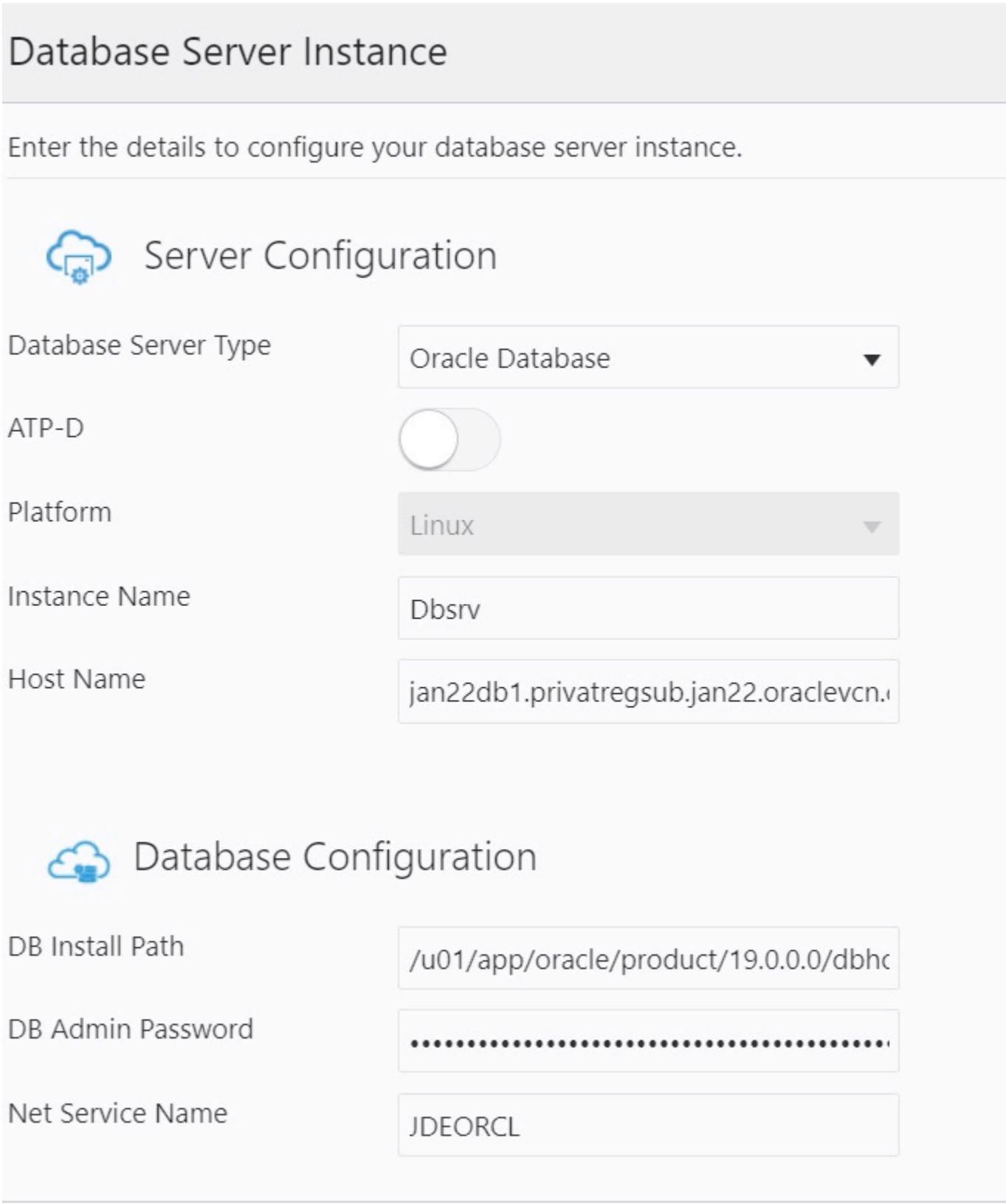
  Click the Schemas field and select the schemas you want from the auto-suggest text. The schemas available are: Shared, Development, Prototype, Production, and Pristine with Demo data.

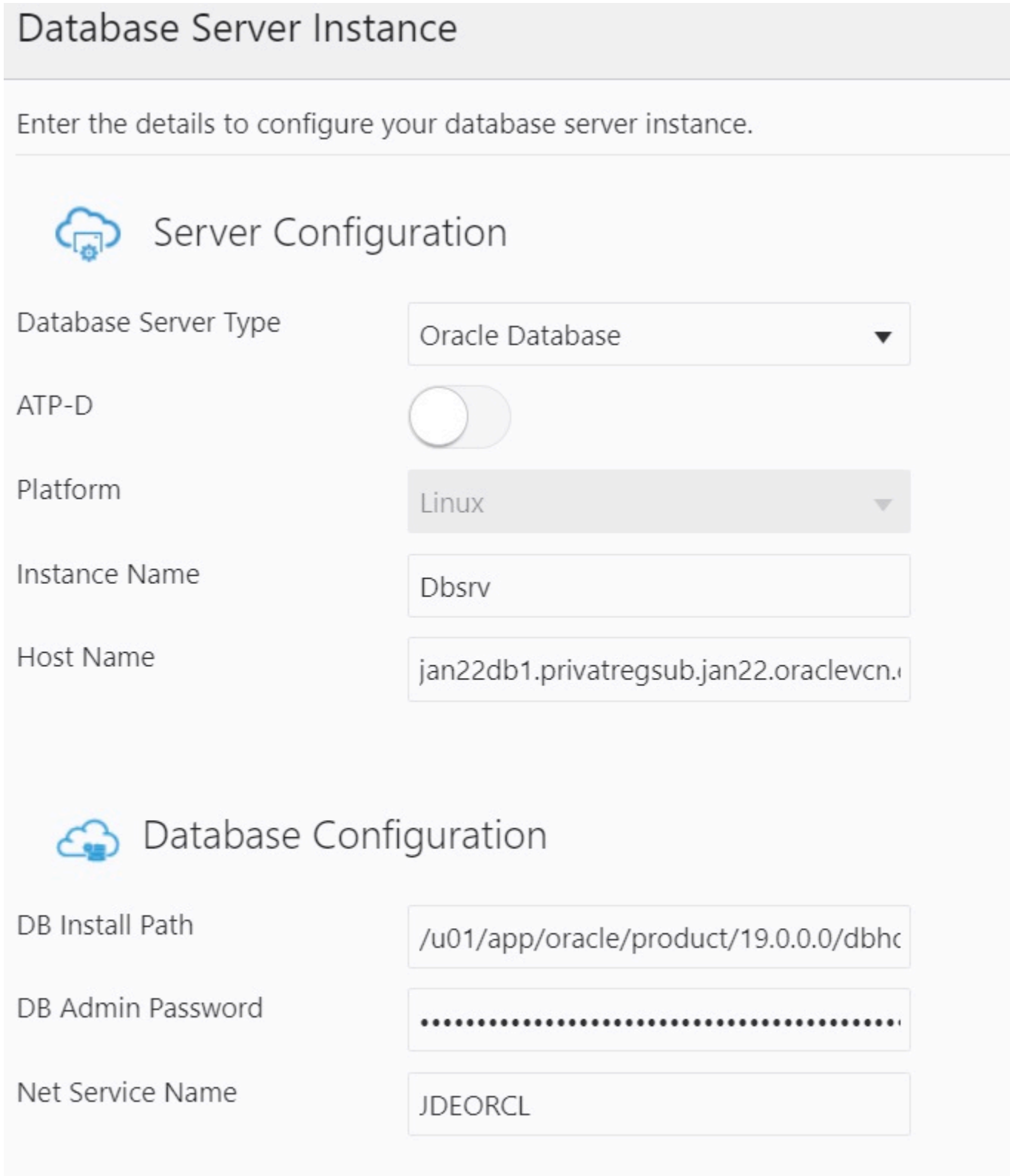
  > **Note:** It is mandatory to add the Shared schema.

  > **Note:** At this point, you should ensure that you specify **all** the schemas you might plan to use. The schemas you choose to install on the Database Server can only be deployed once, which is specified at this point in the Provisioning Console. You can use the Provisioning Console to programmatically add additional schemas after deploying the orchestration.

- *Demo Data*

  Click the **Demo Data** field and select the demo data from the auto-suggest text. Demo data is available depending on the schema selected. For example, if you select the schema as Development, the Development demo data will be available.


Database Server Instance
Enter the details to configure your database server instance.
Server Configuration
Database Server Type
Oracle Database
ATP-D
Platform
Linux
Instance Name
Dbsrv
Host Name
jan22db1.privatregsub.jan22.oraclevcn.
Database Configuration
DB Install Path
/u01/app/oracle/product/19.0.0.0/dbhc
DB Admin Password
Net Service Name
JDEORCL


Database Server Instance
Enter the details to configure your database server instance.
Server Configuration
Database Server Type
Oracle Database
ATP-D
Platform
Linux
Instance Name
Dbsrv
Host Name
jan22db1.privatregsub.jan22.oraclevcn.
Database Configuration
DB Install Path
/u01/app/oracle/product/19.0.0.0/dbhc
DB Admin Password
Net Service Name
JDEORCL

11. Click the **Next** button. Because you will be connecting to an existing Oracle Cloud Infrastructure Service database instance, the system validates all the input that you provide. If the validation is successful, the JD Edwards Enterprise Server page is displayed.

12. On Enterprise Server Instance page, complete these fields to create and configure the Enterprise Server instance.

Server Configuration

- *Platform*

  This field is disabled and it is automatically populated as Linux.
- *Instance Name*

  Create an instance name for the Enterprise Server. The conditions to set the instance name is displayed in the tooltip when you click the field.
- *Host Name*

  Enter the host name.

Enterprise Server Preferences

- *Server Type*

  Select one or both of the available server types for this Enterprise Server.

  Single Enterprise Server. If you are deploying only a single Enterprise Server, select both Logic and Batch as the server types.

  Multiple Enterprise Servers. If you are deploying multiple Enterprise Servers, at least one server must be specified as a Logic server for each pathcode. The other servers can be specified as Batch servers.
- *Pathcodes*

  Click the Available Pathcodes field and select the pathcodes required from the auto-suggest text. The four available pathcodes are: Development, Prototype, Pristine, and Production.

  > **Note:** It is good practice to select pathcodes here that correlate to the schemas you selected for the Database Server. The Provisioning Console programmatically enforce this correlation. If you select pathcodes on the Enterprise Server that are a superset of the database schemas you selected, the Enterprise Server will not be able to access the data required to function correctly. In the Provisioning Console, the pathcodes that you specify at this point for installation on the Enterprise Server can be deployed only once. You can use the Provisioning Console to programmatically add additional schemas after deploying the orchestration.

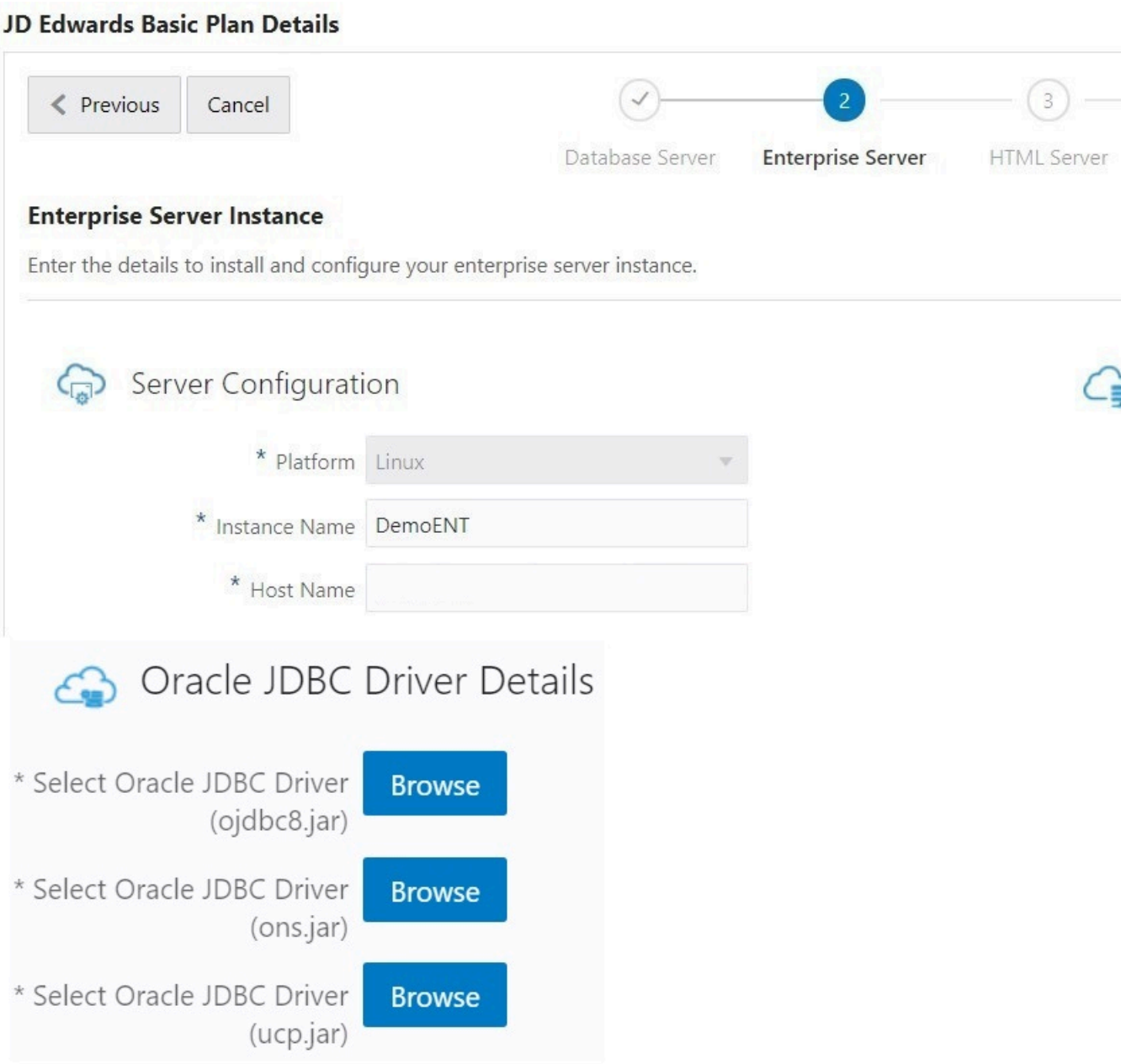
- ***Oracle JDBC Driver Details***

  This driver is required for connectivity between the Enterprise Server and the Oracle database server.

  Click the **Browse** button to select each of the required components for the Oracle JDBC driver. For example:

  - odbc8.jar
  - ons.jar
  - ucp.jar

  > **Note:** Refer to Oracle Certifications for the version of the supported driver and associated components.



13. Click the **Next** button. Because you will be connecting to an existing Oracle Cloud Infrastructure Service EnterpriseOne instance, the system validates all the input that you provide. If the validation is successful, the JD Edwards HTML Server page is displayed.

14. On the HTML Server Instance page, complete these fields to create and configure the HTML Server instance.

Server Configuration

- *Platform*

  This field is disabled and it is automatically populated as Linux.
- *Instance Name*

  Create the instance name of the HTML Server instance.
- *Host Name*

  Enter the host name.
- *Port*

  Enter a unique (available) port number for this server that will use an SSL connection. This port number must be between 1024 and 65535. This port number is used by HTTPS to create a container and deploy

the web component. Ensure the availability of a port that is one less than the port number that you enter here. That is, if you specify port 8081, you must also ensure that port 8080 is available.

> **Note:** For each SSL port that you open in the firewall, you must also open a companion port for non-SSL access required for Server Manager. The numeric value for the companion port must be one less than the value specified for the SSL port. For example, if you specify a port value of 8081 for SSL, in the firewall you must also open a port one less than that value; in this case you must open port 8080. Refer to the section "Enable Inbound Ports in the Firewall for Compute Instances" in the OBE "Performing Common Setup for All Linux Servers" of this Learning Path.

Web Server Preferences

- *Pathcode*

  Select the required pathcode from the drop-down menu.

> **Note:** Using the Quick Start mode, you can specify only a dedicated HTML Server for AIS. If you want to create a standard HTML Server, which is strongly recommended for Production environments, you must use the Advanced Deployment mode. For a description of each HTML Server type, refer to the OBE "Fundamentals" of this Learning Path.x

> **Note:** Each dedicated HTML Server and AIS Server pair can support only one pathcode. If you want additional HTML instances to support additional pathcodes, you must configure additional HTML Server pairs using the Advanced deployment mode of the Provisioning Console. For more information, refer to the OBE "Orchestrating Using Advanced Mode" of this Learning Path.

WebLogic Details

- *User Name*

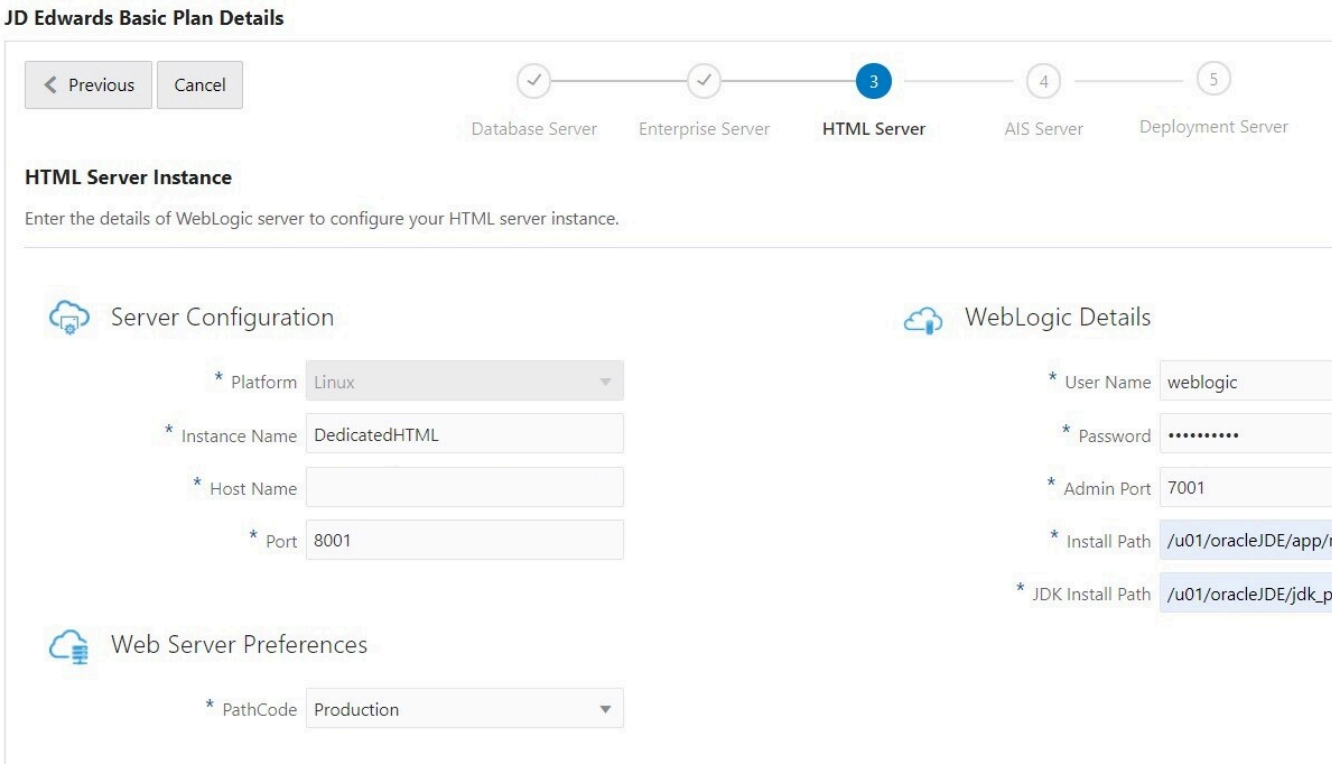
  Enter the user name.
- *Password*

  Enter the WebLogic Server password.
- *Admin Port*

  Enter the port number to access the WebLogic Administration Console.
- *Install Path*

  Enter the installation path of the WebLogic instance.
- *JDK Install Path*

  Enter the JDK installation path.



- *JD Edwards Web Server Details*

  Web Server Instance Details - Dedicated HTML Server for AIS

15. Click the **Next** button. The system validates the input. If the validation is successful, the AIS Server Instance page is displayed.
16. On AIS Server Instance page, complete these fields to configure your AIS Server instance.

Same as HTML Server

This option is selected by default. You cannot deselect it because this AIS Server must be paired with the dedicated HTML Server that you configured in the preceding step.

Server Configuration

- *Platform*

  This field is disabled and it is automatically populated as Linux.
- *Instance Name*

  Create an instance name for the WebLogic Server.
- *Host Name*

  Enter the host name.
- *Port*

  Enter a unique (available) port number for this server that will use an SSL connection. This port number must be between 1024 and 65535. This port number is used by HTTPS to create a container and deploy

the web component. Ensure the availability of a port that is one less than the port number that you enter here. That is, if you specify port 8081, you must also ensure that port 8080 is available.

> **Note:** Important: For each SSL port that you open in the firewall, you must also open a companion port for non-SSL access required for Server Manager. The numeric value for the companion port must be one less than the value specified for the SSL port. For example, if you specify a port value of 8081 for SSL, in the firewall you must also open a port one less than that value; in this case you must open port 8080. Refer to the section "Enable Inbound Ports in the Firewall for Compute Instances" in the OBE "Performing Common Setup for All Linux Servers" of this Learning Path.

Web Server Preferences

- *Type*

  This field is disabled and is automatically populated as **AIS Server**.
- *HTML Server Instance*

  Select the instance of the previously defined dedicated HTML Server from the drop-down menu.

WebLogic Details

- *User Name*

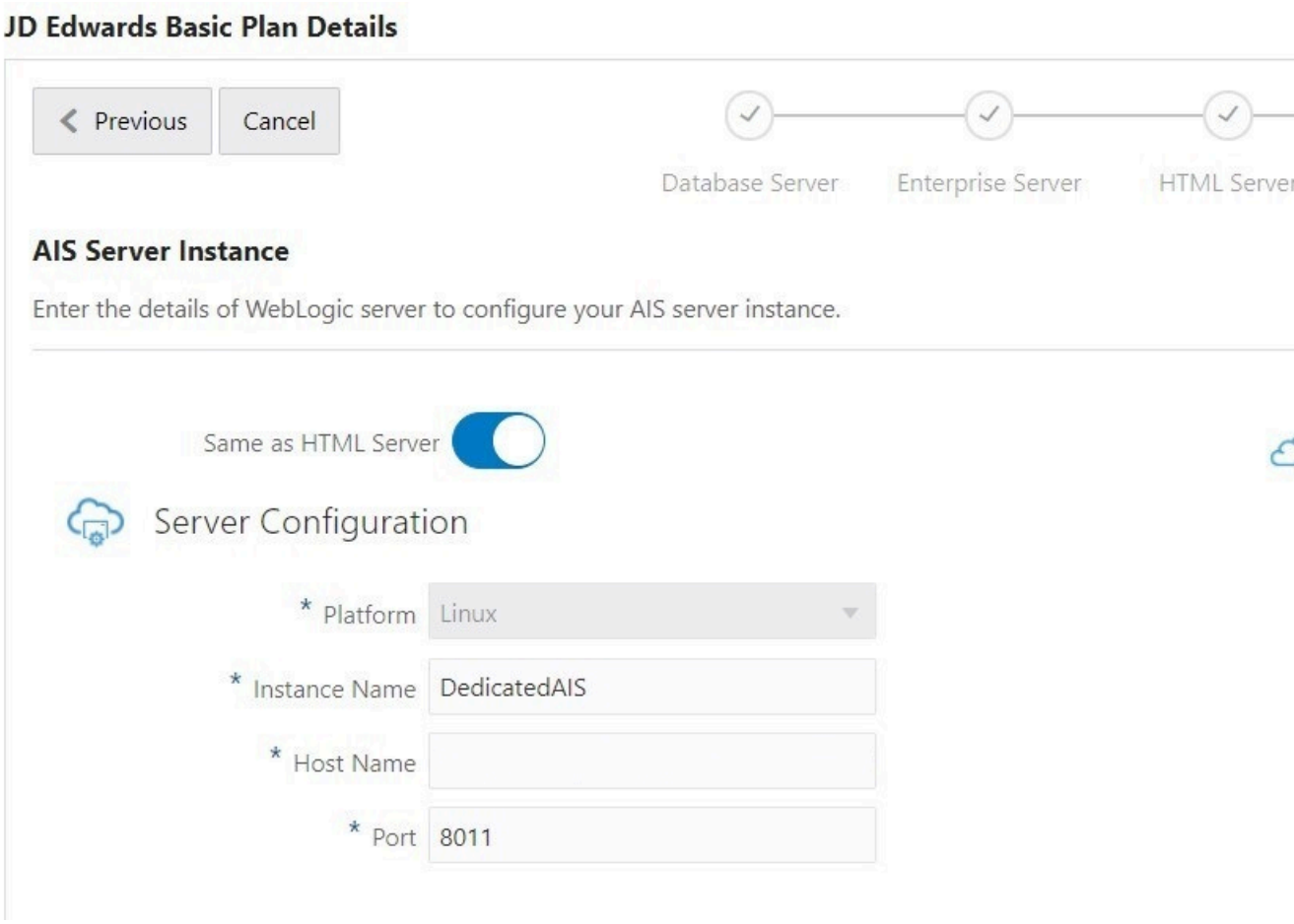
  Enter the user name.
- *Password*

  Enter the WebLogic password.
- *Admin Port*

  Enter the admin port number.
- *Install Path*

  Enter the installation path of the WebLogic instance.
- *JDK Install Path*

  Enter the JDK installation path.



17. Click the **Next** button. The system validates the input. If the validation is successful, the JD Edwards Deployment Server page is displayed.

18. On JD Edwards Deployment Server page, complete these fields to create and configure your Deployment Server instance.

Server Configuration

- *Instance Name*

  Create a name for the Deployment Server instance. The conditions to set the instance name is displayed in the tooltip when you click the field.
- *Host Name*

  Enter the host name.
- *Windows User*

  Enter the name of the Windows user.
- *Windows Password*

  Enter the password of the Windows user.

