

JD Edwards EnterpriseOne Tools

Server Manager Installation Guide

9.2

Copyright © 2011, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	i
1 Working with the Server Manager Management Console	1
Understanding the Server Manager Management Console Installation, Upgrade, and Update	1
Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools	10
Understanding the Installation, Upgrade, and Update Strategy for JD Edwards EnterpriseOne Tools for Release 9.2	11
Update Center Components for JD Edwards EnterpriseOne Tools	12
Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools	12
Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools	16
Installing the Management Console on WebLogic Server	19
Complete the Management Console Setup Wizard	95
Upgrade the Server Manager Management Console with Oracle WebLogic Server 12.1.2	108
2 Install a Server Manager Management Agent	131
Obtain the Management Agent Installer Application	131
Distribute and Unzip the Management Agent Installer Application	133
Run the Management Agent Installer	135
Post Installation Steps for Web Server Instances on WebLogic 11g, WebLogic 12c, WebSphere 7.0, WebSphere 8.5.5.0, or WebSphere 9.0	192
Troubleshoot the Management Agent Installation	193
Deinstall a Management Agent	202
3 Uninstall the Server Manager Management Console	219
Uninstall the Server Manager Management Console	219

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.
<i>Italics</i>	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 Working with the Server Manager Management Console

Understanding the Server Manager Management Console Installation, Upgrade, and Update

You can run the Server Manager Management Console installer for new installations. For Upgrade there are two methods: one is through Update and the other method is through the Manual Upgrade process. The Update process will update the Server Manager Console from the previous tools release to the latest version through the Server Manager Console. To upgrade older OC4J based Server Manager Consoles to release 9.2, you will need to follow the manual upgrade process.

- Installation

Use this mode to install a new installation of the Management Console onto a machine on which the Server Manager Console has not previously been installed. This installation mode is described in the section of this guide entitled: *Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools*

- Update

Use the Server Manager Update feature to update an existing installation of the Server Manager Console. For instance, moving from a 9.1.x tools release to a 9.2.x tools release is considered to be an Update. The Update mode is described in the chapter of the *Server Manager Guide* entitled: *Update Server Manager*.

- Upgrade

Since OC4J is discontinued in release 9.2, please follow the documentation in the next section (*Restoring existing OC4J Server Manager Console data onto a WebLogic/WebSphere Server Manager Console*) to manually upgrade from an older release to release 9.2.

Restoring existing OC4J Server Manager Console data onto a WebLogic/WebSphere Server Manager Console

Before You Begin Restoration

Before beginning the process of restoring the existing OC4J Server Manager Console data onto a WebLogic/WebSphere Server Manager Console, consider the following:

- The OC4J based Server Manager Console should be installed at `z:\jde_home_oc4j`.
- It is assumed that the WebLogic based Server Manager Console is installed to `z:\wlssmc` on the Windows Platform and installed to `/home/oracle/jde_home_wlssmc` on Linux and Solaris platforms.
- When moving files from Windows to Linux/Solaris it is necessary to FTP the files in ASCII mode for text files (for example.xml files ...etc) and to use BINARY mode for encrypted or binary files (for example, .xsl filesetc).