Deployment Server Preferences

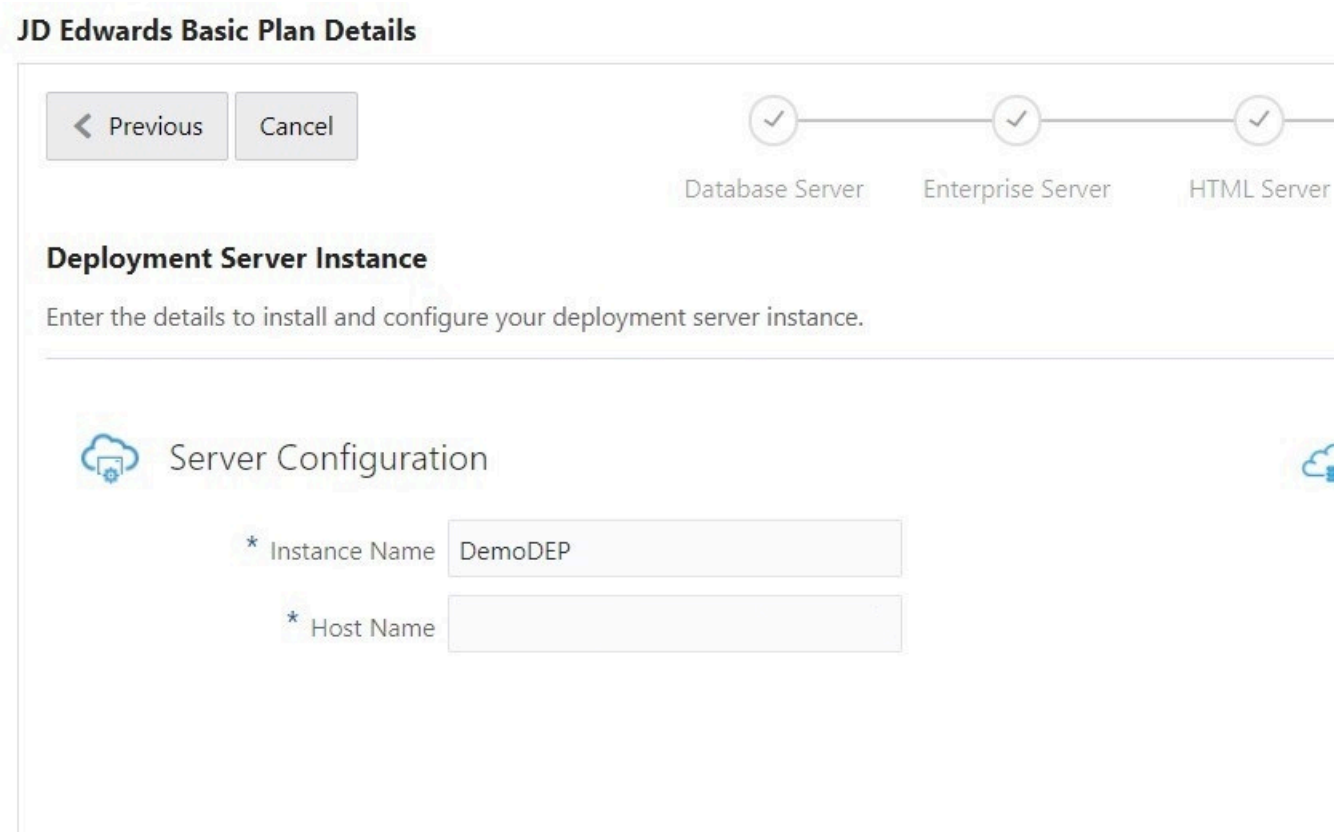
- *Location*

  Enter the location.

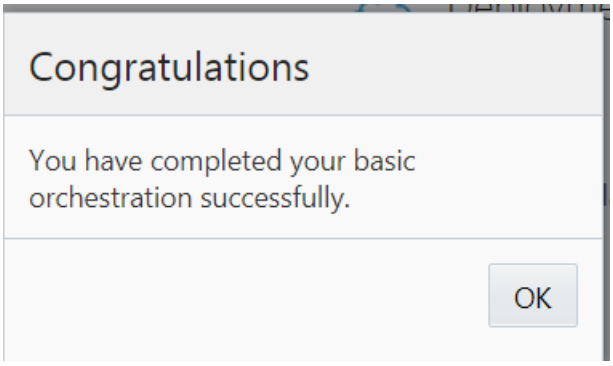
  This value is the base location for your JD Edwards EnterpriseOne machines. For example, typical values might be a city name (such as Denver or Austin), a geographical region name (such as US or India), or a general location name (such as Corporate).
- *Installation Drive*

  Enter the drive for the installation.
- *Pathcodes*

  This field is automatically populated.

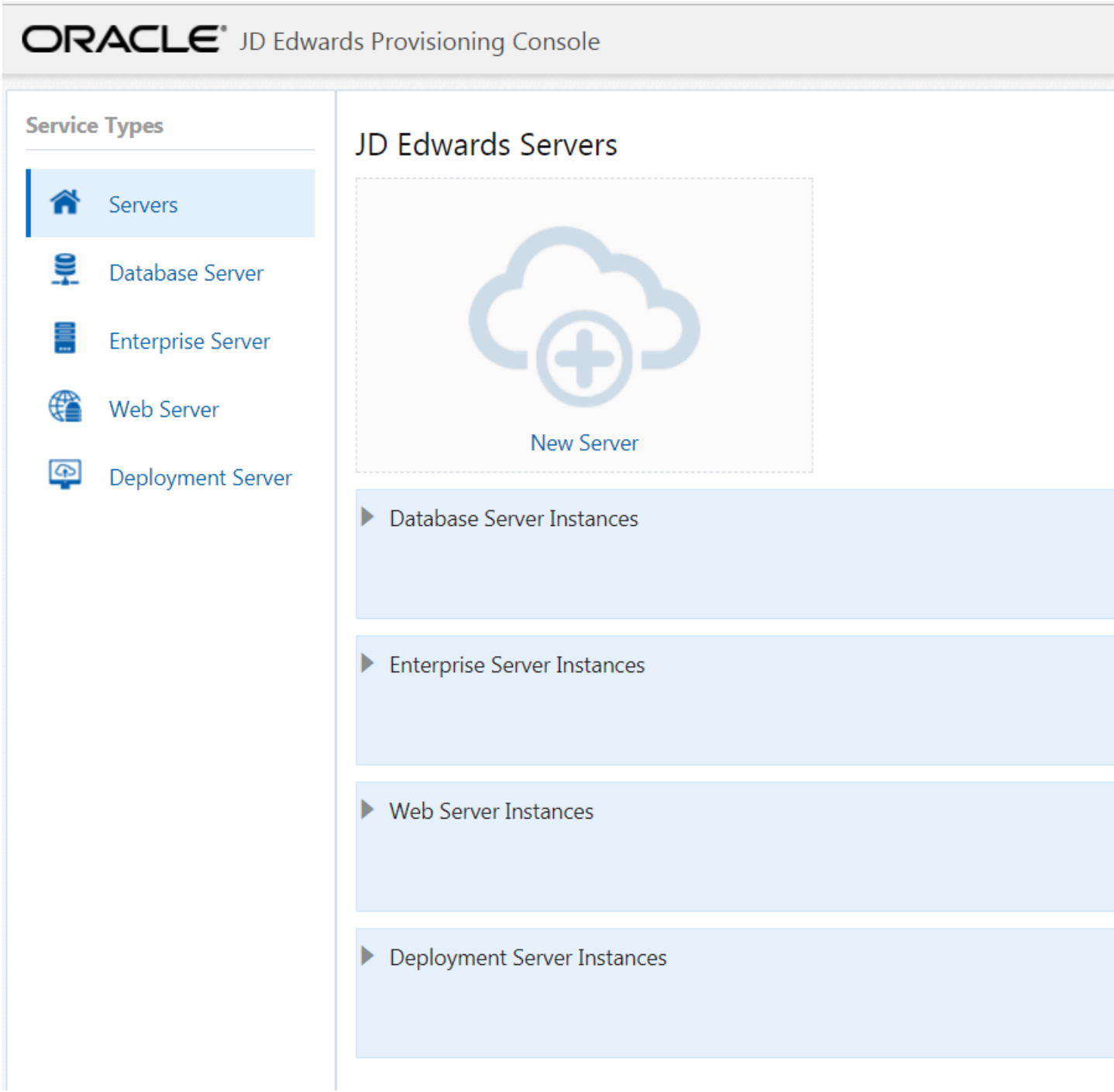


19. Click the **Finish** button.



20. Click **OK** in the success message window.

21. The summary window is displayed. In the summary window, you can see that one instance is created for each of the servers. Click the **Back** button to proceed to deploy your services as described in the OBE "Deploying an Orchestration" of this Learning Path.



> **Note:** You can click **Options** in the menu bar and then select the menu item to change your Global Settings or to reset your settings (that is, delete your configuration details, global settings, and orchestration data). Also optionally, you can further customize a completed Quick Start Deployment Plan using the **Advanced** deployment function of the JD Edwards Provisioning Console. For more information, refer to the OBE "Orchestrating Using Advanced Mode" of this Learning Path.

Orchestrating an Advanced Deployment Plan

This tutorial

Orchestrating Using Advanced Mode

This section section shows how to orchestrate a deployment plan using the advanced mode on Linux using the JD Edwards One-Click Provisioning Console.

You can orchestrate a Deployment Plan using Advanced mode, which allows you to:

- Modify and add servers to an existing Orchestration that was created using the Quick Start wizard.
- Create a new Orchestration with no guidance from a wizard. Unlike using the Quick Start wizard, the Advanced mode will ***not*** guide you through the required sequence of machines to satisfy dependencies of the configuration. For example, the allowable pathcodes for an Enterprise Server are dependent on the schemas previously selected for the Database Server.

Prerequisite

- You must have configured the administrator passwords for WebLogic Server and Server Manager Console in the Configure section of the JD Edwards One-Click Provisioning Console.
- Before orchestrating an Advanced Deployment Plan, the recommended practice is to first orchestrate a basic Deployment Plan using the Quick Start mode. The Quick Start procedure is documented in the section of this document entitled: Orchestrate Using Quick Start Mode. After this Quick Start orchestration is created, you can use the Advanced mode to modify, delete, or add on additional server instances.
- Alternately, experienced users can use Advanced Mode to create an orchestration without assistance from a structured wizard, which assumes they are aware of the required sequence of creation and the inter dependencies.

Orchestrating an Advanced Deployment Plan

> **Note:** The following procedure explains how to modify and add servers to an existing orchestration that was created using the Quick Start mode.

The required sequence of adding instances to an orchestration and the rules related to the machines and pathcodes is as follows:

1. **Database Server**

You can create five database instances if you select one schema per instance.

2. **Enterprise Server**

   One to many Enterprise Servers can be created. At least one Enterprise Server must be created with selected pathcodes available from the available schemas that were selected for the Database Server. An Enterprise Server must be configured before you can add HTML Servers. If multiple Enterprise Servers are deployed, at least one must be configured as a Logic Server per pathcode. Additional Enterprise Servers can be added to an Orchestration and they can be deployed after your initial plan is deployed.

3. **Web Servers**

   HTML Server. Web Servers include the JD Edwards EnterpriseOne HTML Server. There are two types of HTML Servers: **Standard JAS** and **Dedicated HTML for AIS**.

   One to many HTML Server instances can be created and each will be associated with one specific pathcode that is available on the Enterprise Server. Additional HTML Servers can be added to an Orchestration and they can be deployed after your initial plan is deployed.

   Refer to the *Fundamentals* section of this Learning Path for a description of each type of HTML Server.

   AIS Server. Another type of Web Server for JD Edwards EnterpriseOne is the AIS Server, which must be installed and configured along with a Dedicated HTML Server for AIS.

   Zero to many AIS Server instances can be created and each will be associated with a specific HTML Server instance. Additional AIS Server instances can be added on to your plan and deployed after your initial plan is deployed.

   > **Note:** If you do not specify at least one AIS Server, the full functionality of certain JD Edwards EnterpriseOne applications will not be available. If you used the Quick Start mode to configure a basic environment, the workflow required the inclusion of this server.

   > **Note:** You cannot specify a single HTML Server instance to also support an AIS Server; that is, you cannot combine two servers in the same instance. You must create a separate instance for each AIS Server.

4. **Deployment Server**

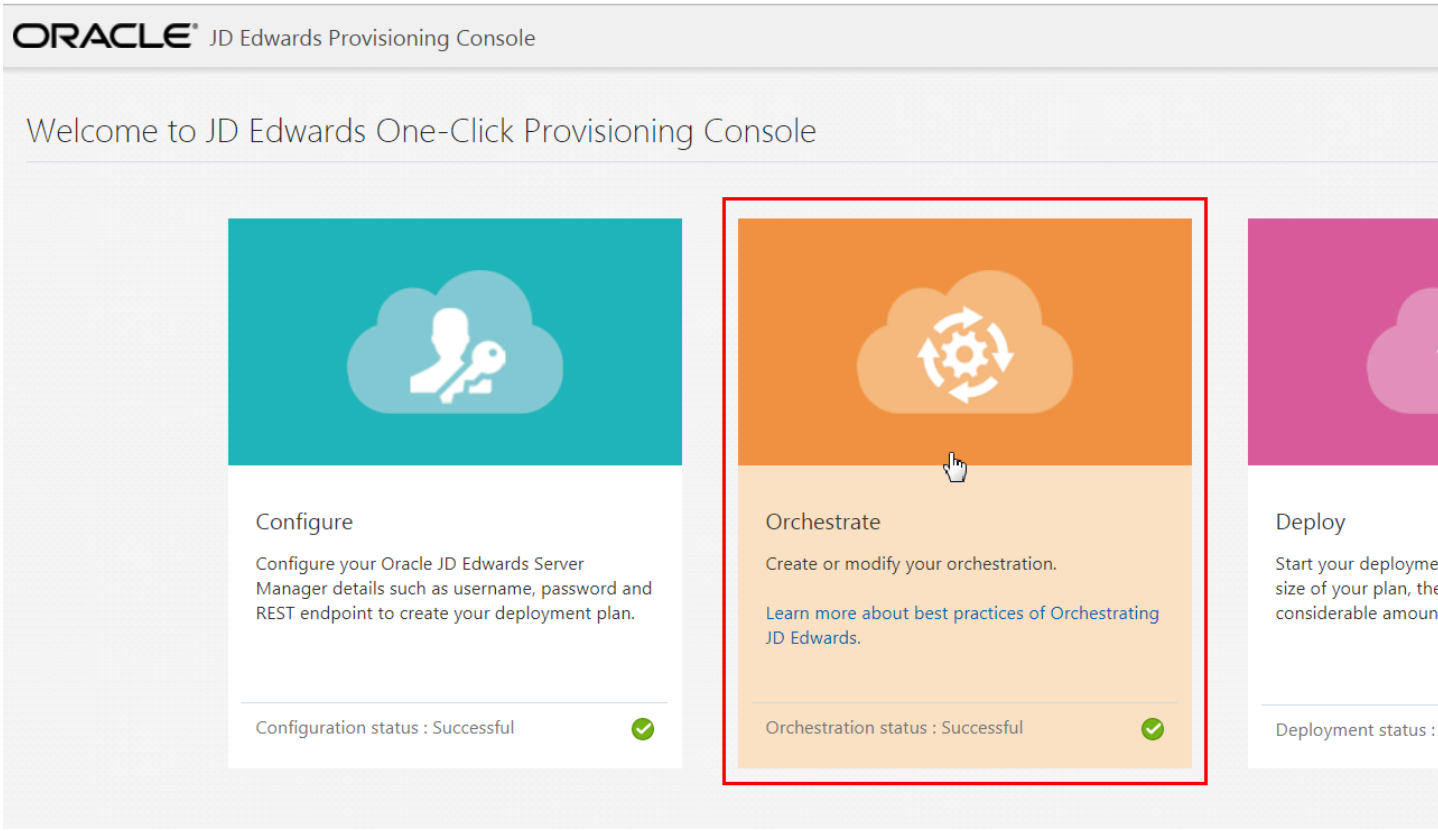
   A single Deployment Server can be created and all pathcodes can be selected regardless of pathcodes selected for your runtime servers.

   > **Note:** For any orchestration created or modified using the Advanced Mode Deployment Plan, you can click the **Options** function from the menu bar to change your Global Settings or to Reset your settings (that is, to delete your configuration details, global settings, and orchestration data)

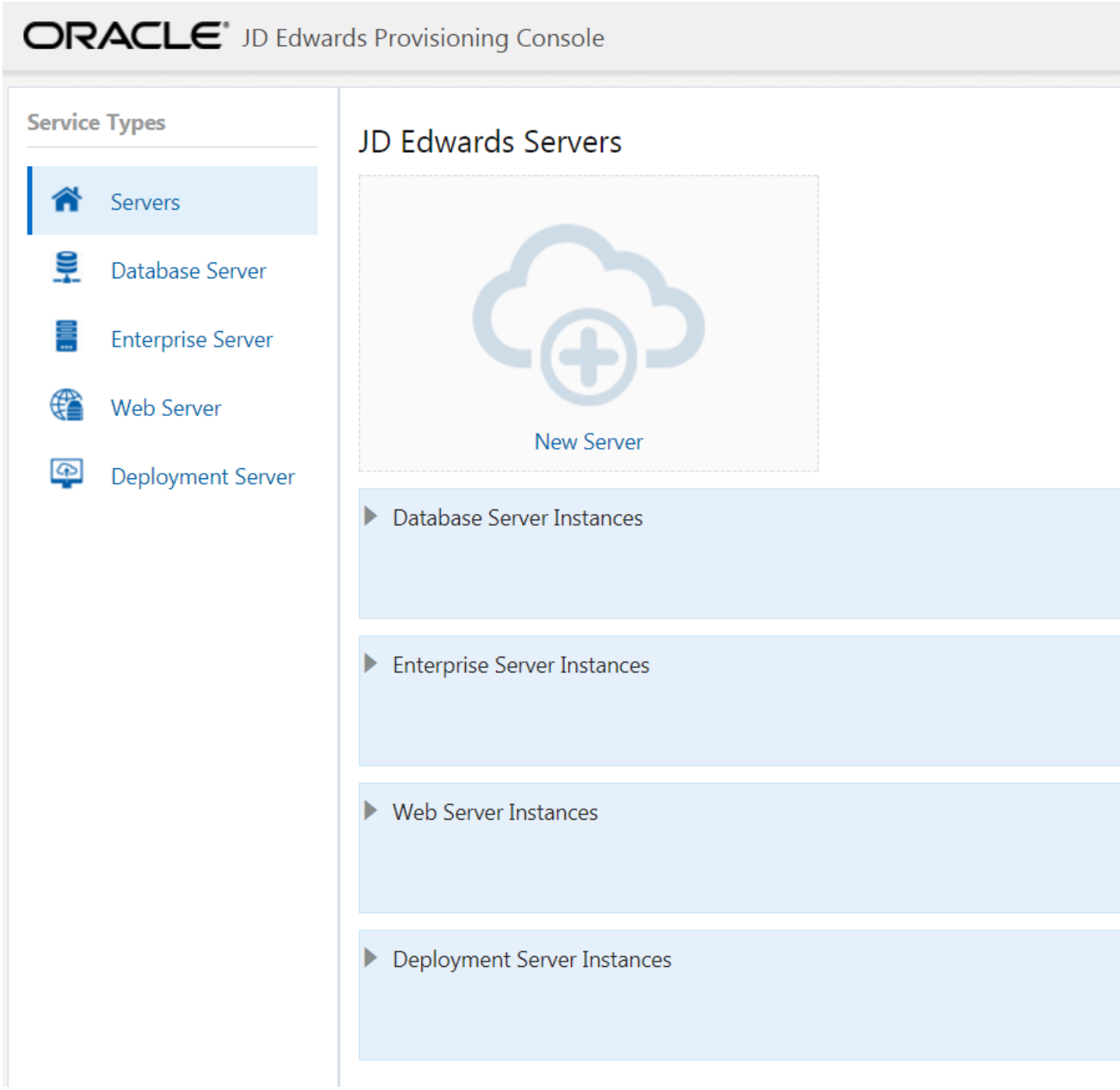
   .

To use the JD Edwards Provisioning Console to orchestrate an Advanced Deployment Plan:

1. On the JD Edwards Provisioning Console, click the **Orchestrate** icon.



2. On JD Edwards Servers, click on the instance of an existing server, or click the **New Server** icon to add a new JD Edwards service. Alternately you can select the desired server from **Service Types** on the left tab, and then click **New Server** to add a New Server.



Note: The remainder of this procedure includes steps to either add (where allowed) or modify (existing) these instances:

- Database Server
- Enterprise Server
- Web Server (for example, HTML Server and AIS Server)
- Deployment Server*

* The Provisioning Console will not allow you to add more than one of these server types because only one server of this type is supported per deployment.

Database Server

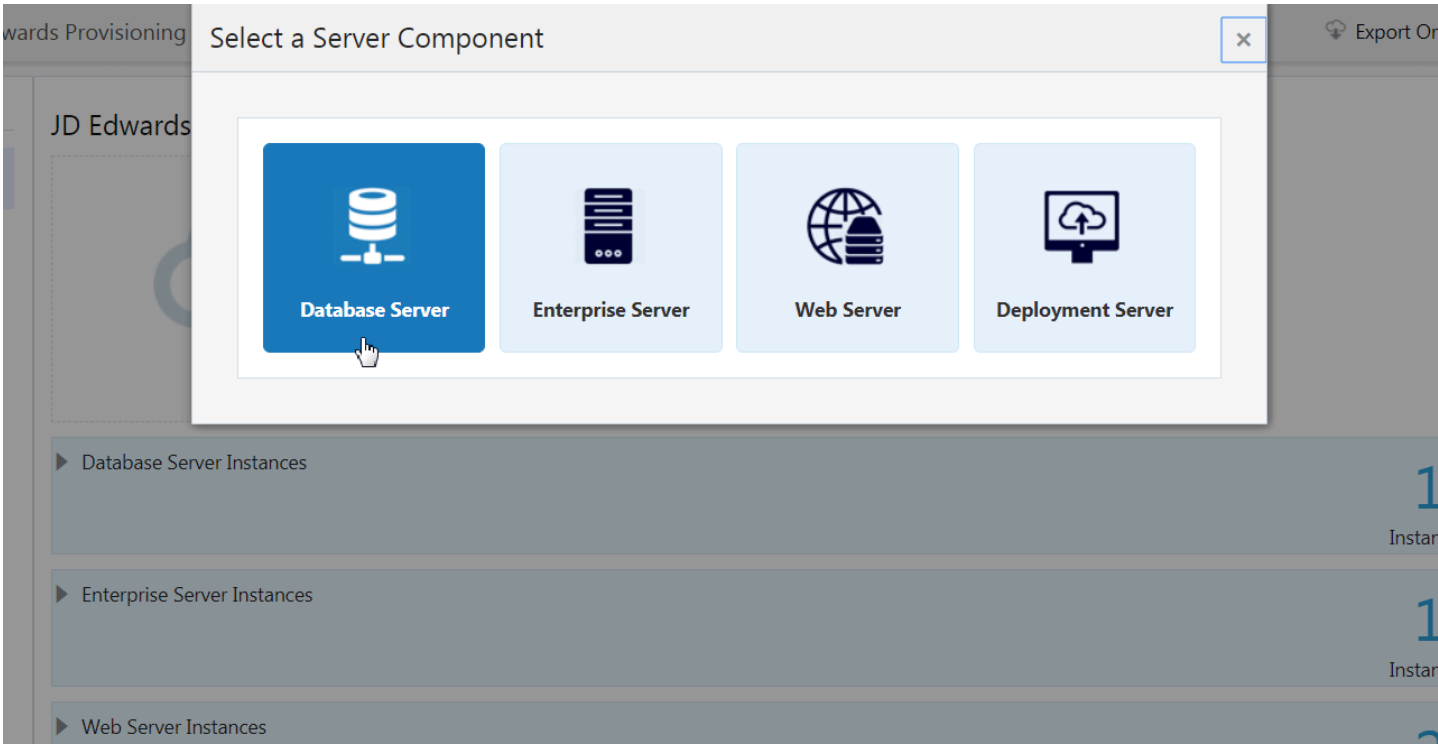
You can create five database instances if you select one schema per instance. For example, if you select Development and Shared schemas for an instance, you can create three more database instances. For one deployment instance, you can have a maximum number of five schemas distributed across one or many database instances.

You can provision the Database Server instance with the available schemas as required. The following schemas are available for the database instance:

- Development
- Shared (required)
- Prototype
- Production
- Pristine

To add a Database Server:

1. Click the **New Server** icon and select Database Server from the Select a Server Component window.



2. On Database Server Instance page, complete the following fields to create and configure the Database Server instance.

   The below sections and supported screens are separated for Standard Oracle Database and Oracle Autonomous Database.

   Standard Oracle Database

   Server Configuration

   - *Database Server Type*

     The Database Server Type is populated by default as Oracle Database.
   - *ATP-D*

     You should only enable the ATP-D option if you are using an Oracle Autonomous Database Dedicated; this database is only supported in Oracle Cloud Infrastructure. This functionality is described in the

Learning Path "Deploying JD Edwards EnterpriseOne on Oracle Cloud Infrastructure on Linux with Autonomous Database."

A description of the fields specific to Autonomous Database are presented below the first figure below.

- *Platform*

  This field is disabled and it is automatically populated as Linux.
- *Instance Name*

  Create an instance name for your database instance.
- *Host Name*

  Enter the host name.

Database Configuration

- *DB Install Path*

  Enter the DB installation path.
- *DB Admin Password*

  Enter the password of the database administrator.
- *Net Service Name*

  Enter the net service name.

JD Edwards Database Configuration

- *Use ASM feature*

  Enable this option if you are using RAC DB as your Database Server.

  If you disable ASM in your Orchestration, you must enter valid values for the install, table, and index directories for your Oracle database. For example:

  - `/u01/DataDB`
  - `/u01/ORATABLE`
  - `/u01/ORAINDEX`

  If you enable ASM in your Orchestration, you must enter valid values for your DISK group. By default the values for are assumed to be DATA. Otherwise, you can enter any other name that you have created. An example screen is shown below as Database Server Instance - ASM Enabled.
- *JDE DB Install Directory*

  Enter the installation path.

  Path Rules. All directories in the specified path must preexist, ***except*** the last directory in the path. Therefore you must manually create the directory structure except for the last directory, which the Provisioning Server deployment process creates. For example, if you specify /u01/ORCL/INSTALL,

the /u01/ORCL directory must preexist and the Provisioning Server deployment creates the /INSTALL directory.

- *JDE DB Table Directory*

  Enter the path to install the table data.

  Path Rules: All directories in the specified path must preexist, ***except*** the last directory in the path. Therefore you must manually create the directory structure except for the last directory, which the Provisioning Server deployment process creates. For example, if you specify /u02/ORCL/TABLE, the /u02/ORCL directory must preexist and the Provisioning Server deployment creates the /TABLE directory.

- *JDE DB Index Directory*

  Enter the path to install the indexes.

  Path Rules: All directories in the specified path must preexist, ***except*** the last directory in the path. Therefore you must manually create the directory structure except for the last directory, which the

Provisioning Server deployment process creates. For example, if you specify /u03/ORCL/INDEX, the /u03/ORCL directory must preexist and the Provisioning Server deployment creates the /INDEX directory.

- *Schemas*

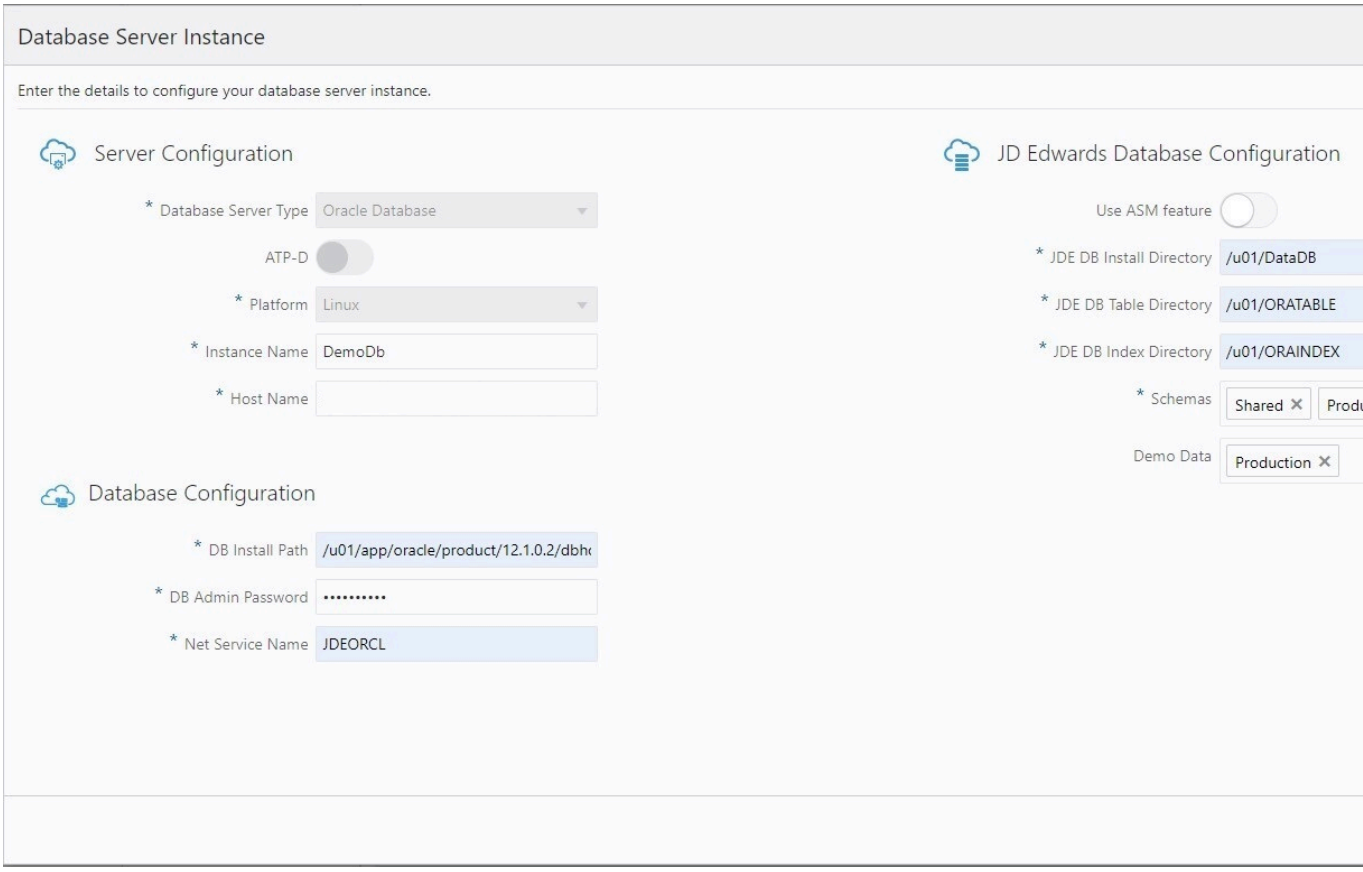
  Click the Schemas field and select the schemas you want from the auto-suggest text. The schemas available are: Shared, Development, Prototype, Production, and Pristine with Demo data.

  > **Note:** Note: It is mandatory to add the Shared schema.

  > **Note:** At this point, you should ensure that you specify all the schemas you might plan to use. The schemas you choose to install on the Database Server can only be deployed once, which is specified at this point in the Provisioning Console. You can use the Provisioning Console to programmatically add additional schemas after deploying the orchestration.

- *Demo Data*

  Click the **Demo Data** field and select the demo data from the auto-suggest text. Demo data is available depending on the schema selected. For example, if you select the schema as Development, the Development demo data will be available.



Oracle Autonomous Database

Server Configuration

- *Database Server Type*

  The Database Server Type is displayed as Oracle Database.
- *ATP-D*

  Enable this selector button for Oracle Autonomous Database ATP-D.
- *Platform*

  This field is disabled and it is automatically populated as Linux.
- *Instance Name*

  Create an instance name for your database instance.
- *Host Name*

  Enter the host name.

Database Configuration

- *DB Admin Password*

  Enter the password of the database administrator.
- *DB Wallet*

  Click the **Browse** button to locate and select the DB Wallet that you created by following the steps in the section "Downloading a Database Wallet for Autonomous Transaction Processing on Dedicated Infrastructure" of this Learning Path.

JD Edwards Database Configuration

- *JDE DB Install Directory*

  Enter the installation path.

  Path Rules. All directories in the specified path must preexist, except the last directory. Therefore you must manually create the directory structure except for the last directory, which the Provisioning Server

deployment process creates. For example, if you specify /u01/ORCL/INSTALL, the /u01/ORCL directory must preexist and the Provisioning Server deployment creates the /INSTALL directory.

- *Schemas*

  Click the Schemas field and select the schemas from the auto-suggest text. The schemas available are: Shared, Development, Prototype, Production, and Pristine with Demo Data.

  > **Note:** Note: It is mandatory to add the Shared schema.

  > **Note:** point, you should ensure that you specify all the schemas you plan to use. The schemas you choose to install on the Database Server can only be deployed once, which is specified at this point in the Provisioning Console. You can use the Provisioning Console to programmatically add additional schemas after deploying the orchestration.

- *Demo Data*

  Click the **Demo Data** field and select the demo data available from the auto-suggest text. Demo data will be available depending on the schema selected. For example, if you select the schema as Development, the Development demo data will be available.

OCI Object Storage Details

- *Tenancy*

  Enter the tenancy where you have access to the Object Storage Service in Oracle Cloud Infrastructure.
- *User Name*

  Enter the user name with which you can access the Object Storage Service in Oracle Cloud Infrastructure.
- *Auth Token*

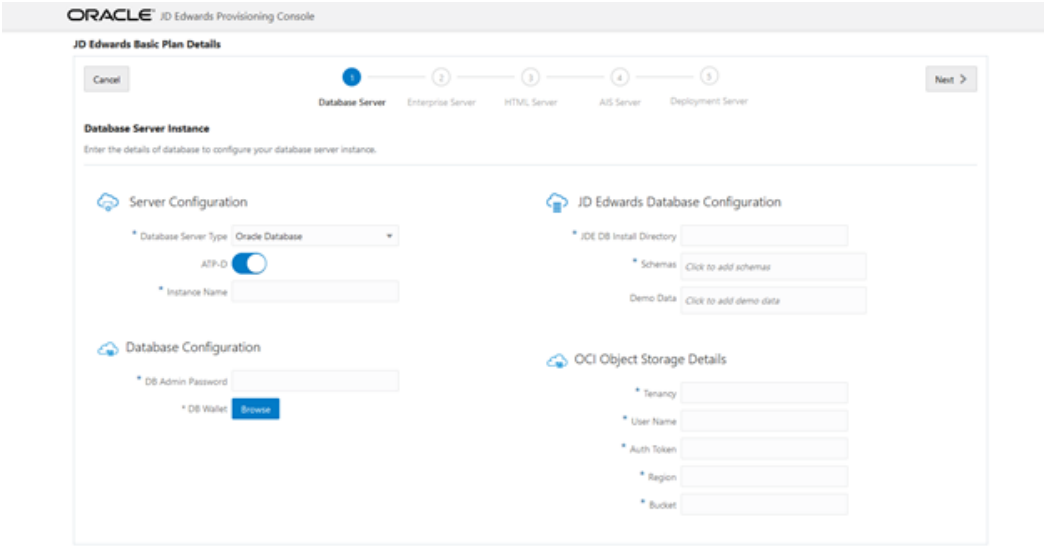
  Enter the Auth Token for the given user. This token is used to upload the JD Edwards database dump files into the Object Storage Service in Oracle Cloud Infrastructure.

  For additional details, see the section *Getting an Auth Token*
- *Region*

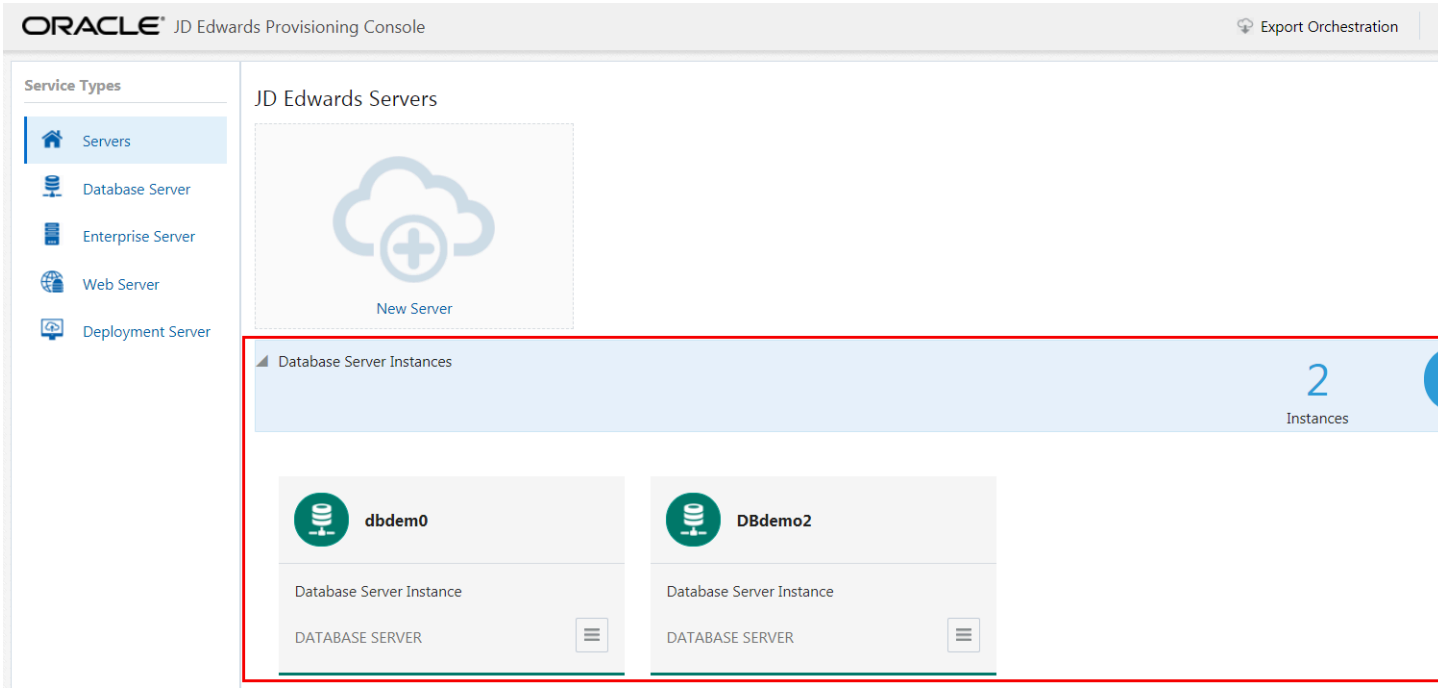
  OCI Region
- *Bucket*

  Enter the bucket name that you have previously created for use with Oracle Cloud Infrastructure Object Storage Service.

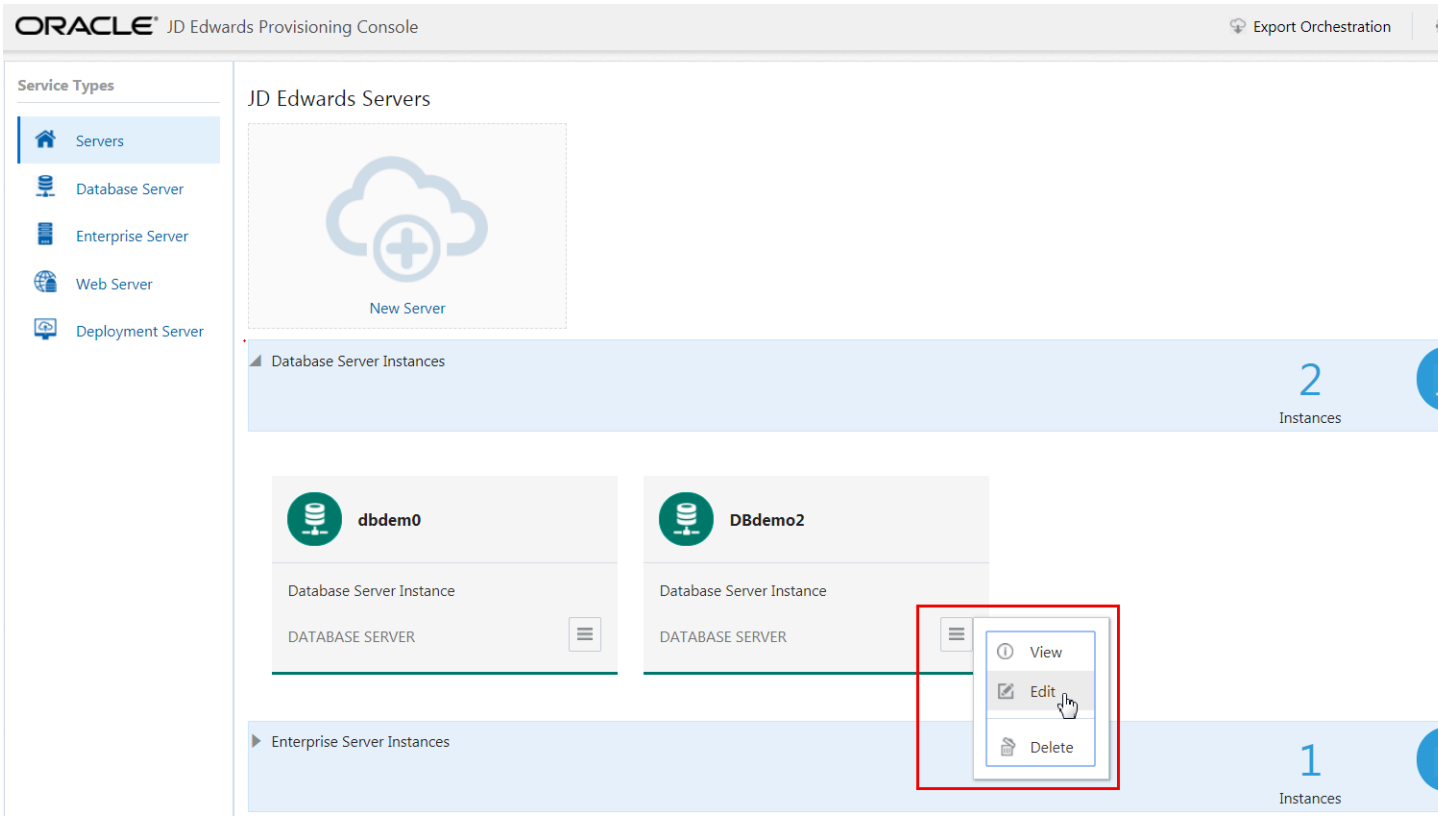
  For additional details, see the section "Managing Buckets" in this Learning Path.



3. You should now be able to view multiple instances of the Database Server.



4. If a Database Server exists, click **View** from the Application Options tab to view the existing configuration for the Database Server. To modify the instance configuration use the Application Options tab and choose the **Edit** option.



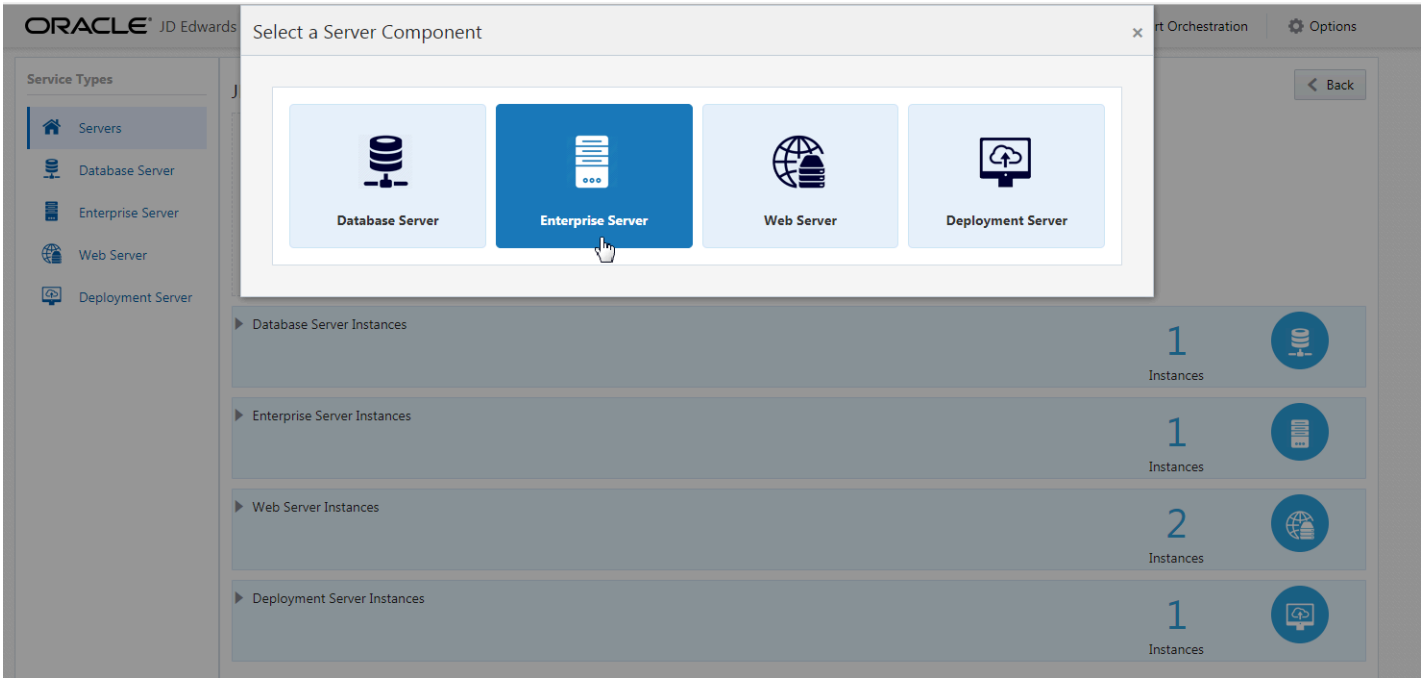
5. To delete the instance, use the Application Options tab to select **Delete.**

Enterprise Server

You can define any number of Enterprise Server instances. If you only want one Enterprise Server, you should define it to run both Logic and Batch. If you want to define multiple Enterprise Servers, at least one must be a Logic Server per pathcode.

To add an Enterprise Server:

1. Click the **New Server** icon and select **Enterprise Server** from the Select a Server Component window.



2. On Enterprise Server Instance page, complete these fields to create and configure the Enterprise Server instance.

   Server Configuration

   - *Platform*

     This field is disabled and it is automatically populated as Linux.
   - *Instance Name*

     Create an instance name for the Enterprise Server. The conditions to set the instance name is displayed in the tooltip when you click the field.
   - *Host Name*

     Enter the host name.

   Enterprise Server Preferences

   - *Server Type*

     Select one or both of the available server types for this Enterprise Server.

     Single Enterprise Server. If you are deploying only a single Enterprise Server, select both Logic and Batch as the server types.

     Multiple Enterprise Servers. If you are deploying multiple Enterprise Servers, at least one server must be specified as a Logic server for each pathcode. The other servers can be specified as Batch servers.
   - *Pathcodes*

     Click the Available Pathcodes field and select the pathcodes required from the auto-suggest text. The four available pathcodes are: Development, Prototype, Pristine, and Production.

     > **Note:** Important: It is good practice to select pathcodes here that correlate to the schemas you selected for the Database Server. The Provisioning Console programmatically enforce this correlation. If you select pathcodes on the Enterprise Server that are a superset of the database schemas you selected, the Enterprise Server will not be able to access the data required to function correctly. In the Provisioning Console, the pathcodes that you specify at this point for installation on the Enterprise Server can be deployed only once. You can use the Provisioning Console to programmatically add additional schemas after deploying the orchestration.

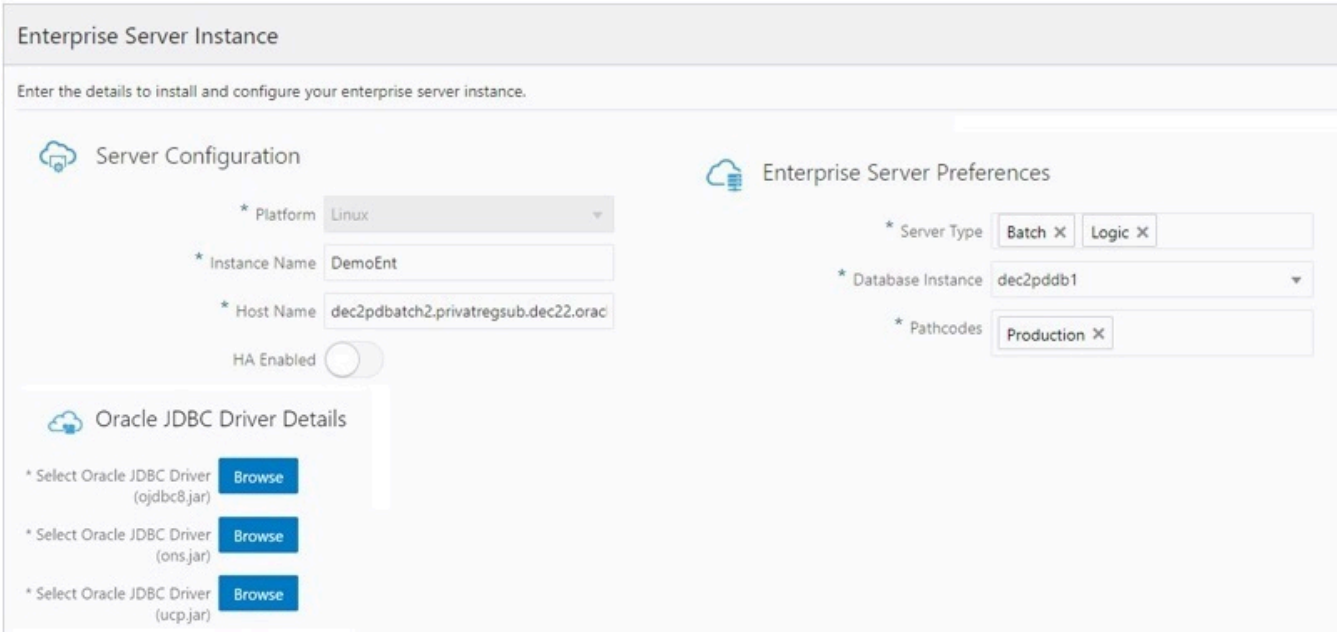
   - **Oracle JDBC Driver Details**

     This driver is required for connectivity between the Enterprise Server and the Oracle database server.