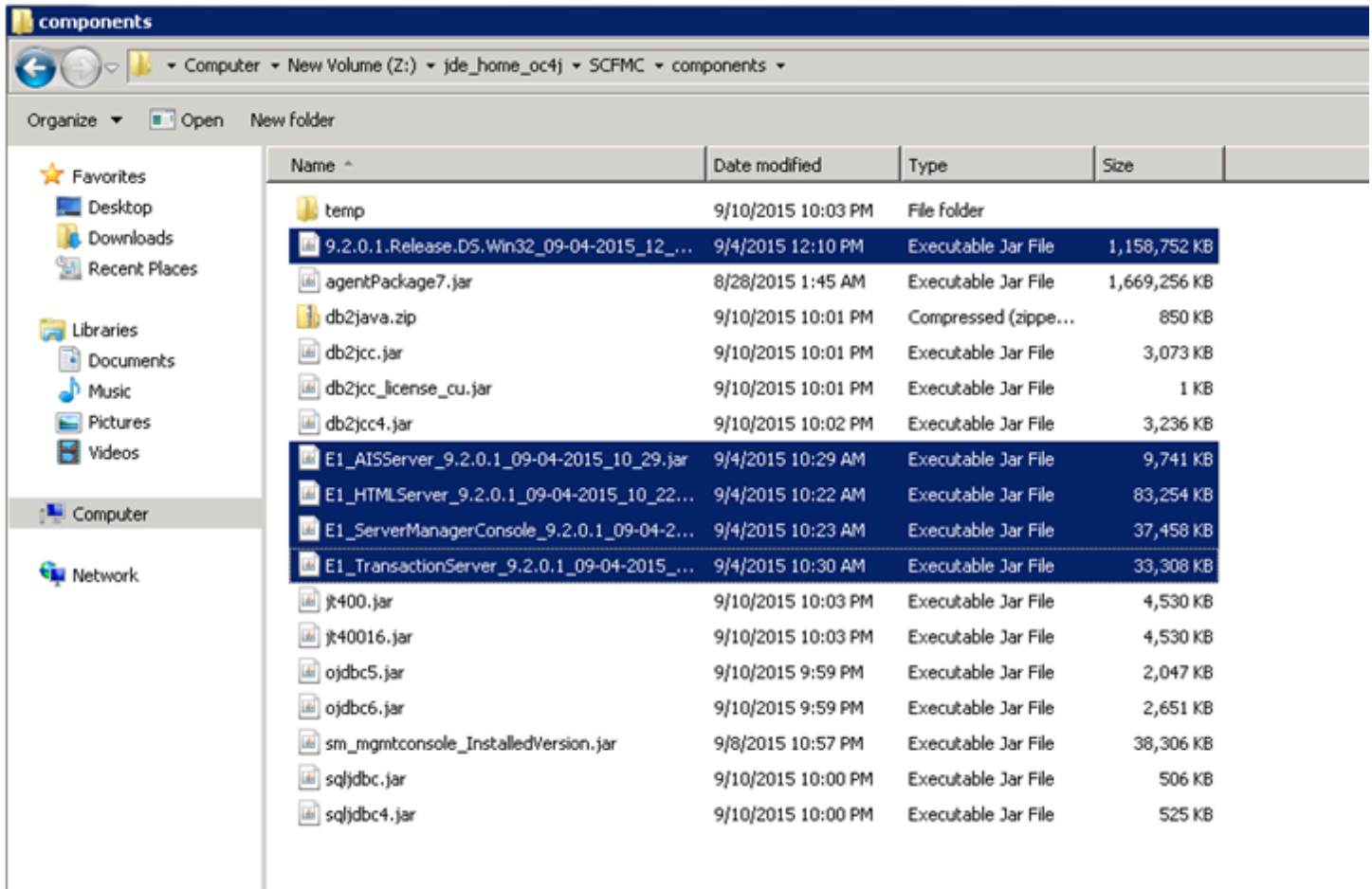
- While FTPing files from Windows to Linux/Solaris, the files should be FTPed using the same user account that was used to install the Server Manager Console and that will run the Server Manager Console (i.e oracle user).
- A WebSphere based Server Manager Console installation on the Windows Platform can be assumed to be `z:\wasmc`.
- Ensure that both the OC4J based and WebLogic/WebSphere based Server Manager Consoles are stopped before starting with the Restoration process.
- Ensure that you backup the files to a different location before overwriting the files as part of the restoration process.
- Ensure that the WebLogic/WebSphere Server Manager Console is started after the entire restoration activity is complete.

Managed Software Components

The screenshot shows the 'Managed Software Components' page in the Oracle JD Edwards EnterpriseOne Server Manager Management Console. The page has a blue header with the Oracle logo and 'JD Edwards EnterpriseOne Server Manager'. On the left is a navigation sidebar with sections for 'What do you want to do?' (INSTALL, CONFIGURE, TRACK) and 'WebSphere Admin Client Tasks'. The main content area is titled 'Managed Software Components' and includes an 'Upload Software Components' section with a file upload form and instructions. Below this is a table of managed software components.

Description	Software Type	Applicable Platform(s)	Version
Agent Installer Bundle Version 7	Management Agent Installer Bundle	windows,os400, aix, hpux, hpia64, solaris, linux	7
EnterpriseOne Server Manager Management Console Version 9.1.5.7 09-29-2015_12_56	Management Console	windows, os400, aix, hpux, hpia64, solaris, linux	9.1.5.7
EnterpriseOne RTE Server 9.2.0.1 09-04-2015_10_29	EnterpriseOne Transaction Server	windows, os400, aix, hpux, hpia64, solaris, linux	9.2.0.1
EnterpriseOne HTML Server 9.2.0.1 09-04-2015_10_22	EnterpriseOne HTML Server	windows, os400, aix, hpux, hpia64, solaris, linux	9.2.0.1
EnterpriseOne Application Interface Services Server 9.2.0.1 09-04-2015_10_29	EnterpriseOne Application Interface Services	windows, os400, aix, hpux, hpia64, solaris, linux	9.2.0.1
EnterpriseOne Server Manager Management Console Version 9.2.0.1 09-04-2015_10_22	Management Console	windows, os400, aix, hpux, hpia64, solaris, linux	9.2.0.1
EnterpriseOne Deployment Server 9.2.0.1 09-04-2015_12_05	target.type.depserver	windows	9.2.0.1

The Managed Software Components screen shows the list of managed software components in the `z:\jde_home_oc4j\components` directory.



The managed software components need to be copied over to the `z:\wlssmc\components` directory.

Database Drivers (JDBC Drivers)

ORACLE JD Edwards EnterpriseOne Server Manager Documentation and Support [Sign Out](#)

Management Dashboard

Select Instance... **JDBC Drivers**

What do you want to do?
INSTALL
 Management Agents
 Manage Software
 Database Drivers
CONFIGURE
 Server Manager Users
 Server Groups
TRACK
 User Activity
 Server Activity
 Table Cache

Use this page to manage the JDBC drivers that may be used throughout the management domain. Once uploaded a JDBC driver may be installed to the application servers.

- Oracle 10g (JDK 1.4)
- Oracle 11g (JDK 1.5)
- Oracle 11g (JDK 1.6)
- SQL Server (JDK 1.4/JDK 1.5)
- SQL Server (JDK 1.6)
- IBM DB2 UDB Type-2 (JDK 1.4/JDK 1.5)
- IBM DB2 UDB Type-4 (JDK 1.4/JDK 1.5)
- IBM DB2 UDB (JDK 1.6)
- IBM DB2 - iSeries (JDK 1.4/JDK 1.5/JDK 1.6)
- IBM DB2 - iSeries (JDK 1.6)

Oracle 9i

Oracle 10g (JDK 1.4) [Return To Top](#)

Oracle 11g (JDK 1.5) [Return To Top](#)

A JDBC driver has been successfully uploaded for this database type. It may be installed to the application servers/Data Access Servers/Data Access Drivers within the management domain.

Servers Utilizing Driver

Select [J2EE Server]:

Select All | Select None

Managed Home	Instance Name	J2EE Application Server	Status
DENP00S11.oraclejv.oraclecorp.com Z:\jde_home_11\SCFHA	WLS1035	Oracle WebLogic Instance: WLS1035, Domain: EOne, Cluster: Cluster1	Installed
DENP00S11.oraclejv.oraclecorp.com Z:\jde_home_11\SCFHA	WLS1035	Oracle WebLogic Instance: WLS1035, Domain: EOne, Cluster: Cluster1	Installed

✓ The available J2EE servers may not be listed for an application server that is not currently running.

Data Access Servers Utilizing Driver

Select [Data Access Server]:

Select All | Select None

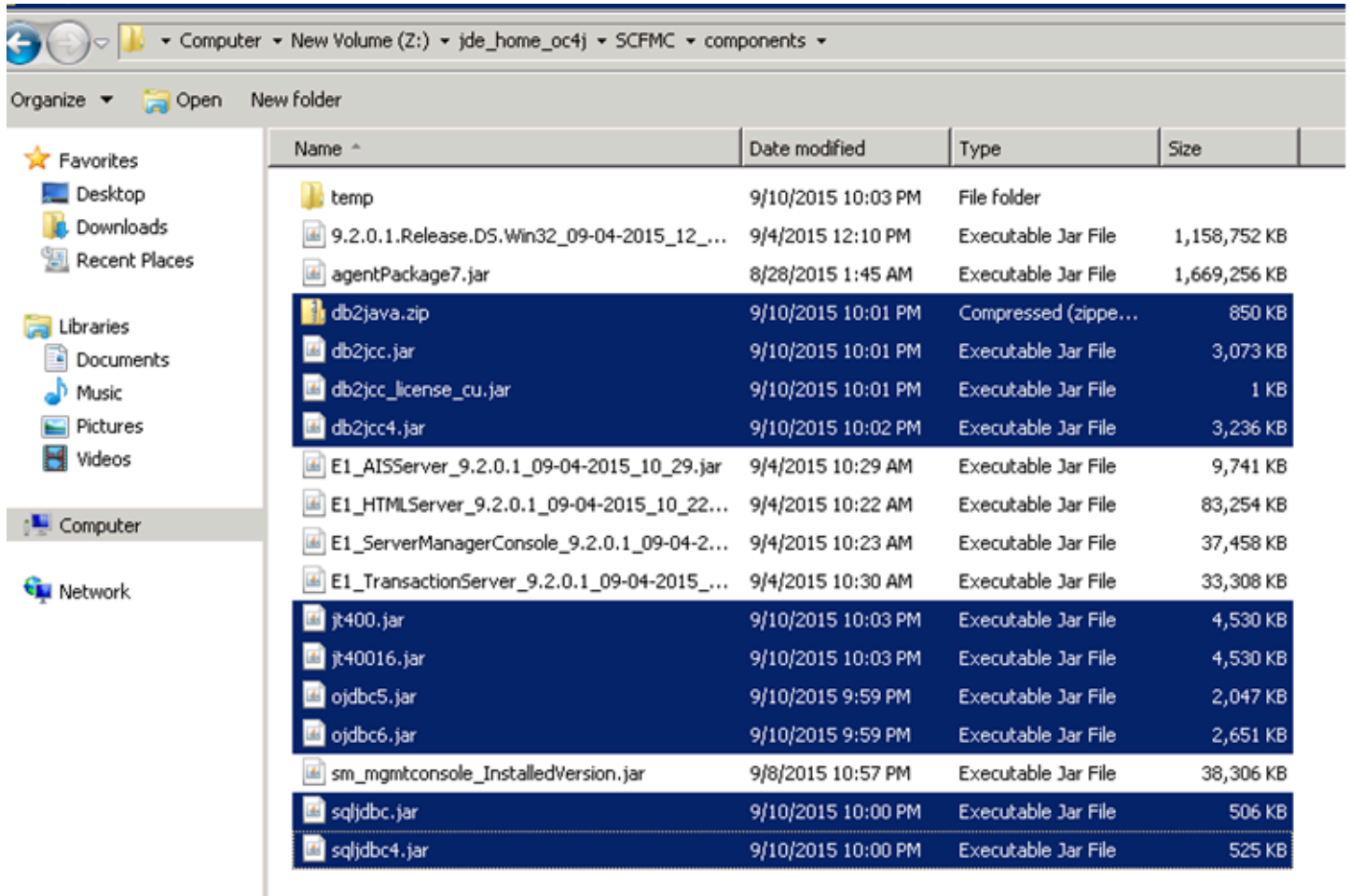
Managed Home	Instance Name	Status
--------------	---------------	--------

✓ The available EnterpriseOne Data Access servers do not require an application server and thus are listed separately.

EDne Data Access Driver Utilizing Driver

Select [Data Access Driver]:

The Database Drivers screen shows the list of managed software components in the `z:\jde_home_oc4j\components` directory.



The Database Driver files need to be copied over to the `z:\w1ssmc\components` directory.