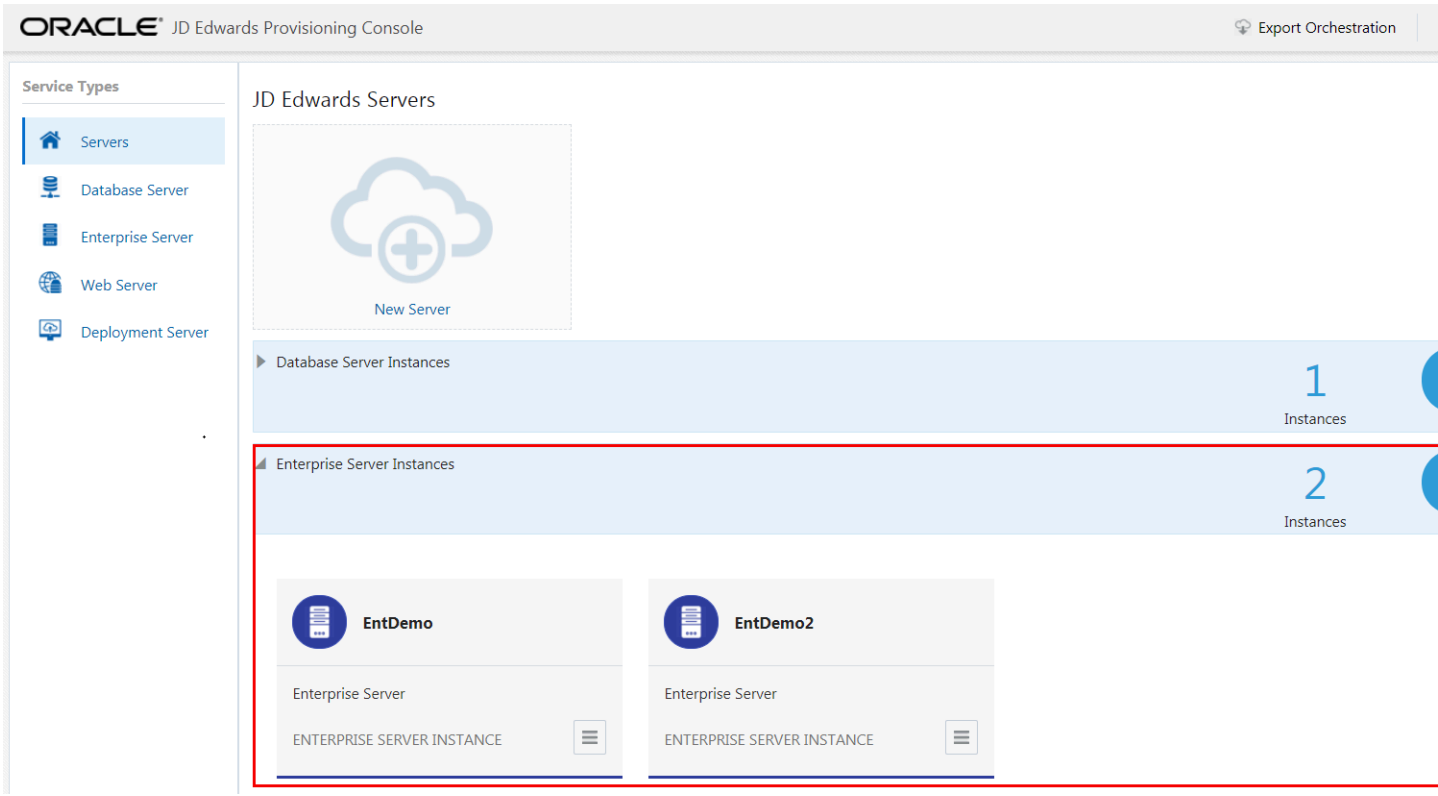
     Click the Browse button to select each of the required components for the Oracle JDBC driver. For example:

     - odbc8.jar
     - ons.jar
     - ucp.jar

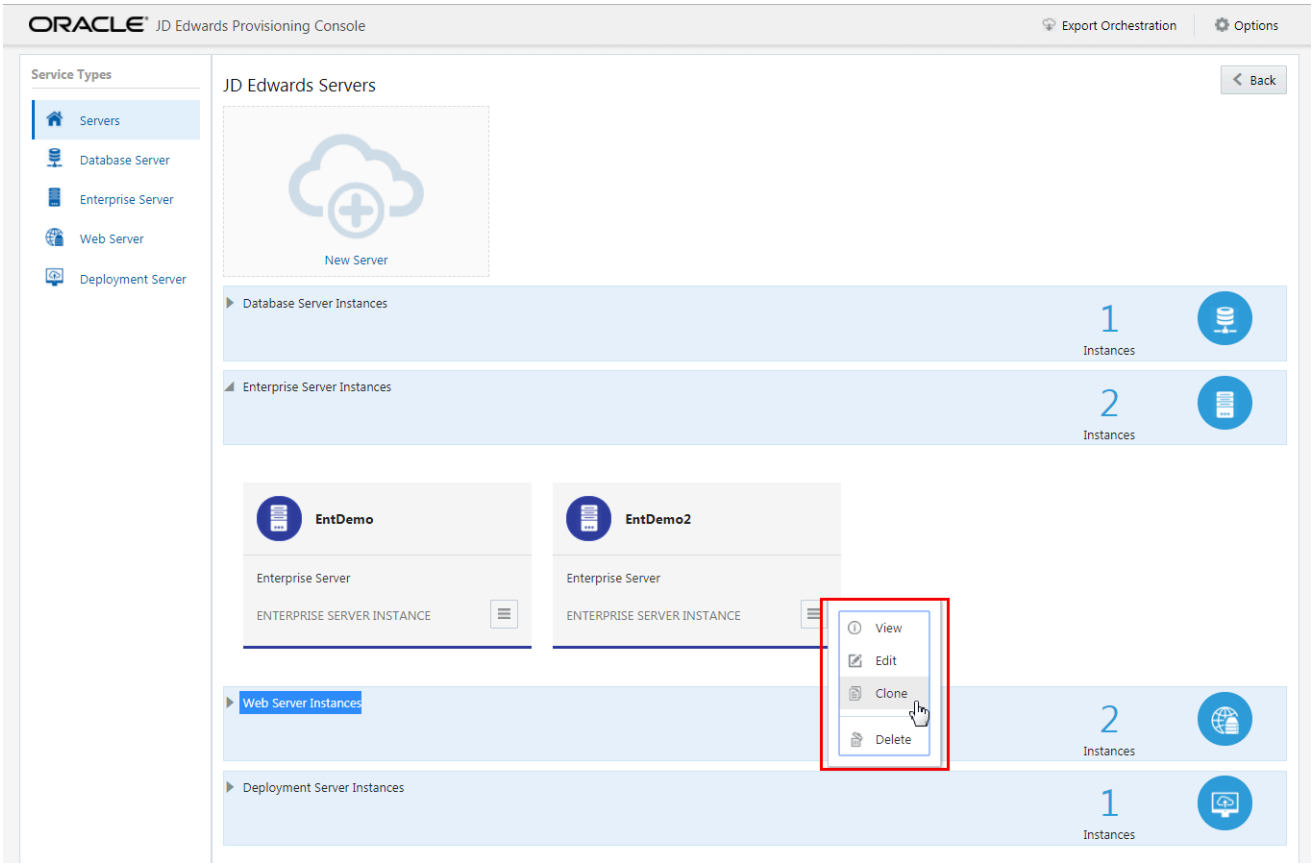
Note: Refer to Oracle Certifications for the version of the supported driver and associated components.



3. You should now be able to view multiple instances of the Enterprise Server.



4. If an Enterprise Server exists, click **View** from the Application Options tab to view the existing configuration for the Enterprise Server. To modify the instance configuration use the Application Option tab and choose the **Edit** option. Use the Clone option to **clone** the Enterprise Server instance.



5. To delete the instance, use the Application option tab to select **Delete**.

Web Server

The Instance Type for Web Servers can be any of the available servers types that are selectable from the drop-down list; however, you must have at least one configured Dedicated HTML Server saved prior to creating an associated AIS instance.

You can define any number of Web Server instances.

To add or modify a Web Server instance:

1. Select the Service Type for Web Server.
   - To create a new Web Server, click the **New Server** icon and then the **Web Server** icon and complete the required fields.
   - To modify an existing Web Server, click **View** from the Application Actions tab to view the existing configuration for the Web Server. To modify the instance configuration use the action tab and choose the **Edit** option.

2. On the Web Server Instance, you can configure each of these Web Server types:
   - HTML Server (Dedicated HTML Server for AIS)

     At least one of these servers must be specified in a pair with an AIS Server.
   - Application Interface Services (AIS) Server

     At least one of these servers must be specified in a pair with a Dedicated HTML Server for AIS.
   - Standard JAS Server

     This is a traditional JAS Server, which is optional and can be none to many.

     > **Note:** For Oracle Cloud Infrastructure only, you can select the HA Enabled option if required, and when prompted, should enter the Virtual Host Name, and then click OK.

   > **Note:** For a description of each HTML server type (Dedicated for AIS or Standard), refer to the Fundamentals section of this Learning Path.

   > **Note:** Because multiple Web Servers instances can run on the same WebLogic Server running in Oracle Cloud Infrastructure, you MUST specify different ports for each instance.

3. On the HTML Server Instance page, complete these fields to create and configure the HTML Server instance.

   Server Configuration

   - *Platform*

     This field is disabled and it is automatically populated as Linux.
   - *Instance Name*

     Create the instance name of the HTML Server instance.
   - *Host Name*

     Enter the host name.
   - *Port*

     Enter a unique (available) port number for this server that will use an SSL connection. This port number must be between 1024 and 65535. This port number is used by HTTPS to create a container and deploy

the web component. Ensure the availability of a port that is one less than the port number that you enter here. That is, if you specify port 8081, you must also ensure that port 8080 is available.

> **Note:** For each SSL port that you open in the firewall, you must also open a companion port for non-SSL access required for Server Manager. The numeric value for the companion port must be one less than the value specified for the SSL port. For example, if you specify a port value of 8081 for SSL, in the firewall you must also open a port one less than that value; in this case you must open port 8080. Refer to the section "Enable Inbound Ports in the Firewall for Compute Instances" in the OBE "Performing Common Setup for All Linux Servers" of this Learning Path.

Web Server Preferences

- *Pathcode*

  Select the required pathcode from the drop-down menu.

  > **Note:** Using the Quick Start mode, you can specify only a dedicated HTML Server for AIS. If you want to create a standard HTML Server, which is strongly recommended for Production environments, you must use the Advanced Deployment mode. For a description of each HTML Server type, refer to the section "Fundamentals" of this Learning Path.

  > **Note:** Each dedicated HTML Server and AIS Server pair can support only one pathcode. If you want additional HTML instances to support additional pathcodes, you must configure additional HTML Server pairs using the Advanced deployment mode of the Provisioning Console. For more information, refer to the OBE "Orchestrating Using Advanced Mode" of this Learning Path.

WebLogic Details

- *User Name*

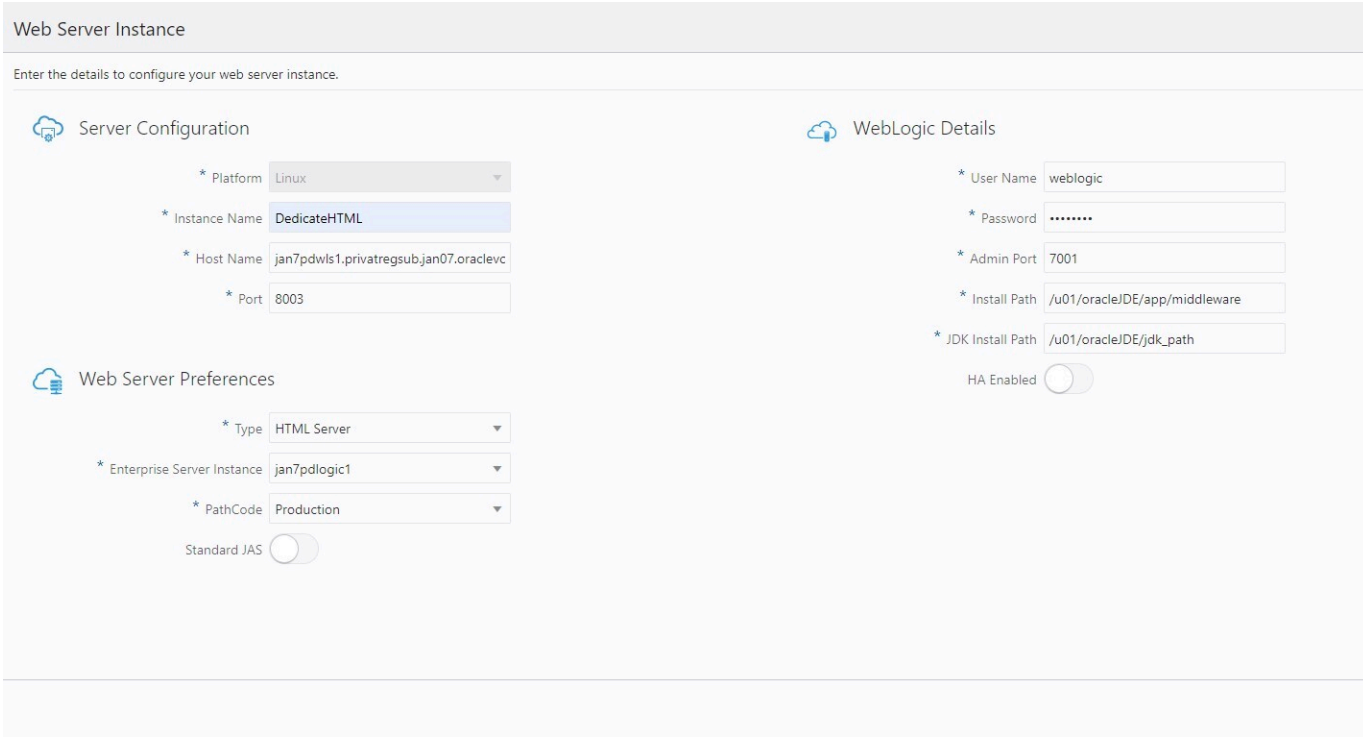
  Enter the user name.
- *Password*

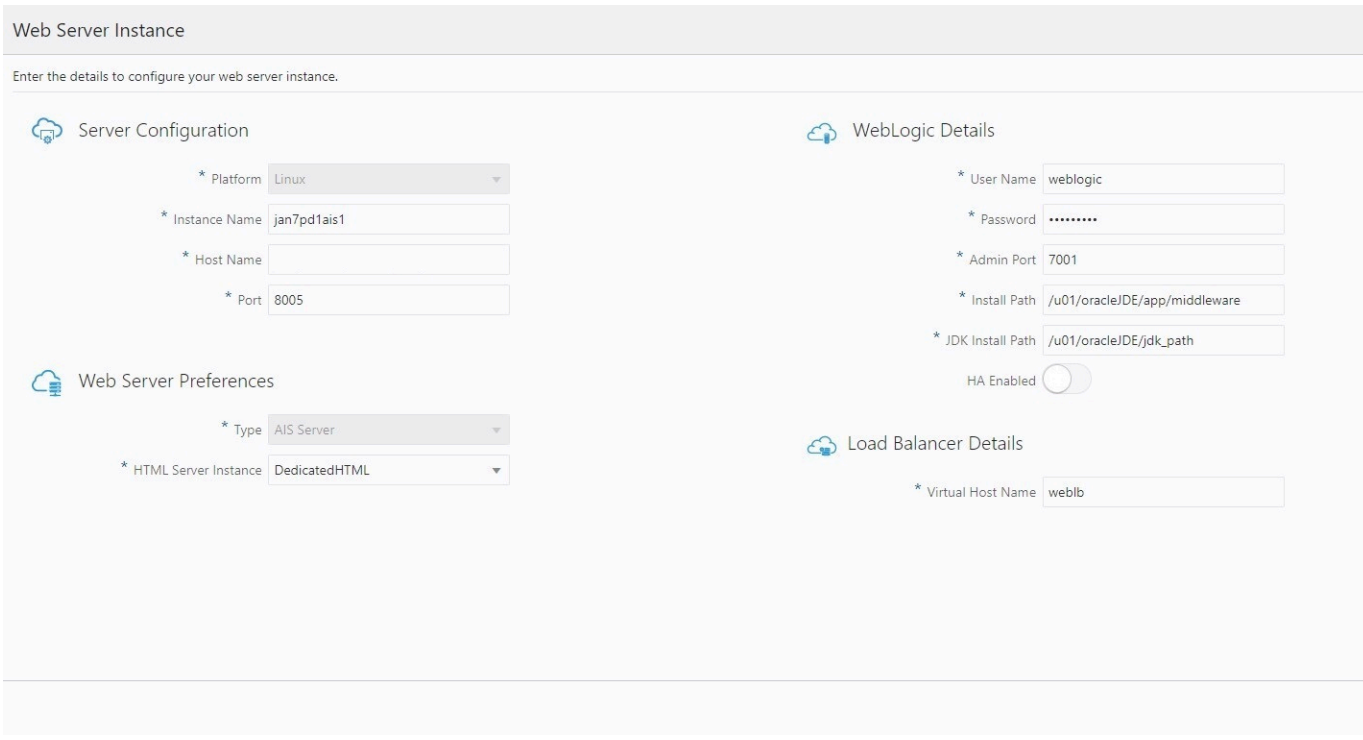
  Enter the WebLogic Server password.
- *Admin Port*

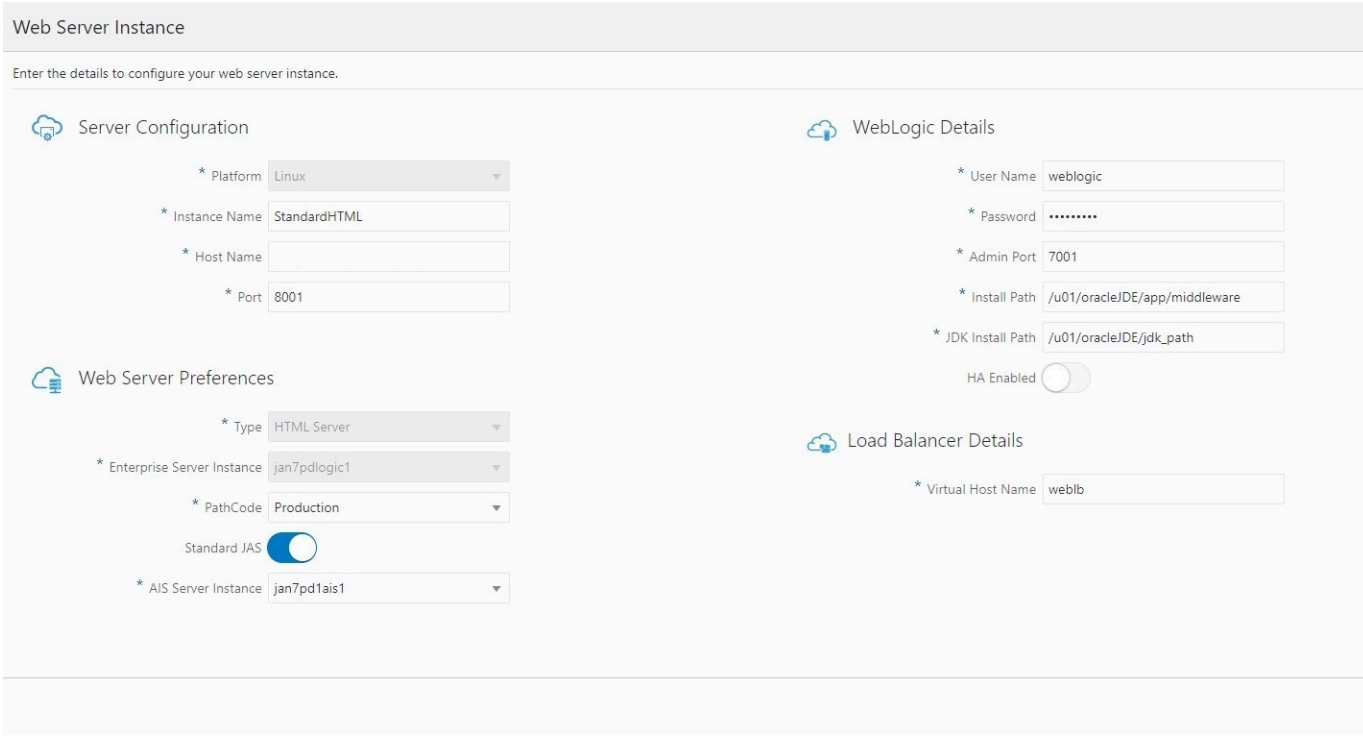
  Enter the port number to access the WebLogic Administration Console.
- *Install Path*

  Enter the installation path of the WebLogic instance.
- *JDK Install Path*

  Enter the JDK installation path.

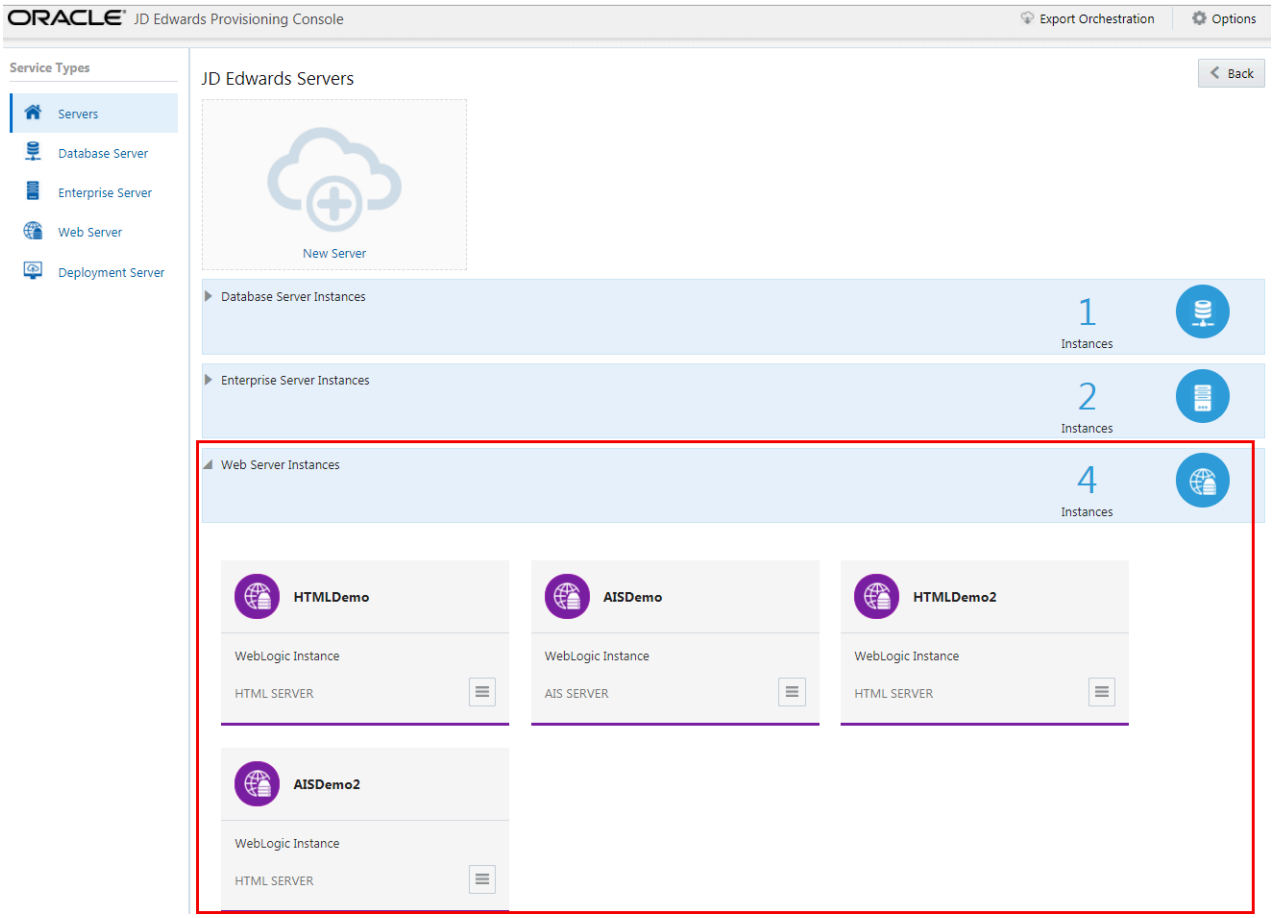

Web Server Instance
Enter the details to configure your web server instance.
Server Configuration
* Platform Linux
* Instance Name DedicateHTML
* Host Name jan7pdwls1.privatregsub.jan07.oraclevc
* Port 8003
WebLogic Details
* User Name weblogic
* Password ••••••••
* Admin Port 7001
* Install Path /u01/oracleJDE/app/middleware
* JDK Install Path /u01/oracleJDE/jdk_path
HA Enabled
Web Server Preferences
* Type HTML Server
* Enterprise Server Instance jan7pdlogic1
* PathCode Production
Standard JAS


Web Server Instance
Enter the details to configure your web server instance.
Server Configuration
* Platform Linux
* Instance Name jan7pd1ais1
* Host Name
* Port 8005
WebLogic Details
* User Name weblogic
* Password ••••••••••
* Admin Port 7001
* Install Path /u01/oracleJDE/app/middleware
* JDK Install Path /u01/oracleJDE/jdk_path
HA Enabled
Web Server Preferences
* Type AIS Server
* HTML Server Instance DedicatedHTML
Load Balancer Details
* Virtual Host Name weblb



4. Click the **OK** button.

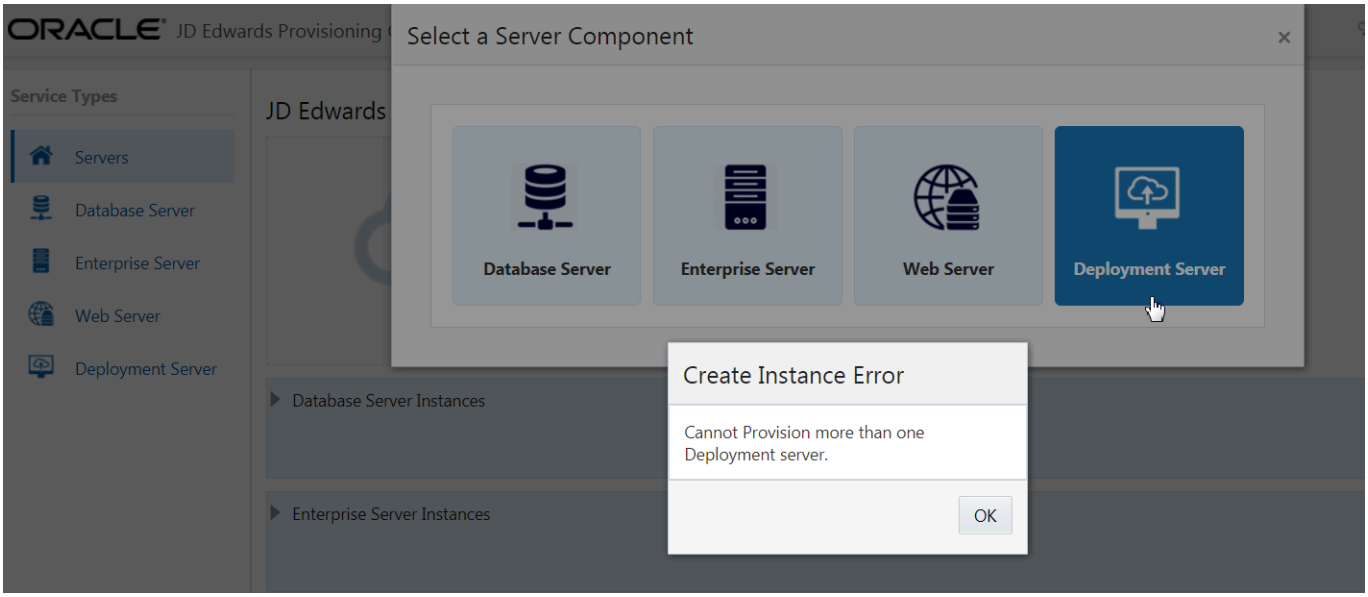
5. Verify the Web Server instances you modified or added is displayed in the JD Edwards Servers window.