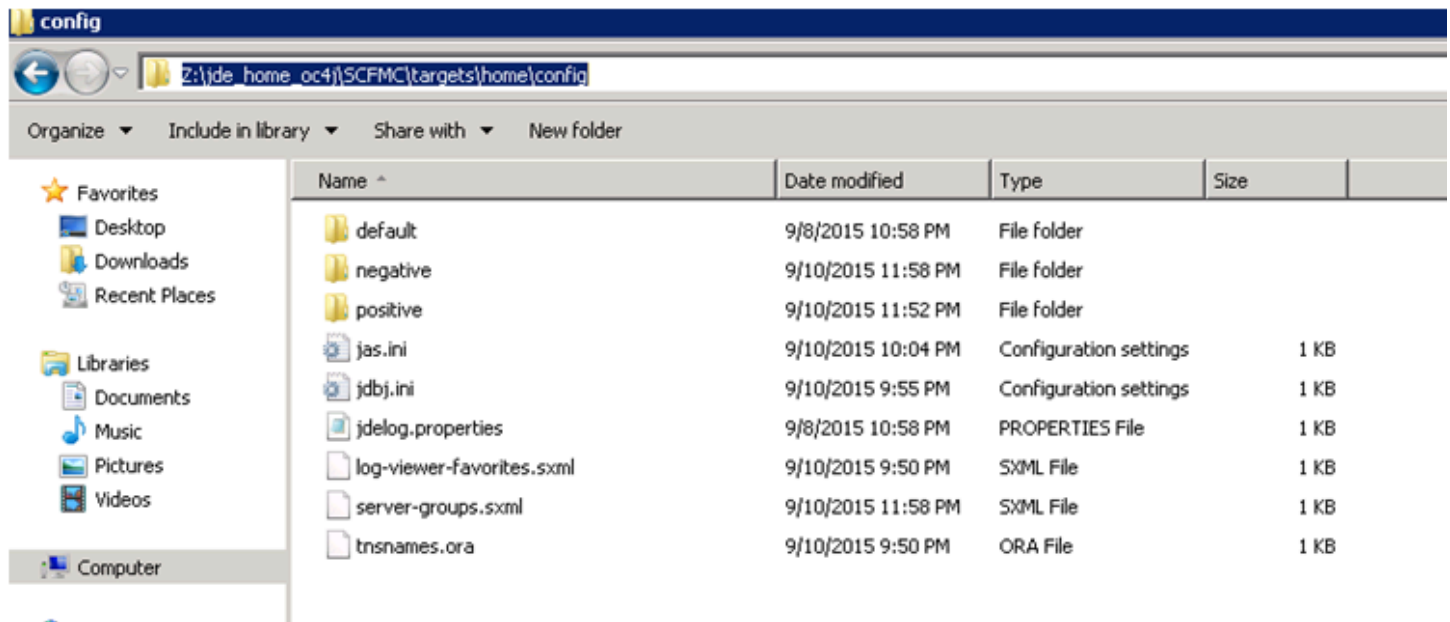
Server Manager Users

The screenshot displays the 'Server Manager Users' configuration page in the Oracle JD Edwards EnterpriseOne Server Manager console. The page is divided into several sections:

- Navigation and Header:** Includes the Oracle logo, 'JD Edwards EnterpriseOne Server Manager', and navigation links like 'Documentation and Support' and 'Sign Out'.
- Left Sidebar:** Contains navigation menus for 'What do you want to do?' (INSTALL, CONFIGURE, TRACK), 'User Management Tasks', and a password change form for the 'jde_admin' user.
- Main Content Area:**
 - Server Manager Users:** A section with tabs for 'User Groups' and 'Management Console Users'. It includes instructions and a 'Server Manager User Authentication' configuration area with fields for 'Primary Security Server' (denqz.us.oracle.com) and 'Outgoing JDENET Port' (6016).
 - User Groups:** A section with instructions to create user groups. It features a table with columns for 'User Group Name', 'User Group Description', 'Users Belonging to User Group', and 'Granted Permissions'.

User Group Name	User Group Description	Users Belonging to User Group	Granted Permissions
console_user	Any user who successfully authenticates and poses this role may utilize the management console. If a user does not have this role they will not be permitted to access any of the management console pages.	<ul style="list-style-type: none"> jde_admin SRSRSPIN SH10 	No permissions have been assigned.
console_admin	This role is equivalent to having all permissions granted to a user. The jde_admin user will always have this role assigned. This permission permits to delete the console log files.	<ul style="list-style-type: none"> jde_admin 	No permissions have been assigned.
negative_user_group	User Group for Negative Server Group	<ul style="list-style-type: none"> SRSRSPIN 	No permissions have been assigned.
positive_user_group	User Group for Positive Server Group	<ul style="list-style-type: none"> SH10 	No permissions have been assigned.