6. To delete any web instance, use the Application Options tab to select **Delete.**

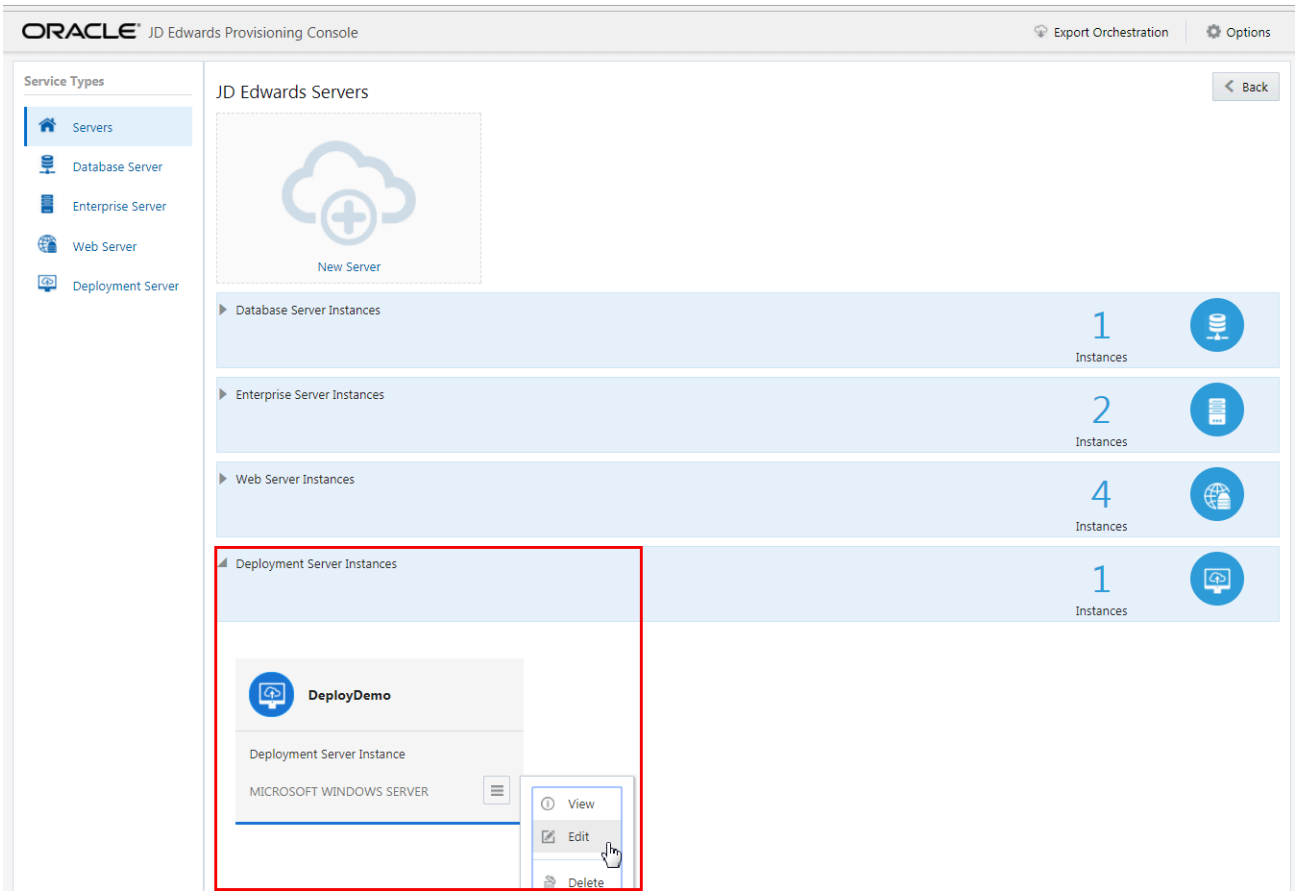
Deployment Server

You can use only one Deployment Server per deployment. If you attempt to add more than one Deployment Server, the Provisioning Console displays an error.


ORACLE JD Edwards Provisioning
Service Types
Servers
Database Server
Enterprise Server
Web Server
Deployment Server
JD Edwards
Database Server Instances
Enterprise Server Instances
Select a Server Component
Database Server
Enterprise Server
Web Server
Deployment Server
Create Instance Error
Cannot Provision more than one Deployment server.
OK

To modify the Deployment Server instance:

1. On JD Edwards Servers, click the existing Deployment Server instance, click the **Applications Options** icon, and then click **Edit**.



2. On JD Edwards Deployment Server page, complete these fields to create and configure your Deployment Server instance.

   Server Configuration

   - Instance Name

     Create a name for the Deployment Server instance. The conditions to set the instance name is displayed in the tooltip when you click the field.
   - Host Name

     Enter the host name.
   - Windows User

     Enter the name of the Windows user.
   - Windows Password

     Enter the password of the Windows user.

   Deployment Server Preferences

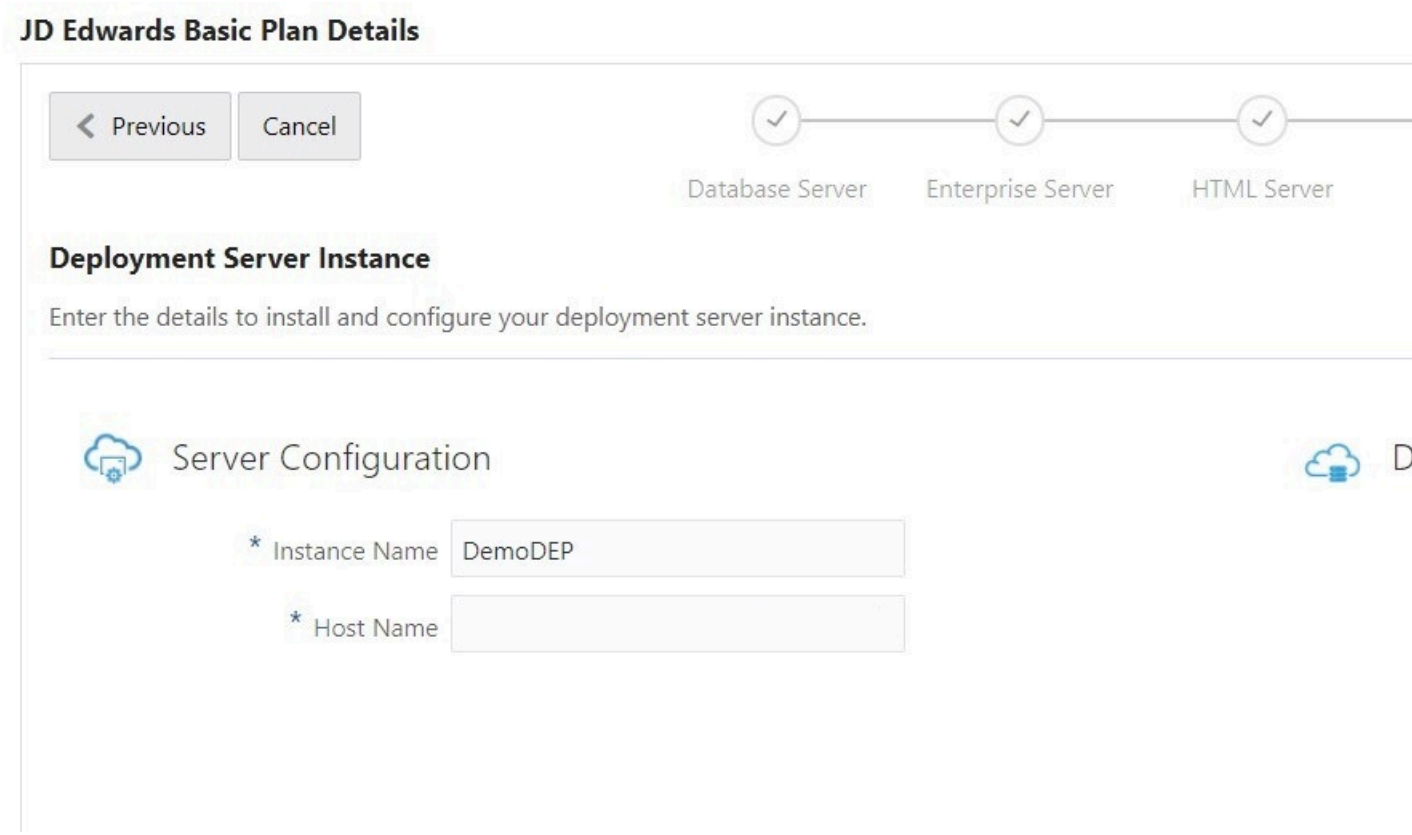
   - *Location*

     Enter the location.

     This value is the base location for your JD Edwards EnterpriseOne machines. For example, typical values might be a city name (such as Denver or Austin), a geographical region name (such as US or India), or a general location name (such as Corporate).
   - *Installation Drive*

     Enter the drive for the installation.
   - *Pathcodes*

     This field is automatically populated.



3. Verify that the Deployment Server instance you modified is displayed in the JD Edwards Servers window.
4. You can choose the **Delete** option in the action tab to delete the Deployment Server instance. After you delete the existing Deployment Server instance, you can click the **New Server** icon, and then select Deployment Server from the Select a Component page to add a new Deployment Server instance.

Note: To deploy an orchestration, refer to the section of this tutorial entitled: ***Deploying an Orchestration.***

8 Deploying JD Edwards EnterpriseOne

Deploying an Orchestration

This section shows you how to deploy an Orchestration.

You can create a Quick Start or an Advanced Deployment Plan in the Orchestrate section of the JD Edwards One-Click Provisioning Console. When you start your deployment, the system initiates the scripts for the automated provisioning of the EnterpriseOne system.

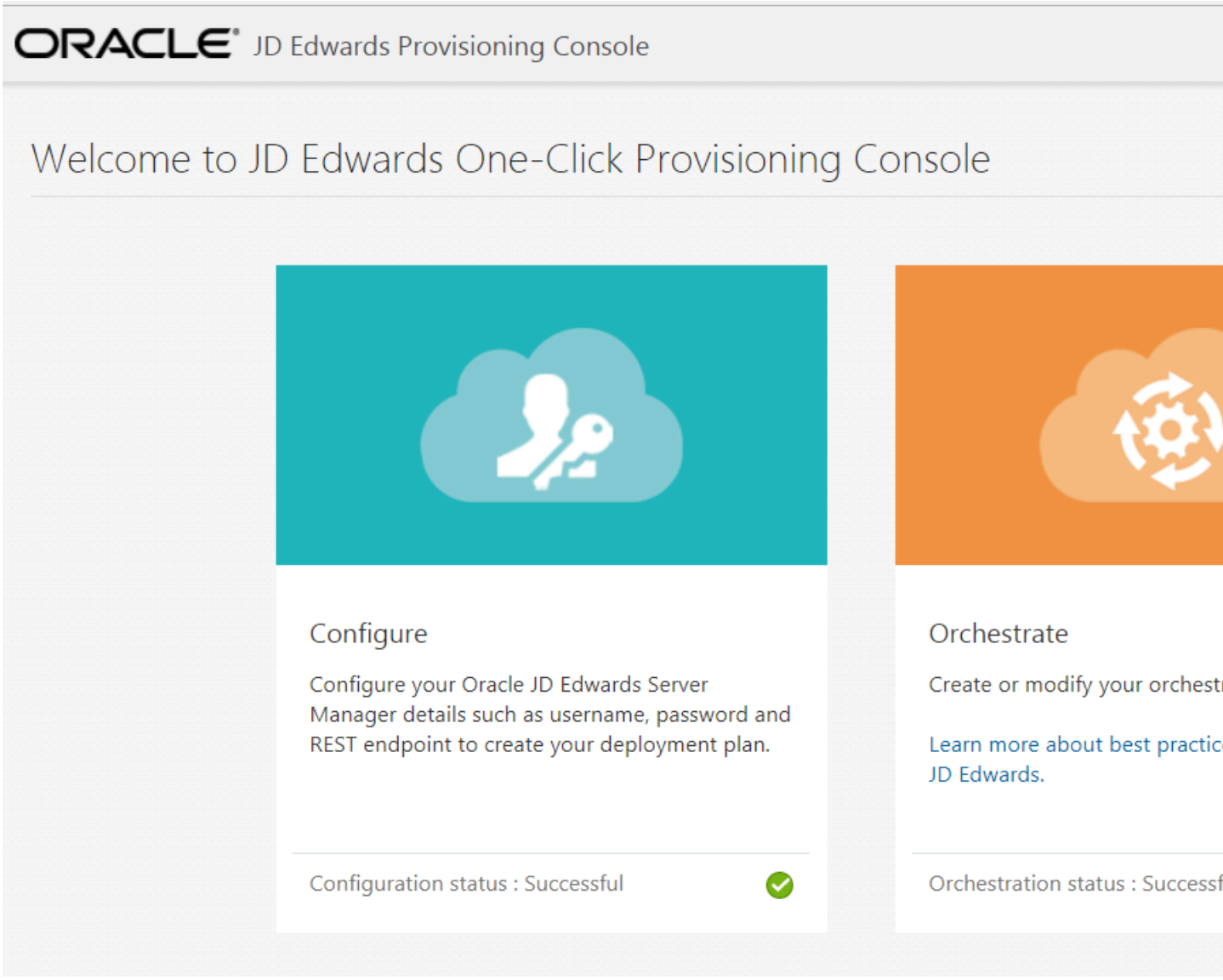
Prerequisite

A completed Quick Start or an Advanced Deployment Plan created using the JD Edwards One-Click Provisioning Console.

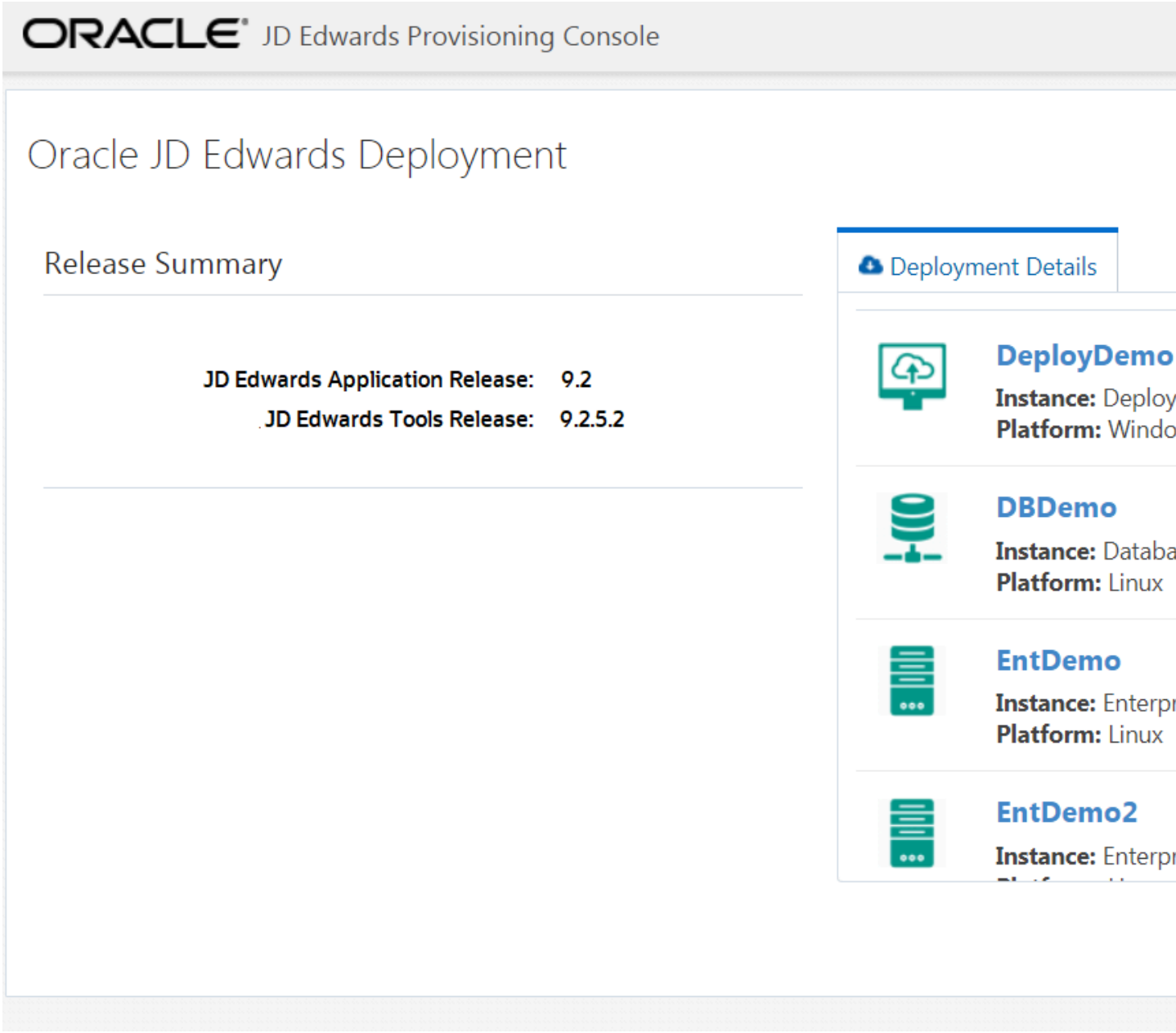
Deploying an Orchestration

This procedure describes how to deploy an orchestration, whether it is a Quick Start or an Advanced mode Deployment Plan.

1. After you create a Deployment Plan, from the JD Edwards Provisioning Console, click the **Deploy** icon.

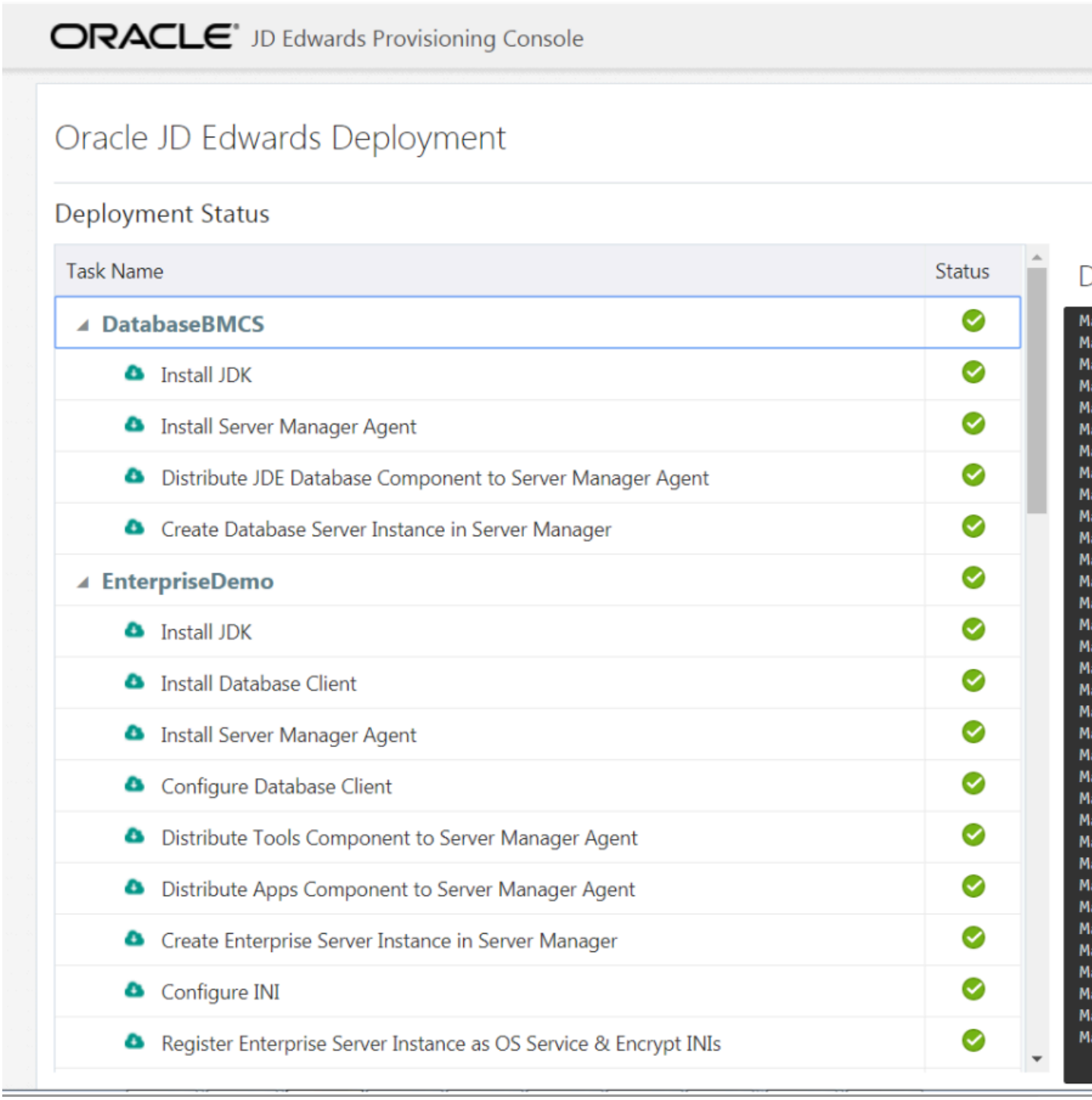


2. To view the Account details and Global Settings Summary, in the **Deployment Details** tab click the "**>**" icon for each server in the Deployment Details to see the details of the servers you provisioned.



3. Click the **Back** button if required to make additional changes to the server instances.
4. To start the deployment, click the **Start Deployment** button.

5. On Deployment Status, you can see all the instances and task details and their progress. You can also view the log or summary of each of the tasks. The time taken to deploy the servers depends on your customization.



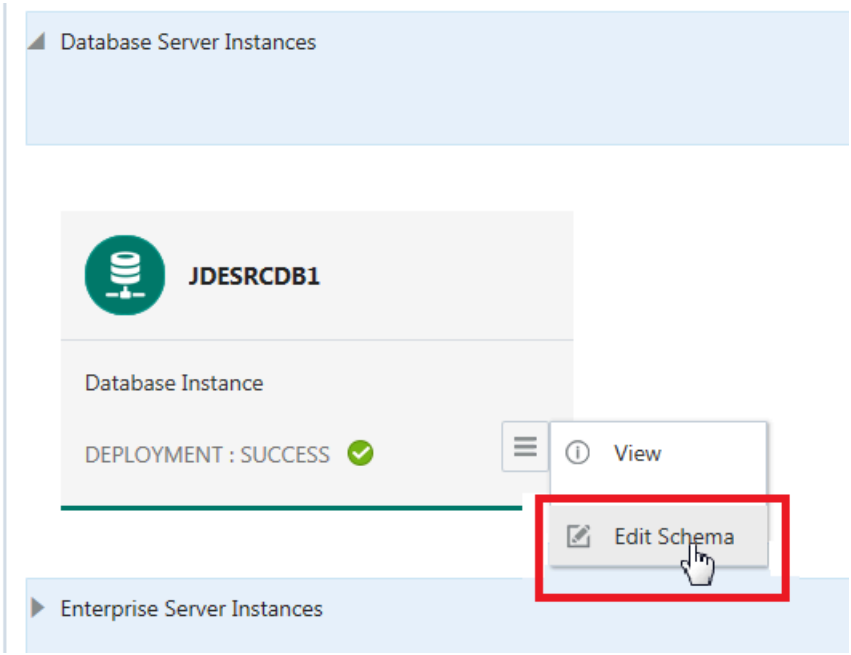
6. Click the **Back** button if you want to go back to the Deployment Summary window.

Adding Additional Pathcodes Post Deployment

You can add additional pathcodes to the Database Server instance after the deployment is successful.

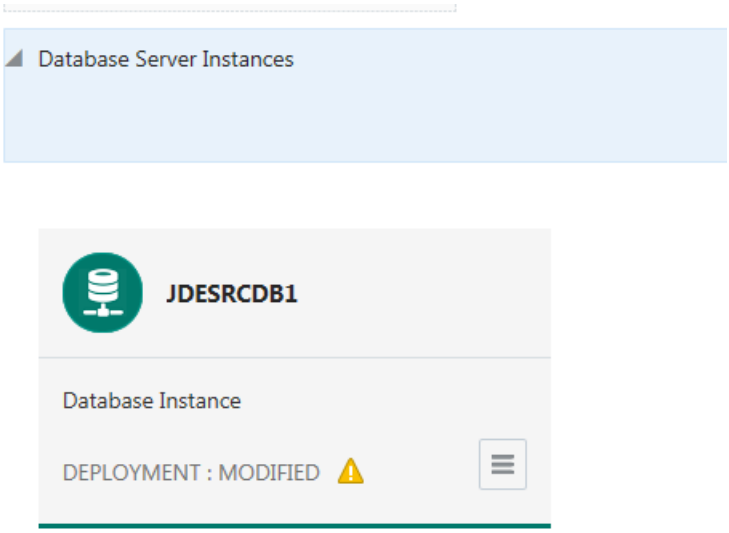
To add additional pathcodes:

1. On Welcome to the JD Edwards Provisioning Console, click the **Orchestrate** icon.
2. On JD Edwards Servers, click on **Database Server Instances**.
3. Select the Database Server instance, and then use the action tab to choose **Edit Schema** option.



4. On Existing Database Instance Details, select the available pathcodes. An error message window appears if you attempt to delete the previously installed schema or the demo data.
5. Click the **OK** button.

6. Now you can see the Deployment status as **MODIFIED**.



7. Click the **Back** button, and then click **Deploy** icon to start your modified deployment.

Orchestrating an Advanced Deployment Plan by Adding Web Servers and Enterprise Servers Post Deployment

This section shows you how to orchestrate an advanced deployment plan by adding Web Servers and Enterprise Servers post deployment.

You can add additional Web Servers and Enterprise Servers after you complete your Deployment. You cannot add any other server type after the deployment.

Prerequisite

Successfully completed the Deployment of a Quick Start or an Advanced Deployment Plan using the JD Edwards One-Click Provisioning Console. These tasks are described in preceding sections of this Learning Path.

Orchestrating an Advanced Deployment Plan by Adding Web Servers and Enterprise Servers Post Deployment

To add additional servers post deployment:

1. On JD Edwards One-Click Provisioning Console, click the **Orchestrate** icon .
2. On JD Edwards Servers, click the **New Server** icon, and in the Select a Component window, select **Web Server**.
3. On Web Server Instance Details, enter appropriate values for your installation.
4. Click the **OK** button. Similarly, you can add new Enterprise Servers.
5. On JD Edwards Servers, click the **Back** button.
6. On **JD Edwards One-Click Provisioning Console**, click the **Deploy** icon.

7. On **JD Edwards Deployment** window, review the deployment summary. You can verify the newly added servers in the **Deployment Details** tab.

   Note: To deploy an orchestration, refer to the section of this guide entitled: ***Deploy an Orchestration.***

9 Saving and Reusing Deployment Plans

Exporting an Orchestration

This section shows you how to export an orchestration.

You can use the export and import functions of the JD Edwards Provisioning Console to save an existing orchestration (export) and to reuse (import) the saved orchestration.

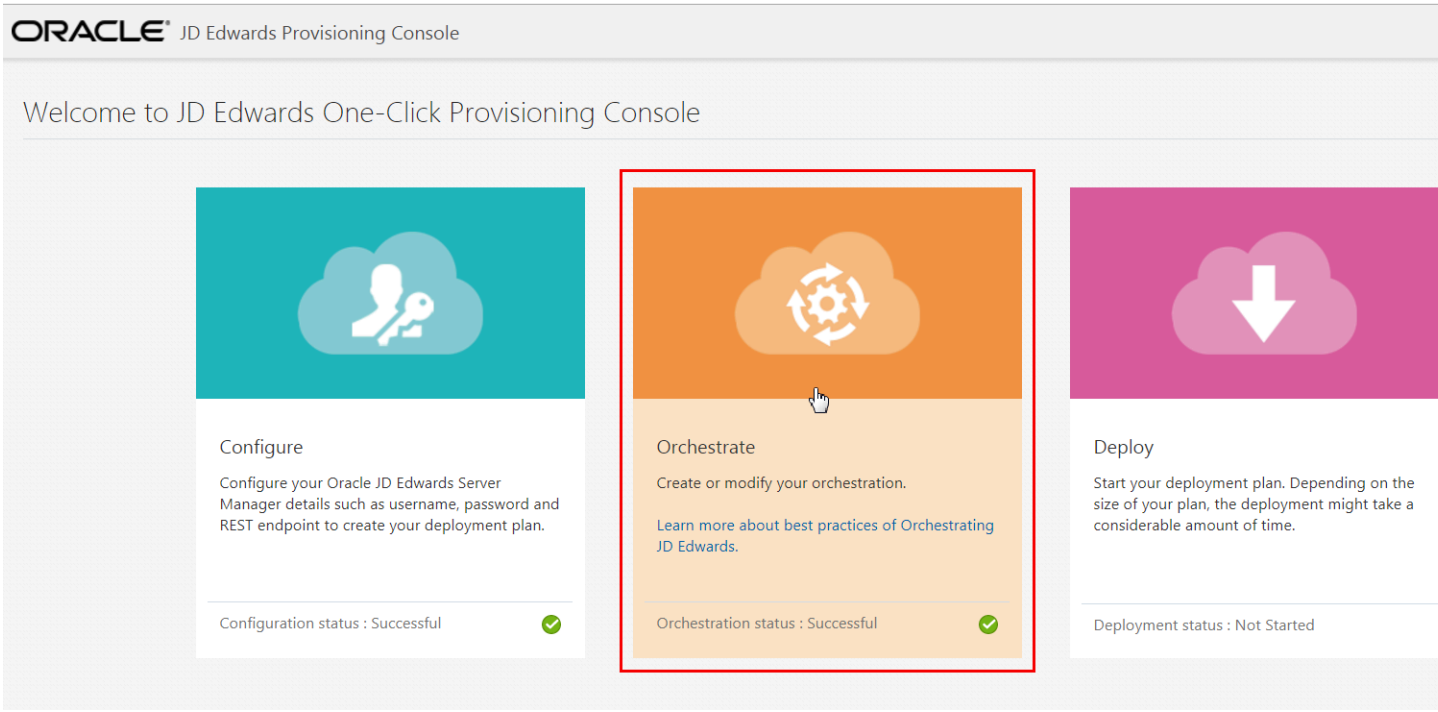
Prerequisite

A completed Quick Start Deployment Plan or an Advanced Deployment Plan created using the JD Edwards One-Click Provisioning Console.

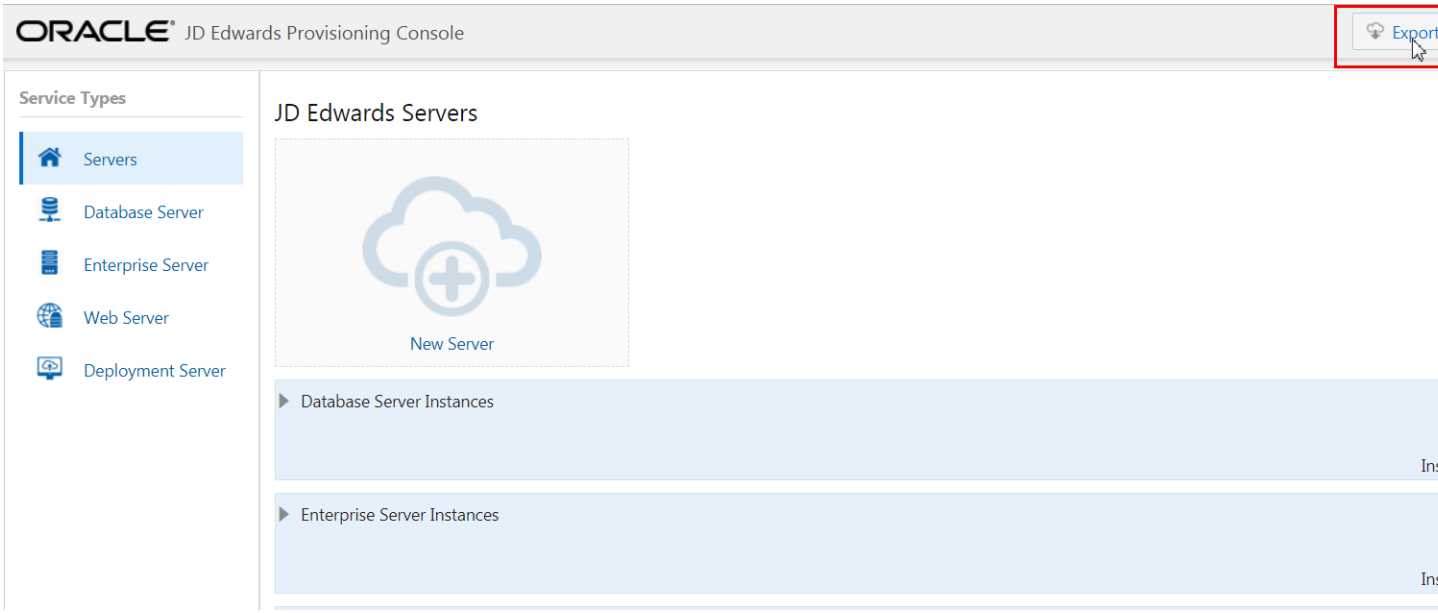
Exporting an Orchestration

To export an orchestration:

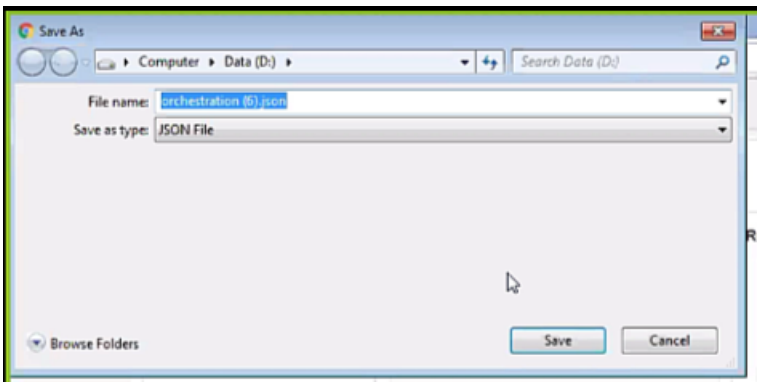
1. On the JD Edwards Provisioning Console window, click the **Orchestrate** icon.



2. To export an existing orchestration, on an existing orchestration, from the title bar select **Export Orchestration**.



3. On the **Save As** dialog box, choose a path and file name for the exported orchestration.



4. Click the **Save** button.

Note: If you want to view the raw contents of the .json file, you can open the file in an ASCII editor as shown in the following screenshot.

orchestration.json

```
{
    "depServer": [
        {
            "instanceName": "DeployDemo",
            "serviceType": "VM",
            "hostDetails": {
                "serviceName": "depfinalAD2",
                "userName": "opc",
                "password": "ADQW20jVUBBtKxl/LBDSbx/rIAsraf0DTJAA==",
                "osPlatform": "WINDOWS"
            },
            "serverDetails": {
                "dependentServer": "DBDemo",
                "pathcodes": [
                    "DEVELOPMENT",
                    "PRISTINE",
                    "PROTOTYPE",
                    "PRODUCTION"
                ],
                "jdeLocation": "Corporate",
                "setupDrive": "D:"
            }
        }
    ],
    "databaseServer": [
        {
            "instanceName": "DBDemo",
            "serviceType": "VM",
            "hostDetails": {
                "serviceName": "dbad2",
```

Importing an Orchestration

This section shows you how to import an orchestration.

You can use the export and import functions of the JD Edwards Provisioning Console to save an existing orchestration (export) and to reuse (import) the saved orchestration.

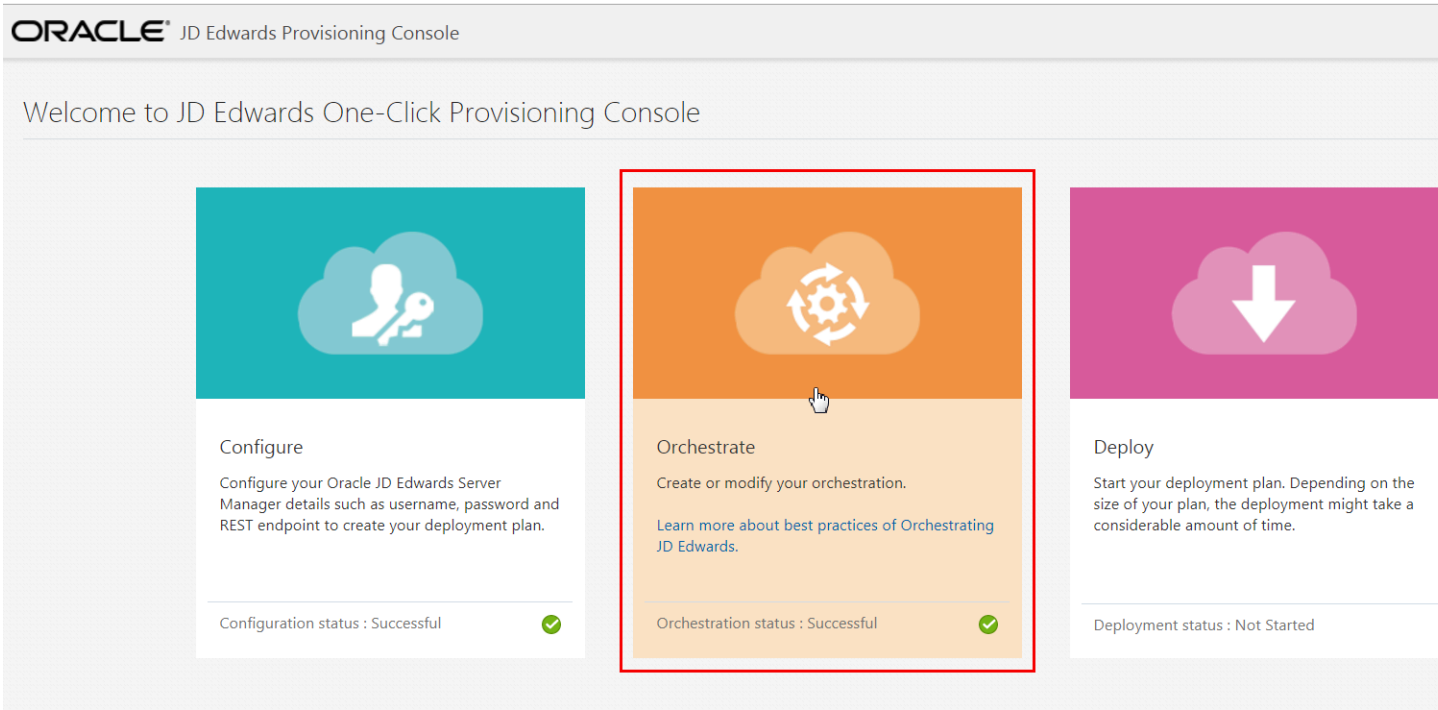
Prerequisite

You must have configured the administrator passwords for WebLogic Server and Server Manager Console in the Configure section of the JD Edwards One-Click Provisioning Console.

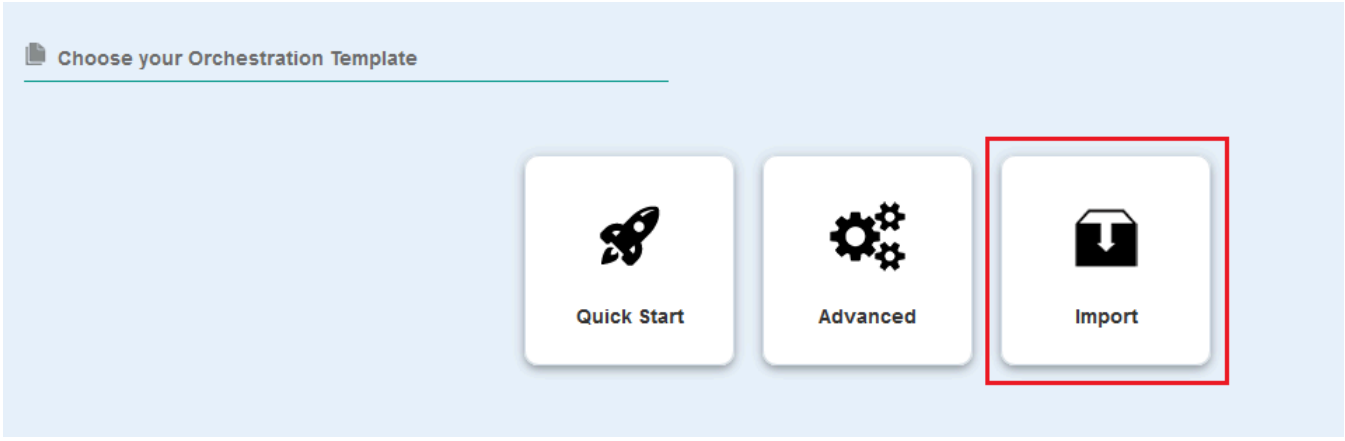
Importing an Orchestration

To import an existing exported orchestration:

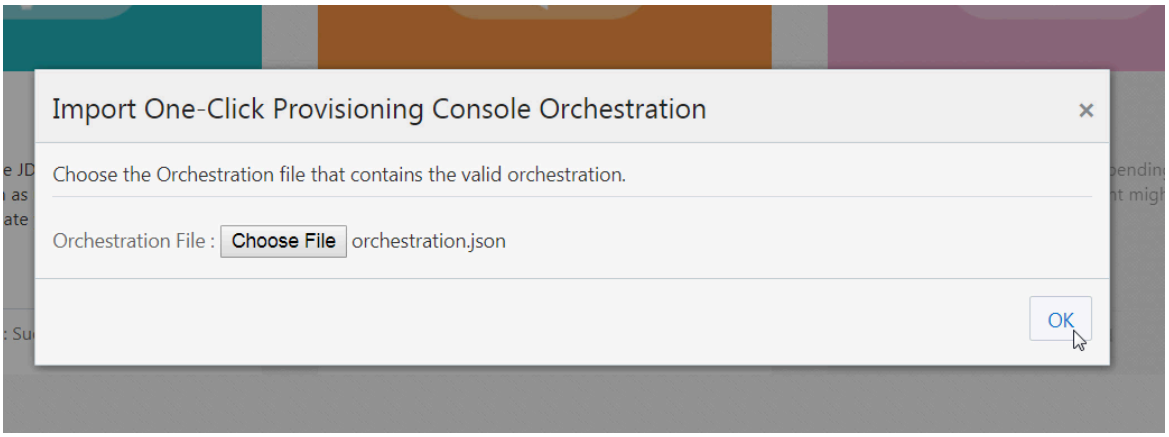
1. On the JD Edwards Provisioning Console, click the **Orchestrate** icon.



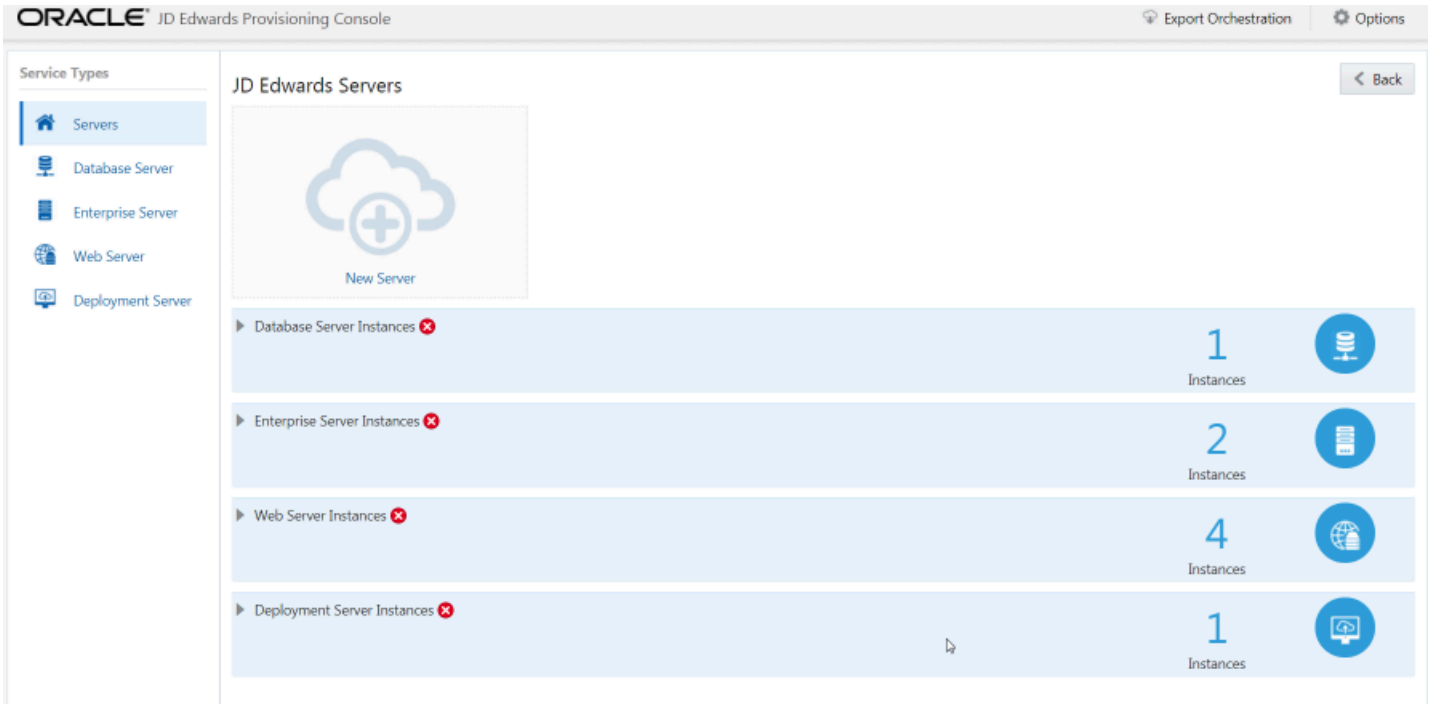
2. Click the **Import** icon.



3. On the Import One-Click Provisioning Console Orchestration window, click **Choose File**, and then browse and select the exported `.json` file.



Note: If an error exists in the orchestration file you imported, the system displays the details of that error. Also, the system displays an error as illustrated in the following screenshot, if password authentication is required. You must edit the instance, enter the required password, and then save the instance.



10 Configuring JD Edwards Components Post Deployment

Performing Post Installation for the Deployment Server

This section shows you how to perform post installation for the Deployment Server.

After you successfully provision all the Servers using the One-Click Provisioning Console, you must build packages on your Deployment Server.

Prerequisite

The complete Visual Studio product (which includes the runtime, the compiler, and associated tools) must be purchased and licensed from Microsoft.

- JD Edwards EnterpriseOne Applications Release 9.2 requires runtime libraries and the full product for Visual Studio.

General

The Deployment Server that is deployed by the Provisioning Server includes all the required third-party products including a JDK, E1Local Oracle database, and the EnterpriseOne database client. If you will be performing package builds, refer to the subsection entitled: Package Build Considerations.

Accessing the Deployment Server

You can access your Deployment Server using Microsoft Windows Remote Desktop Protocol (RDP).

- For One-Click Provisioning, you will need the Public IP address of the Deployment Server and the password.
- For Infrastructure Provisioning, you will need to connect as described in the section entitled "Connecting to a Windows Host in a Private Network Through the Bastion Host".

For information regarding the Public IP address, refer to the section of this Learning Path entitled: ***Accessing the JD Edwards EnterpriseOne Servers Using Their Public IP Addresses.***

The password for the Deployment Server was assigned when you input values in the **Deployment Server Instance** screen in the preceding sections of this Learning Path that are titled: ***Orchestrate a Quick Start Deployment Plan*** . If you followed the recommendation, this password should be recorded on the ***Pre-Install Worksheet*** .

Package Build Considerations

In order to build packages on your Deployment Server, you will need to:

- Install Microsoft Windows Visual Studio and Windows SDK
- Update Visual Studio Version in the jde.ini File
- Refresh CNC Data in JDEPLAN
- Build a New Client Package

- Build a New Server Package

Install Microsoft Windows Visual Studio and Windows SDK

The One-Click Provisioning Server delivers a Deployment Server to Windows 2022 Standard with most of the software already installed with the exception of Microsoft Windows Visual Studio and Microsoft Windows Software Development Kit (SDK). Refer to the JD Edwards Deployment Server Certification page for current updates on supported software versions and software prerequisites. The Certification page can be accessed through the Oracle Support Portal:

https://www.oracle.com/support/index.html

The Visual Studio runtime libraries (which are partial products with no development tools) for each supported release of Visual Studio are freely available from the Microsoft Download Center. The complete Visual Studio product (which includes the runtime and the compiler and associated tools) must be purchased and licensed from Microsoft.

As of the general availability of JD Edwards EnterpriseOne One-Click Provisioning for Tools Release 9.2, the following versions and associated links and navigation are valid.

- **Visual Studio 2022 Full Product**

  > **Note:** You need Visual Studio 2022, which is a licensed product from Microsoft, if you plan on building packages on the Deployment Server. *https://visualstudio.microsoft.com/downloads/*

- **Microsoft Software Development Kit (SDK) for Windows 11**

  > **Note:** Although the SDK download is labelled as Microsoft Windows 11, the same download is applicable to both Windows Client 11 and Windows Server 2022. This SDK is specifically required for any Microsoft Windows-based machine that is building JD Edwards EnterpriseOne packages.Windows Software Development Kit Version 10.0.22621.0 *https://msdn.microsoft.com/en-us/windows/downloads/sdk-archive*

Update Visual Studio Version in the jde.ini File

Ensure that you set the correct version of Visual Studio in the `[JDE_CG]` section of the `jde.ini` file on the Deployment Server. For details, refer to this document on Oracle Technology Network (OTN) for instructions:

JD Edwards EnterpriseOne Development Client Installation Guide for Oracle WebLogic Server (WLS) and WebSphere Application Server (WAS) Express.

- Understanding the Development Client Installation
- Installing Compiler, Linker, and Software Development Kit (SDK)
- Updating the jde.ini File

Refresh CNC Data in JDEPLAN

The ESU process has changed to include automatic generation of OCM mappings and tables for tables that are not in Business Data. In order for this process to work correctly, you must update the CNC information in JDEPLAN before applying any Tools-related ESUs. Also if you have multiple Enterprise Servers, Database Servers, or both, you must perform this procedure in order to synchronize data between the System and Planner pathcodes before you proceed further.

1. Sign into JDEPLAN.

2. Run R9840C, and copy system/planner information

   from: System – 920

   to: Planner – 920

   > **Note:** R9840C will copy any missing CNC from System to Planner.

3. Run R98403A, choosing version XJDE0004, for syncing the data from System – 920 to Planner – 920 database.
4. Change the Data Selection to F98611.
5. Change the Processing Options as follows:
   - Source Data Source = System – 920
   - Target Data Source = Planner – 920
   - Proof Mode = 1
   - Replace Duplicates = Y
   - Clear Table = N

Using these processing options, running the R98403A will add any missing data source definitions in JDEPLAN with the correct definitions from System – 920.

Build a New Client Package

You must build a new Client package in order to obtain source files for the path code and to build future update packages against.

> **Note:** Update packages against the delivered FA packages (PS920FA, PY920FA, PD920FA, and DV920FA) is not supported.

Due to space considerations on the `D:\` drive, you will need to move the `D:\Software` directory and all of its contents to the `C:\` drive or another computer. For example:

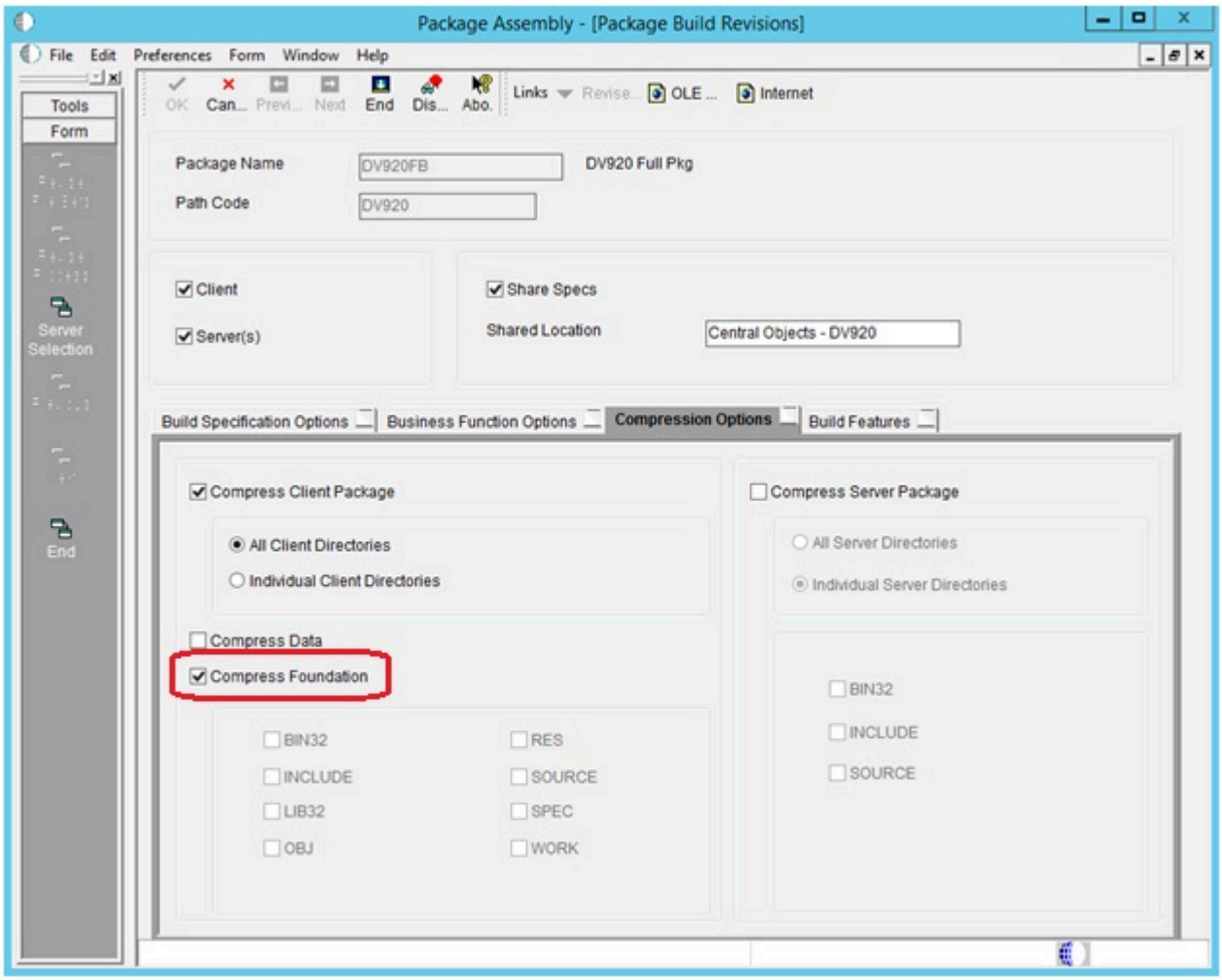
1. Add a new directory under the `C:\` drive labeled:

   `C:\SoftwareBKUP`
2. Copy the `D:\Software` directory (and all its contents) to the `C:\SoftwareBKUP` directory.
3. Delete the `D:\`Software directory.

Complete the following steps to build a full package by following the standard procedure to build a full package with the following important distinctions.

> **Note:** The creation of update packages against the delivered FA packages (PS920FA, PY920FA, PD920FA, and DV920FA) is not supported. In order to build update packages in the future, you must build and deploy a new full package.

1. On the last screen of the Build Definition, on Package Assembly – [Package Build Revisions], select the Compression Options tab.
2. Ensure the **Compress Foundation** check box is selected. This is required to recompress the system folder on the Deployment Server to create a new systemcomp directory that includes a JRE. This JRE is required for use by the Development Client.



Note: If you encounter NER failures during your full package build (server side only), to resolve these failures refer to the My Oracle Support Doc Id 1950295.1 at this link: *https://support.oracle.com/epmos/faces/DocumentDisplay?id=1950295.1*

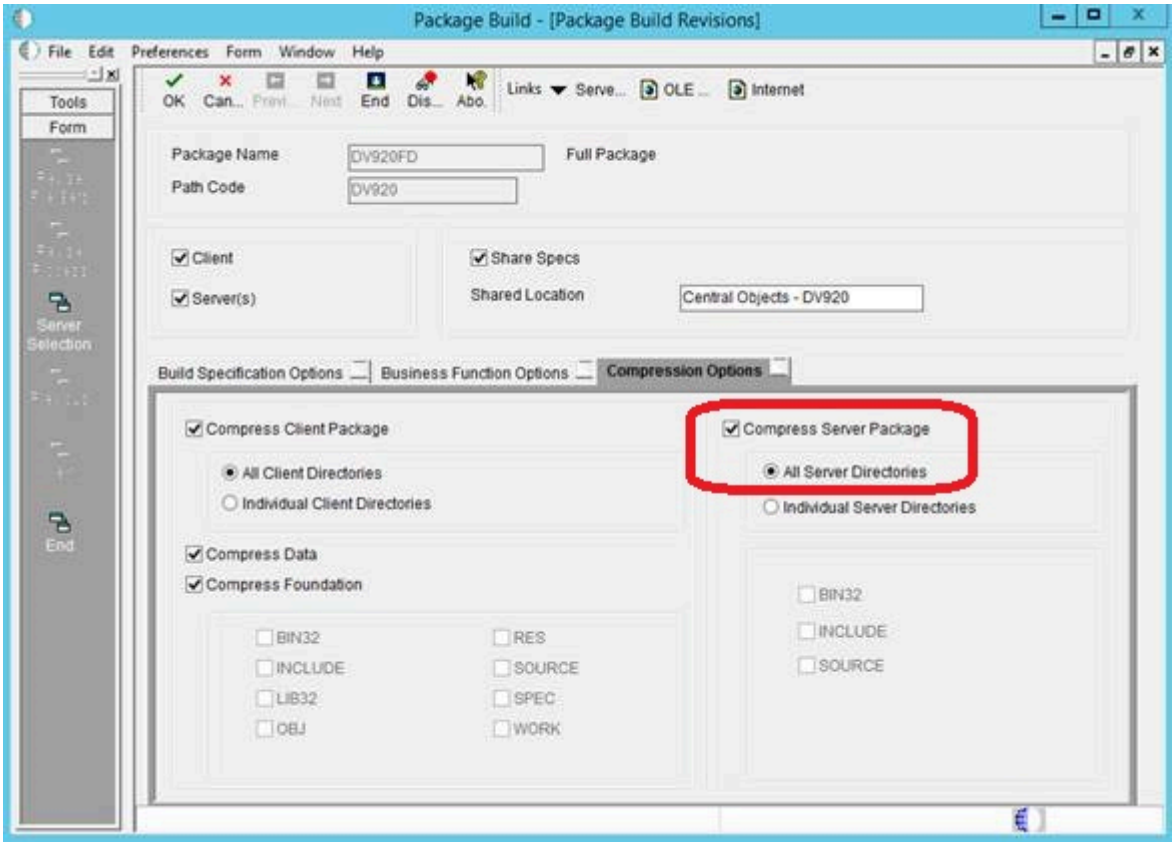
Build a New Server Package

As a best practice it is strongly recommended that you build a new server package. For multiple Enterprise Server environments, the procedures in this section are mandatory.

On Package Build, Package Build Revisions, in addition to the normal compression options, you must select these additional options during the package build process for any full package:

- **Compress Server Package**

- **All Directories**



Performing Postinstallation for the Standalone Deployment Server with Oracle Database

This section shows you how to perform the post installation tasks for the standalone Deployment Server with Oracle database.

> **Note:** This section is *only* applicable if you have deployed a standalone Deployment Server with Oracle database using One-Click Provisioning.

You can use One-Click Provisioning to install a standalone Deployment Server. A standalone Deployment Server is deployed when you first use One-Click Provisioning to provision a Deployment Server only, and then use One-Click Provisioning to provision other servers such as the Database Server, Enterprise Server, and HTML Server. This section describes how to complete the postinstallation steps for such a standalone Deployment Server.

If you have used One-Click Provisioning to deploy a standalone Deployment Server (that is, you did not use One-Click to initially deploy a complete system), you must perform the following procedure on your Deployment Server to enable access by JD Edwards EnterpriseOne.

Enable DEP920 Login for an Oracle Database

> **Note:** This section is only applicable if your deployment of JD Edwards EnterpriseOne includes an Oracle Database Server.

After you have used One-Click Provisioning to deploy the complete suite of JD Edwards EnterpriseOne servers, you need to enable EnterpriseOne access to the Oracle database from the Deployment Server.

1. Access the Deployment Server as described in the preceding section "Accessing the Deployment Server".
2. Edit the jde.ini file, which is typically located in this directory:

   ```
   c:\Windows
   ```
3. Edit the jde.ini file to provide a valid value for the **SecurityServer**= setting. This is the machine name for your Enterprise Server. For example:

   ```
   [SECURITY]

   SecurityServer=oraes
   ```
4. Save and close the `jde.ini` file.
5. Navigate to the location of the Oracle Client that is installed on your Deployment Server. For example:

   ```
   C:\JDE\oracle1212\product\client_1\network\admin
   ```
6. In the above directory, edit the `tnsnames.ora` file to add the listener details. You can copy these details from the `tnsnames.ora` file on your Server Manager machine or your Enterprise Server machine. This `tnsnames.ora` file is located in the same location on each machine. From the Server Manager, use this navigation to find this `tnsnames.ora` file on either the Server Manager machine or the Enterprise Server:

   From the HTML Server, select DATABASE, and then select Tnsnames.

   For example, this is the listener section you should copy:

   ```
   JDEORCL =
    (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = oradb.subnet.vcn.com)(PORT = 1521))
    (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = jdeorcl.subnet.vcn.com)
    )
   )
   ```
7. Save and close the `tnsnames.ora` file.
8. Navigate to the location of the E1Local Network, which is typically:

   ```
   C:\JDE\DEP\Oracle\E1Local\NETWORK\ADMIN
   ```
9. In the above directory, edit the `tnsnames.ora` file to add the same listener details that you obtained and copied in a previous step in this procedure.
10. Save and close the `tnsnames.ora` file.
11. Validate the configuration of the tnsnames.ora file by running `ActiveConsole.exe` and logging in to the DEP920 environment.

Considerations for Development Client

This section explains the required considerations before you create the Development Clients.

Prerequisites

- If you want to install a JD Edwards EnterpriseOne Development Client that will work with JD Edwards EnterpriseOne One-Click Provisioning, you must manually provision an additional Microsoft Windows machine. After the Microsoft Windows machine is provisioned, the process to set up and install a Development Client is the same regardless of where the client is installed.
- You must also install all the required third-party software and build a full client package on the Deployment Server.
- Refer to the *JD Edwards EnterpriseOne Development Client Installation Guide* for detailed instructions.

Considerations for Development Client

Consider the following requirements before you create the Development Clients:

- Microsoft Windows machines must be on the same private network on which the JD Edwards EnterpriseOne Database Server and Enterprise Server exist, and the machines must be able to communicate with those servers.
- Ensure that a full package build is completed on the Deployment Server. This package build creates the Development Client package installation. The delivered FA package will technically install a Development Client, but such a Development Client is not suitable for most developer activities.
- Ensure that IPv6 is disabled on the Microsoft Windows machine on which you will install the JD Edwards EnterpriseOne Development Client.
  Run this command to disable IPv6:
  ```
  reg add hklm\system\currentcontrolset\services\tcpip6\parameters /v DisabledComponents /t REG_DWORD /d 0xFFFFFFFF
  ```
  Use **ipconfig** to verify that the status of IPv6 is set to disabled.

Obtaining and Installing CA Certificates in the Oracle WebLogic Servers and the Deployment Server

This section shows you how to obtain and install CA Certificates in the Oracle WebLogic Servers and the Deployment Server.

The deployment of JD Edwards EnterpriseOne One-Click Provisioning includes temporary Certificate Authority (CA) certificates. Because these certificates are set to expire at preset and non-extendable times, you must obtain and install your own CA certificates. These must be certificates that are verified by a verified CA authority such as Entrust and Symantec Corporation.

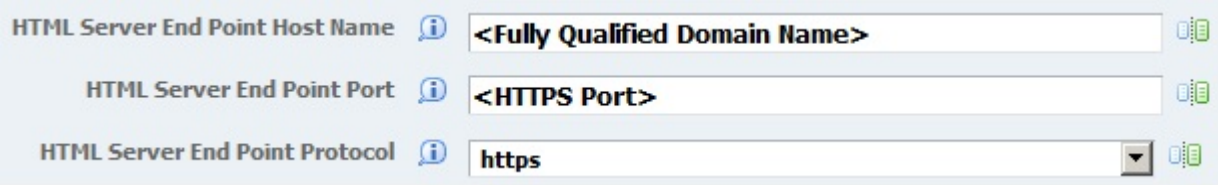
Prerequisite

Installed Java Keystore.

The following outlines the general procedure to create a Keystore and to generate a Certificate Signing Request (CSR).

1. In your local environment, obtain and install a Java Keystore. This is a repository for security certificates – either authorization certificates or public key certificates – plus corresponding private keys. These keys are used for SSL encryption by the Oracle WebLogic Server. A file with extension jks serves as keystore.
2. From the Keystore, generate a Certificate Signing Request (CSR).
3. Export the Certificate Signing Request (CSR).
4. Validate the CSR. For example, you could use the validation tools provided by Symantec such as "checker".
5. Submit the CSR to the Certificate Authority such as Entrust or Symantec Corporation.
6. Upon return receipt, import the validated certificates to the Keystore for each server. That is, each server that must communicate with another must have its own certificate ***plus*** that of the target server. In this case, the HTML Server must have its own certificate plus that of the AIS Server, and vice versa.
7. Logged in as the WebLogic Adminstrator, you must manually modify each of these instance of Oracle WebLogic Server within your One-Click deployment to use the new Keystore:
   - Server Manager Console
   - Each instance of a JD Edwards EnterpriseOne HTML Server (JAS)
   - Each instance of a JD Edwards EnterpriseOne AIS Server
8. You should also modify the parameters using Server Manager to use the https connection for communication between the HTML Server and the AIS Server.
   a. In the **HTML instance**, modify the following Web Runtime parameters to use https, a fully qualified domain name, and https port:

   b. In the **AIS instance**, modify the following HTML Server parameters to use https, a fully qualified domain name, and https port:



Tip: After you have SSL configured and tested, it is recommended that you disable all the non-SSL ports.

For additional details on working with CA certificates on your Oracle WebLogic Server, refer to this guide: *Administering Security for Oracle WebLogic Server.*.

11 Accessing the Provisioned Servers

Performing Post-Provisioning Tasks

This section shows you how to perform the post-provisioning tasks.

Prerequisite

Successfully completed a deployment plan using the Quick Start mode or the Advanced mode on the JD Edwards One-Click Provisioning Console.

Enabling Enterprise Server Predefined Ports

You must enable the predefined ports in the jde.ini file on the Enterprise Server. Use Server Manager to ensure this setting exists:

```
[JDENET]

enablePredefinedPorts=1
```

For Release 9.2, the `serviceNameListen` value is `6017`. The next port for use by the net services on the Enterprise Server is defined by the value `serviceNameListen+1` until the value set by `maxNetProcesses=` is reached, the default value being 6 net processes. Therefore, in the firewall on the Enterprise Server you must open ports 6018 through 6023 for use by the net processes. These ports cannot be in use by any other process running on the Enterprise Server. If they are already in use, then whichever program is using them must be reconfigured to use different ports.

Accessing the JD Edwards EnterpriseOne Servers Using the Host Name

This section shows you how to access the JD Edwards EnterpriseOne Servers using the host name.

Prerequisite

Successfully completed a deployment plan using the Quick Start mode or the Advanced mode on the JD Edwards One-Click Provisioning Console.

Accessing the JD Edwards EnterpriseOne Servers Using the Host Name

After the successful deployment of all the servers according to the orchestration created using the JD Edwards One-Click Provisioning Console, you can access these deployed JD Edwards EnterpriseOne Servers and Development Client by using the host name:

- Server Manager Console
- HTML Server
- AIS Server

- Deployment Server

Server Manager Console

After the Server Manager Console is started, you can access it using its host name using this syntax:

```
http://<Host Name>:8999/manage
```

For example:

```
http://abc.pqr.xyz:8999/manage
```

> **Note:** You should always use HTTP to access the Server Manager Console for normal operations. Although the Server Manager Console is also enabled for HTTPS/SSL protocol, such access is restricted for internal use as part of the REST/API functionality, and should not be used for normal operations.

HTML Server

After your HTML Server is deployed, you can access it using its host name using this syntax:

```
https://<Host Name>:<port as defined in orchestration>/jde/E1Menu.maf
```

> **Note:** The file name `E1Menu.maf` is case-sensitive and must be specified exactly as shown here.

For example:

```
https://abc.pqr.xyz:8001/jde/E1Menu.maf
```

AIS Server

After your AIS Server is deployed, you can access it using its host name using this syntax:

```
https://<Host Name >:<port as defined in orchestration>/jderest/defaultconfig
```

For example:

```
https://abc.pqr.xyz:8002/jderest/defaultconfig
```

Deployment Server

You can access your Deployment Server using Microsoft Windows Remote Desktop Protocol (RDP). To do so, you will need the public IP address of this instance.

12 Troubleshooting

Troubleshooting Your One-Click Deployment

This section shows you the list of troubleshooting topics and resolutions for your One-Click deployment.

One-Click Provisioning Console Troubleshooting Tips

This section contains the following troubleshooting tips for the EnterpriseOne One-Click Provisioning Console:

- Accessing a Previously Saved Provisioning Console Configuration
- Console Administration
- Console Service Status
- Start the Console
- Stop the Console
- View the Console Logs

Accessing a Previously Saved Provisioning Console Configuration

Symptom:	You cannot access a previously created Quick Start deployment plan.
Cause:	After you created a Quick Start deployment plan (either complete or partial), you exited the browser used to connect to the One-Click Provisioning Console.
Resolution:	When you next access the Provisioning Console, you are prompted to enter the same credentials that you entered for the first access to the console. Those credentials are the password for the Server Manager for JD Edwards EnterpriseOne. After the credentials are validated, you can access the previously saved configuration.

Console Administration

The One-Click Provisioning Console process is configured as a systemd service in the One-Click Provisioning Server image. The configuration file (`E1CloudConsole.service`) is located in this directory:

```
C:\JDE\bin\E1CloudConsoleWin.ps1
```

Console Service Status

Access the Task Manager and verify that node.exe is running in the Provisioning Server machine:

Start the Console

Run the following command in the power shell to start the One-Click Provisioning Console service.

```
PS C:\JDE> E1CloudConsoleWin.ps1
```

Outside the machine, you can access the One-Click Provisioning Console application using the below URL:

```
https://<#PUBLIC_IP#>:3000/
```

Stop the Console

Access the Task Manager and terminate the node.exe process if it is running in the Provisioning Server machine.

View the Console Logs

See the following One-Click Provisioning Console log files in `C:\JDE\PP\E1CloudConsole\logs`:

`E1ProvisionConsole.err`

`E1ProvisionConsole.out`

The input validation logs files are located in this path: `C:\JDE\PP\E1ProvisionPrime\InputValidation\log`

Press Page-Down to scroll through the logs.

Press Shift + G to scroll to the end of the log.

Note: The One-Click Provisioning Console logs are completely regenerated each time the console is run.

Enterprise Server Provisioning Fails - Communication Failure

Symptom:	Provisioning fails to deploy the Enterprise Server with an error returned indicating a communication failure.
Cause:	A timeout may have occurred during communications between the One-Click Provisioning processes and the on-premises machine.
Resolution:	Restart the deployment of One-Click Provisioning.

Enterprise Server Provisioning Fails - Health Check Fails

Symptom:	PORTTEST runs remotely, but fails.
Cause:	The kernels are not starting up fast enough to run a PORTTEST successfully possibly because of a timing issue.
Resolution:	Rerun the deployment. It should quickly skip to the Ent Health Check and pass.

Enterprise Server Not Able to Run PORTTEST Manually

Symptom:	Not able to run PORTTEST manually on a Microsoft Windows Enterprise Server.
Cause:	The Service user for the Enterprise Server is not set to opc.
Resolution:	You must set the Windows Service user on the Enterprise Server Service User to opc using the procedure documented here:

	JD Edwards EnterpriseOne Administration Guide 4. Administering the Windows Server 4.3 Working with Network Services 4..3.2 Setting Up the Network Service https://docs.oracle.com/cd/E53430_01/EOTSW/windows_server.htm#EOTSW00222

HTML Server Intermittently Unavailable

Symptom:	The HTML Server provisioned on the WebLogic Server is intermittently going down and the users are not being able to access the EnterpriseOne HTML login page. Generally, when this issue occurs, the below error is displayed in the WebLogic Server logs or in the HTML Server logs: **java.lang.OutOfMemoryError: PermGen space**

Resolution:	To bring up the EnterpriseOne HTML Server when the above error happens, try one of the following steps:
	
	1. Restart the EnterpriseOne HTML Server instance from the Server Manager Console and then check if the EnterpriseOne HTML login page is accessible.
	2. If the JD Edwards EnterpriseOne HTML Server login page is not accessible even after restart, then reset the below JVM arguments in the HTML Server from the WebLogic Server console and then restart the HTML Server.
	o Log in to the WebLogic Server console.
	o Go to Servers on the Environment tab and then select the HTML Server.
	o Go to the Server Start tab and click the Lock & Edit button in the left upper corner.
	o In the Arguments section, change the values for the following arguments from their existing value to 1024m:
	`-XX:PermSize=1024m`
	`-XX:MaxPermSize=1024m`
	o In the Arguments section, go to the end and enter one line space and paste the below arguments:
	`-XX:+CMSClassUnloadingEnabled`
	`-XX:+CMSPermGenSweepingEnabled`
	`-XX:+UseConcMarkSweepGC`
	o Click the Save button.
	o Click the Activate Changes button in the left upper corner.
	o Restart the EnterpriseOne HTML Server.
	3. If the JD Edwards EnterpriseOne HTML Server login page is still not accessible then, free up some resources (OCPU and memory) from the cloud domain and restart the EnterpriseOne HTML Server from the Server Manager Console.

Server Manager Console Fails to View Log File and Download Log for Enterprise Server and HTML Server

Symptom:	Server Manager Console fails to view the log file and download the log for Enterprise Server and HTML Server.
Resolution:	You should always use HTTP to access the Server Manager Console for normal operations. Although the Server Manager Console is also enabled for the HTTPS or SSL protocol, such access is restricted for internal use as part of the REST/API functionality, and should not be used for normal operations.

PDB on Compute Not Open

The Console checks to ensure the Pluggable Database (PDB) on premises is open (set to READ WRITE) as you begin to provision it. If the PDB is not open, the Console scripts will issue commands to open it. However, if the PDB is still closed (not set to READ WRITE) when the deployment commences, the deployment will fail. Use the following procedure to determine if the PDB is open, and if not how to set it to open.

1. Connect to the database using this command:

   ```
   sqlplus '/as sysdba';
   ```
2. Verify the pluggable database JDEORCL is open using this command:

   ```
   select OPEN_MODE from v$pdbs where NAME = 'JDEORCL';
   ```
3. If the OPEN_MODE is set to READ WRITE, then the PDB is ready to be provisioned by the JD Edwards EnterpriseOne One-Click Provisioning Server.
4. If the OPEN_MODE is not READ WRITE, then the PDB is not open. Open the PDB using this command:

   ```
   alter pluggable database JDEORCL open;
   ```

Not Able to View and Download Server Manager Home Logs When Server Manager is SSL-Enabled

When the Server Manager is SSL-enabled, the users may not be able to view and download the Server Manager Home logs. The root cause may be because the proper security certificates are not available. For instructions on how to create and import security certificates, refer to these documents:

- JD Edwards EnterpriseOne Tools Server Manager Guide
- JD Edwards EnterpriseOne Tools Security Administration Guide

JD Edwards EnterpriseOne HTML Server Login Fails

If the JD Edwards EnterpriseOne HTML Server login fails, run PORTTEST on the JD Edwards EnterpriseOne Enterprise Server. If PORTTEST fails, check the host entries in the /etc/hosts file. See Edit the `/etc/hosts` File for Connectivity in this Learning Path.

JD Edwards Enterprise Server - PORTTEST Fails

If PORTTEST fails on the JD Edwards EnterpriseOne Enterprise Server, check the host entries in the `/etc/hosts` file. See Edit the /etc/hosts File for Connectivity section in this Learning Path.

Resolving Host Name Issues During Provisioning

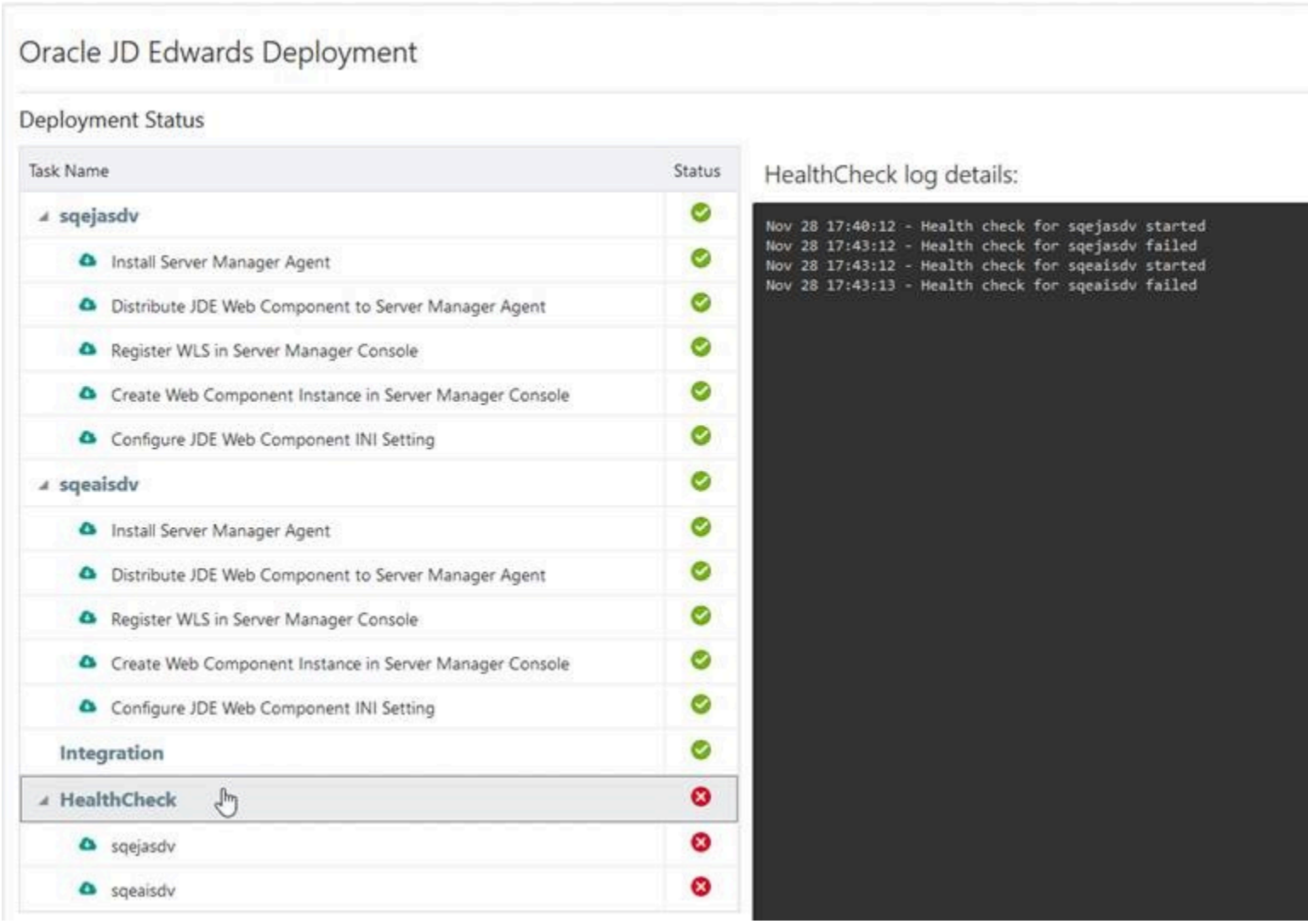
If you encounter host name issues during an orchestration because the provisioning was run against machines with the long host names, FQDNs, or both, then use the following procedure to resolve the issue:

1. On the operating system level, change the host names of all the servers in the on-premises architecture to a short host name without the FQDN.
2. On the database level, change all the host names in the JDE tables to short host names without the FQDN.
3. Ping all the machines with short host names and verify that the ping test is successful.

See Understanding Machine Names for more information.

Health Checks Fails During Final Step in One-Click Provisioning

If predefined ports for the Enterprise Server are either not enabled or not properly defined in the VCN, health checks can fail during the final step in One-Click Provisioning (as shown in the example below). For details on enabling this setting, For details on the required settings, refer to: Enterprise Server Predefined Ports.



Security Server JdeSocket Or SocketException Errors When Logging In To EnterpriseOne

If a JD Edwards EnterpriseOne Server is deployed inside a firewall-protected network, you must enable predefined ports so that all NET server ports are allocated within the predefined port range. For details on enabling this setting, refer to the section of this document entitled: Enterprise Server Predefined Ports.

Error ORA-00904: "NRUSER1": Invalid Identifier for Table F980051

The JAS log files display the following error after you install EnterpriseOne using the JD Edwards One-Click Provisioning Console with Tools 9.2.2.4:

```
[SEVERE] - [JDBJ] SQLException occured in the SQLPhysicalConnection.select():Auto: | Table or View Name
= F980051 - Data Source[0] = System - 920 java.sql.SQLSyntaxErrorException: ORA-00904: "NRUSER1": invalid
identifier

[SEVERE] - [BASE] com.jdedwards.database.base.JDBException: [SQL_EXCEPTION_OCCURRED] An SQL exception occurred:
ORA-00904: "NRUSER1": invalid identifier . java.sql.SQLSyntaxErrorException: ORA-00904: "NRUSER1": invalid
identifier

[SEVERE] - [BASE] com.jdedwards.database.base.JDBException: [SQL_EXCEPTION_OCCURRED] An SQL exception occurred:
ORA-00904: "NRUSER1": invalid identifier . com.jdedwards.database.base.JDBException: [SQL_EXCEPTION_OCCURRED] An
SQL exception occurred: ORA-00904: "NRUSER1": invalid identifier
```

Cause:

The delivered image for One-Click Provisioning has incorrect OCM mappings for the F980051 table. The OCM for this table is pointing to the System - 920 database data source where the structure of the table is not consistent with the table specs.

Solution:

1. Check both the System and the Server Map data source OCM mappings and change the OCM mappings as shown in the following list:
    - F980051 (Bell Status) mapped to Control Tables - <Environment>
    - F980052 (Notification Execution History) mapped to Control Tables - <Environment>
    - F980053 (Subscription Metadata) mapped to Control Tables - <Environment>
    - F980054 (Notification Queue) mapped to System - 920
    - F980055 (Notifications Constants) mapped to System - 920
    - F980056 (Notifications Offline Repository) mapped to System - 920
    - F980057 (Notifications Offline Repository Archive) mapped to System – 920
2. Restart the Enterprise service.

For more information, see My Oracle Support Doc ID 2408472.1.

Orchestrating JD Edwards EnterpriseOne Servers Return IPV6 Is Not Disabled

Use this procedure if One-Click Provisioning returns this message for any Linux server that you are provisioning:

- IPV6 Is Not Disabled
  a. Ensure that the /etc/sysctl.conf file contains the below list of entries:

     ```
     net.ipv6.conf.default.disable_ipv6 = 1

     net.ipv6.conf.all.disable_ipv6 = 1
     ```

  b. If the above settings do not exist, you must update the `/etc/sysctl.conf` file to include the above settings.

     > **Note:** A mandatory reboot is necessary for the settings to take effect.

  c. Verify the output of the below command to ensure there is no entry for the string "`inet6`"

     ```
     sudo ifconfig | grep inet6
     ```

     If the string "`inet6`" continues to be in the output of the above command output, verify your settings.

Regenerating and Reinstalling Self-Signed Certificates for One-Click Provisioning

This section shows you how to regenerate and reinstall Self-Signed Certificates for One-Click Provisioning.

The deployment of JD Edwards EnterpriseOne One-Click Provisioning includes temporary self-signed certificates. By design, these certificates are set to expire at one-year intervals from when they were generated.

> **Note:** After self-signed certificates are expired, Oracle strongly recommends that you generate and install your own CA certificates as described in this section. These must be certificates that are verified by a verified CA authority such as Entrust and Symantec Corporation.

Prerequisite

You must have an installation of Java Keystore.

Generating Self-Signed Certificates on Linux

Use this procedure to generate self-signed certificates on Linux.

1. Log into Provisioning Server.

2. Run the following commands (where each bulleted item is one contiguous line):
    - `sudo -i`
    - `mv /u01/jde920/.vm_unconfigured /u01/jde920/vm_unconfigured`
    - `/u01/jdk1.8.0/jre/bin/keytool -delete -alias cert -keystore "/u01/jdk1.8.0/jre/lib/security/cacerts" -storepass *****`
    - `/u01/CertGen/ConfigureCertKey_CC.sh`
    - `/u01/CertGen/ConfigureCertKey_SMC.sh <WebLogic Admin Password>`
    - `mv /u01/jde920/vm_unconfigured /u01/jde920/.vm_unconfigured`

> **Note:**
> - The `storepass` value ***** in above commands is the WebLogic Admin password.
> - The `generated cert.pem` file is located in: `/u01/E1CloudConsole/keys`
> - The log file path is: `/var/log`

Importing the Self-Signed Certificate into Target Machines on Linux

The self-signed certificate file that you generated in the previous steps must be imported into these target machines that were deployed by JD Edwards EnterpriseOne One-Click Provisioning:

- HTML Server
- Enterprise Server
- Oracle Database Server

HTML Server

Use this procedure to import the self-signed certificate into the HTML Server.

1. Run this command:

    ```
    sudo -i
    ```

2. Get the `cert.pem` file from Provisioning Server, which you generated in the previous procedure in this section entitled: "Generating Self-Signed Certificates on Linux".
3. Use this command is determine if a certificate with an alias of **smcert** is already imported to `jdk/jre/lib/security/cacerts`, where this command is a single contiguous line:

    ```
    /u01/jde_home/SCFHA/jdk/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
    ```

    If the results of the above command indicate that an alias of **smcert** certificate is already imported to the JDK/JRE lib location, use this command to remove it, where this command is a single contiguous line:

    ```
    /u01/jde_home/SCFHA/jdk/jre/bin/keytool -delete -file cert.pem -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
    ```

> **Note:** The storepass value ***** in above commands is the default password for Java trustStore.

4. Use these commands to import the certificate that you generated in the previous procedure of this section entitled: "Generate Self-Signed Certificates" to `/u01/jde_home/SCFHA/jdk`, where each command is a single contiguous line:

   ```
   /u01/jde_home/SCFHA/jdk/jre/bin/keytool -import -file cert.pem -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****

   /u01/jde_home/SCFHA/jdk/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the default password for Java trustStore.

5. Use this command is determine if a certificate with an alias of **smcert** is already imported for the JDK path:

   ```
   /u01/oracleJDE/jdk_path/jre/bin/keytool -list -v -alias smcert -keystore "/u01/oracleJDE/jdk_path/jre/lib/security/cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of **smcert** certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   /u01/oracleJDE/jdk_path/jre/bin/keytool -delete -alias smcert -keystore "/u01/oracleJDE/jdk_path/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the WebLogic Admin password.

6. Use these commands to import the certificate that you generated in the previous procedure of this document entitled: "Generate Self-Signed Certificates" to /u01/oracleJDE/jdk_path, where each command is a single contiguous line:

   ```
   /u01/oracleJDE/jdk_path/jre/bin/keytool -import -file cert.pem -alias smcert -keystore "/u01/oracleJDE/jdk_path/jre/lib/security/cacerts" -storepass *****

   /u01/oracleJDE/jdk_path/jre/bin/keytool -list -v -alias smcert -keystore "/u01/oracleJDE/jdk_path/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the WebLogic Admin password.

Enterprise Server

Use this procedure to import the self-signed certificate into the HTML Server.

1. Run this command:

   ```
   sudo -i
   ```

2. Get the `cert.pem` file from Provisioning Server, which you generated in the previous procedure in this section entitled: "Generating Self-Signed Certificates on Linux".

3. Use this command is determine if a certificate with an alias of **smcert** is already imported to `jdk/jre/lib/security/cacerts`, where this command is a single contiguous line:

   ```
   /u01/jde920/jde_home/SCFHA/jdk/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jde920/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of **smcert** certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   /u01/jde920/jde_home/SCFHA/jdk/jre/bin/keytool -delete -alias smcert -keystore "/u01/jde920/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the default password for Java trustStore.

4. Use these commands to import the certificate that you generated in the previous procedure of this section entitled: ***Generate Self-Signed Certificates*** to `/u01/jde920/jde_home/SCFHA/jdk`, where each command is a single contiguous line:

   ```
   /u01/jde920/jde_home/SCFHA/jdk/jre/bin/keytool -import -file cert.pem -alias smcert -keystore "/u01/jde920/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****

   /u01/jde920/jde_home/SCFHA/jdk/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jde920/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the default password for Java trustStore.

5. Use this command is determine if a certificate with an alias of **smcert** is already imported for the JDK path:

   ```
   /u01/jdk8_32/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jdk8_32/jre/lib/security/cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of smcert certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   /u01/jdk8_32/jre/bin/keytool -delete -alias smcert -keystore "/u01/jdk8_32/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the Site Key password.

6. Use these commands to import the certificate that you generated in the previous procedure of this section entitled: "Generate Self-Signed Certificates" to `/u01/jdk8_32`, where each command is a single contiguous line:

   ```
   /u01/jdk8_32/jre/bin/keytool -import -file cert.pem -alias smcert -keystore "/u01/jdk8_32/jre/lib/security/cacerts" -storepass *****

   /u01/jdk8_32/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jdk8_32/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the Site Key password.

Database Server

Use this procedure to import the self-signed certificate into the Oracle Database Server. Note that is only applicable if you are using Oracle Compute service for your Database Server; it not applicable if you are using the Oracle Database Service (DBS).

1. Log into the Oracle Compute Database Server.
2. Get the cert.pem file from Provisioning Server, which you generated in the previous procedure in this section entitled: "Generating Self-Signed Certificates on Linux".
3. Run this command:

   ```
   sudo -i
   ```
4. Use this command is determine if a certificate with an alias of **smcert** is already imported to jdk/jre/lib/security/cacerts, where this command is a single contiguous line:

   ```
   /u01/jde_home/SCFHA/jdk/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of **smcert** certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   /u01/jde_home/SCFHA/jdk/jre/bin/keytool -delete -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the default password for Java trustStore.
5. Use these commands to import the certificate that you generated in the previous procedure of this document entitled: "Generate Self-Signed Certificates" to /u01/jde_home/SCFHA/jdk, where each command is a single contiguous line:

   ```
   /u01/jde_home/SCFHA/jdk/jre/bin/keytool -import -file cert.pem -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****

   /u01/jde_home/SCFHA/jdk/jre/bin/keytool -list -v -alias smcert -keystore "/u01/jde_home/SCFHA/jdk/jre/lib/security/cacerts" -storepass *****
   ```

   Note: The storepass value ***** in above commands is the default password for Java trustStore.

Generating Self-Signed Certificates on Microsoft Windows

Use this procedure to generate self-signed certificates on Microsoft Windows.

1. Log into Provisioning Server.
2. Open Windows Powershell **As Administrator**.

3. Run the following commands, where each command is a single contiguous line:

```
ren <drive>\JDE\PP\jde920\.vm_unconfigured <drive>\JDE\PP\jde920\vm_unconfigured

<drive>\JDE\jdk1.8_64\jre\bin\keytool -delete -alias cert -keystore "<drive>\JDE\jdk1.8_64\jre\lib
\security\cacerts" -storepass *****
```

> **Note:** The storepass value ***** in above command is the WebLogic Admin password.

```
$env:OPENSSL_CONF += "C:\JDE\bin\openssl.cnf"

<drive>\JDE\PP\CertGen\ConfigureCertKey_CC.ps1

<drive>\JDE\PP\CertGen\ConfigureCertKey_SMC.ps1 <WebLogic Admin Password>

ren <drive>\JDE\PP\jde920\vm_unconfigured <drive>\JDE\PP\jde920\.vm_unconfigured
```

Importing the Self-Signed Certificate into Target Machines on Microsoft Windows

The self-signed certificate file that you generated in the previous steps must be imported into these target machines that were delivered by JD Edwards EnterpriseOne One-Click Provisioning:

- All Servers
- HTML Server
- Enterprise Server

All Servers

Use this procedure to import the self-signed certificate into all Microsoft Windows servers.

1. Log into the each Microsoft Windows server.
2. Get the `cert.pem` file that is located on the Provisioning Server. You generated this key using the previous procedure in this section entitled: "Generating Self-Signed Certificates on Microsoft Windows".

   On the Provisioning Server, this file is located at this location:

   ```
   <drive>\JDE\PP\E1CloudConsole\keys
   ```
3. On each machine, use this command is determine if a certificate with an alias of **smcert** is already imported to `<drive>\JDE\jde_home\SCFHA\jdk`, where this command is a single contiguous line:

   ```
   <drive>\JDE\jde_home\SCFHA\jdk\jre\bin\keytool -list -v -alias smcert -keystore

   "<drive>\JDE\jde_home\SCFHA\jdk\jre\lib\security\cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of **smcert** certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   <drive>\JDE\jde_home\SCFHA\jdk\jre\bin\keytool -delete -alias smcert -keystore "<drive>\JDE\jde_home
   \SCFHA\jdk\jre\lib\security\cacerts" -storepass *****
   ```

   > **Note:** The storepass value ***** in above commands is the default password for Java trustStore.

4. On each machine, use these commands to import the certificate that you generated in the previous procedure of this section entitled: "Generate Self-Signed Certificates" to `<drive>\JDE\jde_home\SCFHA\jdk`, where each command is a single contiguous line:

```
<drive>\JDE\jde_home\SCFHA\jdk\jre\bin\keytool -import -file cert.pem -alias smcert -keystore "

<drive>\JDE\jde_home\SCFHA\jdk\jre\lib\security\cacerts" -storepass *****

<drive>\JDE\jde_home\SCFHA\jdk\jre\bin\keytool -list -v -alias smcert -keystore

"<drive>\JDE\jde_home\SCFHA\jdk\jre\lib\security\cacerts" -storepass *****
```

> **Note:** The storepass value ***** in above commands is the default password for Java trustStore.

HTML Server

Use this procedure to import the self-signed certificate into the HTML Server.

1. Log into the HTML server.
2. Get the `cert.pem` file that is located on the Provisioning Server. You generated this key using the previous procedure in this section entitled: "Generating Self-Signed Certificates on Microsoft Windows".

   On the Provisioning Server, this file is located at this location:

   ```
   <drive>\JDE\PP\E1CloudConsole\keys
   ```
3. Use this command is determine if a certificate with an alias of **smcert** is already imported to `C:\Program Files\Java\jdk1.8.0_201`, where this command is a single contiguous line:

   ```
   <JDK_path>\jre\bin\keytool -list -v -alias smcert -keystore "

   <JDK_path>\jre\lib\security\cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of **smcert** certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   <JDK_path>\jre\bin\keytool -delete -alias smcert -keystore "

   <JDK_path>\jre\lib\security\cacerts" -storepass *****
   ```

   > **Note:** The storepass value ***** in above commands is the WebLogic Admin password.

4. Use these commands to import the certificate that you generated in the previous procedure of this document entitled: "Generate Self-Signed Certificates" to C:\Program Files\Java\jdk1.8.0_201 , where each command is a single contiguous line:

   ```
   <JDK_path>\jre\bin\keytool -import -file cert.pem -alias smcert -keystore "<JDK_path>\jre\lib\security
   \cacerts" -storepass *****

   <JDK_path>\jre\bin\keytool -list -v -alias smcert -keystore "<JDK_path>\jre\lib\security\cacerts" -
   storepass *****
   ```

   > **Note:** The storepass value ***** in above commands is the WebLogic Admin password.

Enterprise Server

Use this procedure to import the self-signed certificate into the HTML Server.

1. Log into the Enterprise Server.
2. Get the `cert.pem` file that is located on the Provisioning Server. You generated this key using the previous procedure in this section entitled: "Generating Self-Signed Certificates on Microsoft Windows".

   On the Provisioning Server, this file is located at this location:

   ```
   <drive>\JDE\PP\E1CloudConsole\keys
   ```
3. Use this command is determine if a certificate with an alias of smcert is already imported to <drive>\JDE\jdk8_32, where this command is a single contiguous line:

   ```
   <drive>\JDE\jdk8_32\jre\bin\keytool -list -v -alias smcert -keystore "

   <drive>\JDE\jdk8_32\jre\lib\security\cacerts" -storepass *****
   ```

   If the results of the above command indicate that an alias of **smcert** certificate is already imported, use this command to remove it, where this command is a single contiguous line:

   ```
   <drive>\JDE\jdk8_32\jre\bin\keytool -delete -alias smcert -keystore

   "<drive>\JDE\jdk8_32\jre\lib\security\cacerts" -storepass *****
   ```

   > **Note:** The storepass value ***** in above commands is the Site Key password.

4. Use these commands to import the certificate that you generated in the previous procedure of this document entitled: "Generate Self-Signed Certificates" to <drive>\JDE\jdk8_32, where each command is a single contiguous line:

   ```
   <drive>\JDE\jdk8_32\jre\bin\keytool -import -file cert.pem -alias smcert -keystore"

   <drive>\JDE\jdk8_32\jre\lib\security\cacerts" -storepass *****

   <drive>\JDE\jdk8_32\jre\bin\keytool -list -v -alias smcert -keystore "

   <drive>\JDE\jdk8_32\jre\lib\security\cacerts" -storepass *****
   ```

   > **Note:** The storepass value ***** in above commands is the Site Key password.

Known Issues

This section describes issues that may be code or documentation bugs created within the Oracle BUG system.

Issue: Ruby Installation Failed In One Click: Build With Error "dtrace: failed to link script"

Resolution: Refer to MOS Document *Doc ID 2723356.1*

Certified Minimum Supported Versions of Oracle Database 19c Server and Client Versions

Refer to the MOS Document *Doc ID 3107355.1* for the minimum supported Oracle Database 19c server and client version requirements to run JD Edwards EnterpriseOne on Oracle Linux 9.

13 Performing Basic Administration

Starting and Stopping Services

This section shows you how to start or stop services.

In general you should use Server Manager to start or stop services, or to check the status of services, for all JD Edwards EnterpriseOne servers.

Prerequisite

A deployment of JD Edwards EnterpriseOne.

Starting and Stopping Services

You can use these commands to manually start, stop, or check the status of the **jde-sm** service for the Server Manager Console Server:

```
sudo su - root

service jde-sm start

service jde-sm stop

service jde-sm status
```

Configuring the Public IP Address as an Internal Hostname on Client Machine

This section shows you how to configure the public IP address as an internal hostname on client machine.

Without this step, the JD Edwards EnterpriseOne application websites can only be accessed using the Public IP Address in a browser.

Prerequisite

A deployment of JD Edwards EnterpriseOne.

Configuring the Public IP Address

As a convenience, in addition to access using a Public IP address, you can also access JD Edwards EnterpriseOne application websites using the hostname. The steps given below assume that you have not configured a public web entry point for the JD Edwards EnterpriseOne application tier. In that case you need to manually add the public IP address and internal DNS hostname of the JD Edwards EnterpriseOne application tier in the hosts file of the client machine.

Alternatively, these steps can be replaced by contacting your site's network administrator and having the address and hostname setup in DNS.

Access from a UNIX Host

Modify the `/etc/hosts` file as shown below. For example:

- public IP: **123.456.789.999**
- public hostname: **demo.company.com**
- Using the above example values, the `/etc/hosts` file must contain this line:

  123.456.789.999 demo demo.company.com

Access from a Microsoft Windows System

Modify the `C:\Windows\System32\drivers\etc\hosts` file as shown below. For example:

- public IP: **123.456.789.999**

14 Considering Optional Administrative Tasks

Understanding JD Edwards EnterpriseOne Security

This section provides an overview of the JD Edwards EnterpriseOne security.

A minimal JD Edwards EnterpriseOne security definition has been shipped with your Database Server.

Prerequisite

A deployment of JD Edwards EnterpriseOne.

JD Edwards EnterpriseOne Security

Follow the instructions in the *JD Edwards EnterpriseOne Applications Release 9.2 Installation Guide for Oracle on UNIX* (in the chapter entitled: Performing Post Installation Tasks, in the section entitled: Working With Signon Security and Table Creation Security to change the passwords within EnterpriseOne for JDE and PS920 so they match any changes you make to the passwords for the Oracle Database users.

Additionally, for table creation security you should use the Datasource Master application using the Database Privilege row exit. For further details refer to the *JD Edwards EnterpriseOne Tools Security Administration Guide Release 9.2.*

JD Edwards One-Click Provisioning provides a preconfigured environment with sample data, user-defined content, roles, and security permissions. The JDE user id you used to sign on is associated with the SYSADMIN role, which has a very broad set of permissions. As such, the JDE user will have access to a large number of applications, EnterpriseOne pages, and other content. UDO View Security has been enabled for 9.2.1.0. It may be necessary to adjust security accordingly. To modify or set up the permissions for the JDE user or other users that you add to this environment, refer to *Provisioning User and Role Profiles* in the JD Edwards EnterpriseOne Tools Security Administration Guide Release 9.2.

Configuring AIS Server Depending on How You Manage Users

This section shows you how to configure the AIS Server depending on how you manage users.

REST services on the JD Edwards EnterpriseOne AIS Server can use HTTP Basic Authentication for access. Support for HTTP Basic Authentication is enabled out of the box and is required to run the EnterpriseOne Orchestrator Client, create custom Java calls from orchestrations, and use the AIS client Java API (versions 1.2.1.x and higher).

Prerequisite

A deployment of JD Edwards EnterpriseOne.

Configuring AIS Server

When the AIS Server is deployed on Oracle WebLogic Server, the Oracle WebLogic Server may require the following additional configuration depending on how you manage users:

- If you are maintaining a user registry in Oracle WebLogic Server that matches the user registry in EnterpriseOne, with identical sets of user names and passwords in each system, you do NOT need to modify your configuration.
- If you are NOT maintaining identical sets of users in Oracle WebLogic Server and EnterpriseOne, then you need to perform the following steps to modify your Oracle WebLogic Server configuration. This ensures that Oracle WebLogic Server will not intercept HTTP Basic Authentication credentials passed from the REST service.

1. In the WebLogic Server domain for your AIS Server, in the Config directory, find the `config.xml` file.
2. Add this configuration as the last line within the `<security-configuration>` element, just before the `</security-configuration>` tag:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   ```
3. Restart the AIS Server for the changes to take effect.

The following is an example of this configuration in the `<security-configuration>` element:

```
<node-manager-password-encrypted>{AES}tzAokzTHACTNNmkuutLPQEpP8bfk7Ble24vmoycooic=</node-manager-password-encrypted>

<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

</security-configuration>

<server>
```

Editing the Java.security File (Optional)

This section provides a description of an optional procedure that describes how to edit the **Java.security** file in a JDK to restore certain settings in server instances that were deployed by One-Click Provisioning.

Prerequisite

A deployment of JD Edwards EnterpriseOne.

Editing the Java.security File

The deployment of a JDK to servers using JD Edwards EnterpriseOne One-Click Provisioning removes the string **anon**, **NULL** from the property **jdk.tls.disabledAlgorithms** in this file:

```
\jre\lib\security\Java.security
```

Optionally, after the One-Click deployment is complete, you can add the string back in the JDK for each deployed server. For example, you can append the string **anon, NULL** in the Java.security file in the **jdk.tls.disabledAlgorithms** section as shown in the **bolded** string below:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, \ EC keySize < 224, 3DES-EDE-CBC, anon, NULL
```

For additional details, refer to *Java.security File* in the Server Manager Guide.

15 Upgrading your One-Click Provisioned Environment

Upgrade Learning Path

The following learning path will guide you through the upgrade process for your One-Click provisioned environment:

Upgrading JD Edwards EnterpriseOne on a One-Click Provisioned Target Environment on Linux