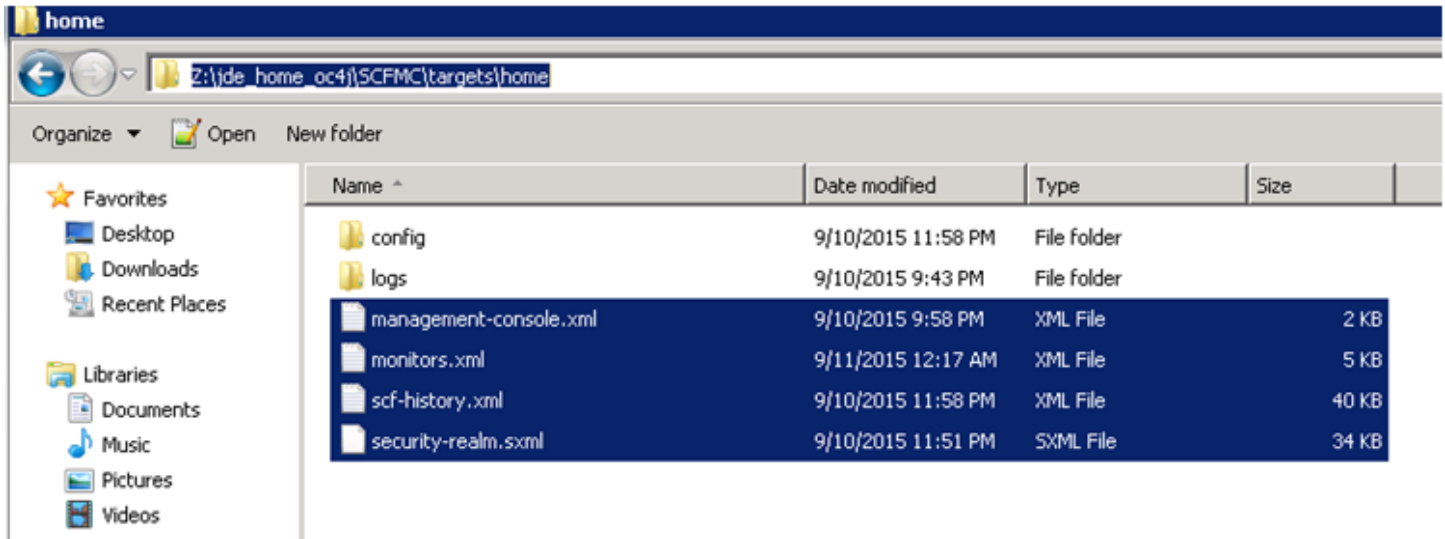
The Server Manager Users screen shows all of the information related to the Security Server configuration for the Server Manager Console, User Groups and Server Manager Console Users.



All of the information is contained in files within the `z:\jde_home_oc4j\SCFMC\targets\home\config` directory (also contained is information about Log File Viewer Favorites Configuration, which is the configuration necessary for importing EnterpriseOne Users into Server Manager Console).

The entire `z:\jde_home_oc4j\SCFMC\targets\home\config` directory contents should be copied over to the `z:\wlssmc\SCFMC\targets\home\config` directory.

The Restoration Process



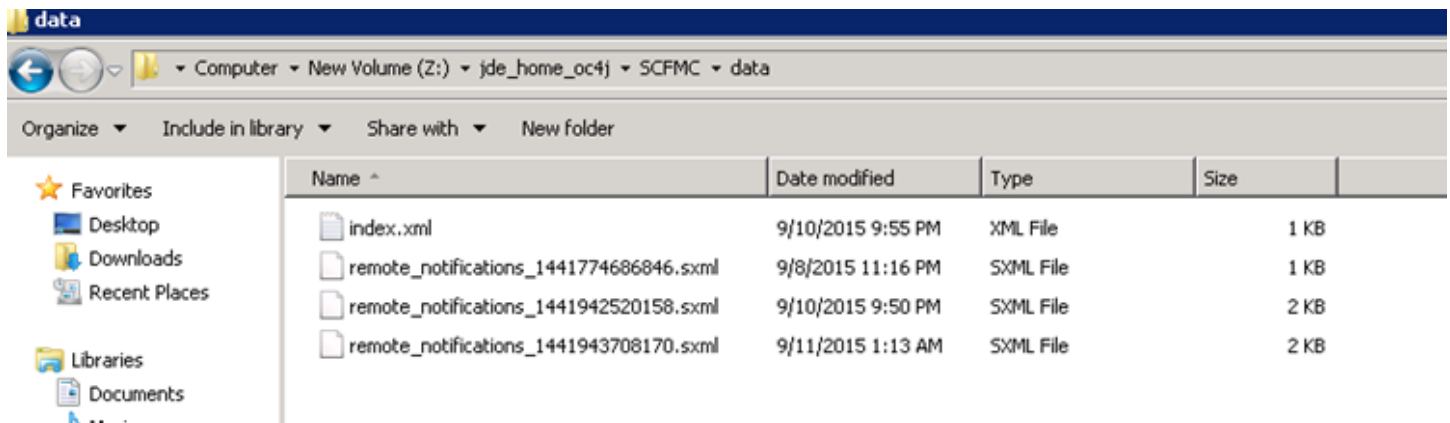
In order to restore:

- The connected Management Agents and Managed Targets information
- Monitors
- Audit History
- The jde_admin user's password

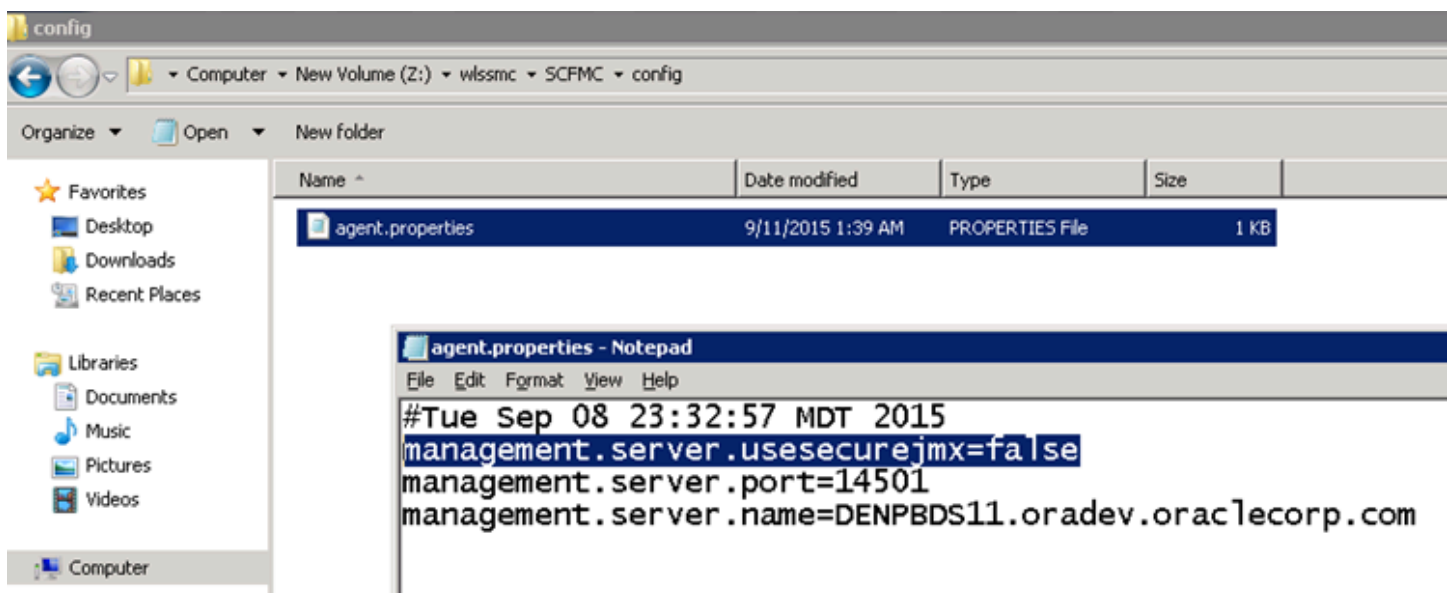
it is necessary to copy:

- management-console.xml
- monitors.xml
- scf-history.xml
- security-realm.sxml

from the `z:\jde_home_oc4j\SCFMC\targets\home` directory to the `z:\w1ssmc\SCFMC\targets\home` directory.



In order to restore the Remote Notification information, it is necessary to copy the contents of the `z:\jde_home_oc4j\SCFMC\data` directory onto `z:\w1ssmc\SCFMC\data` by overwriting the existing files.

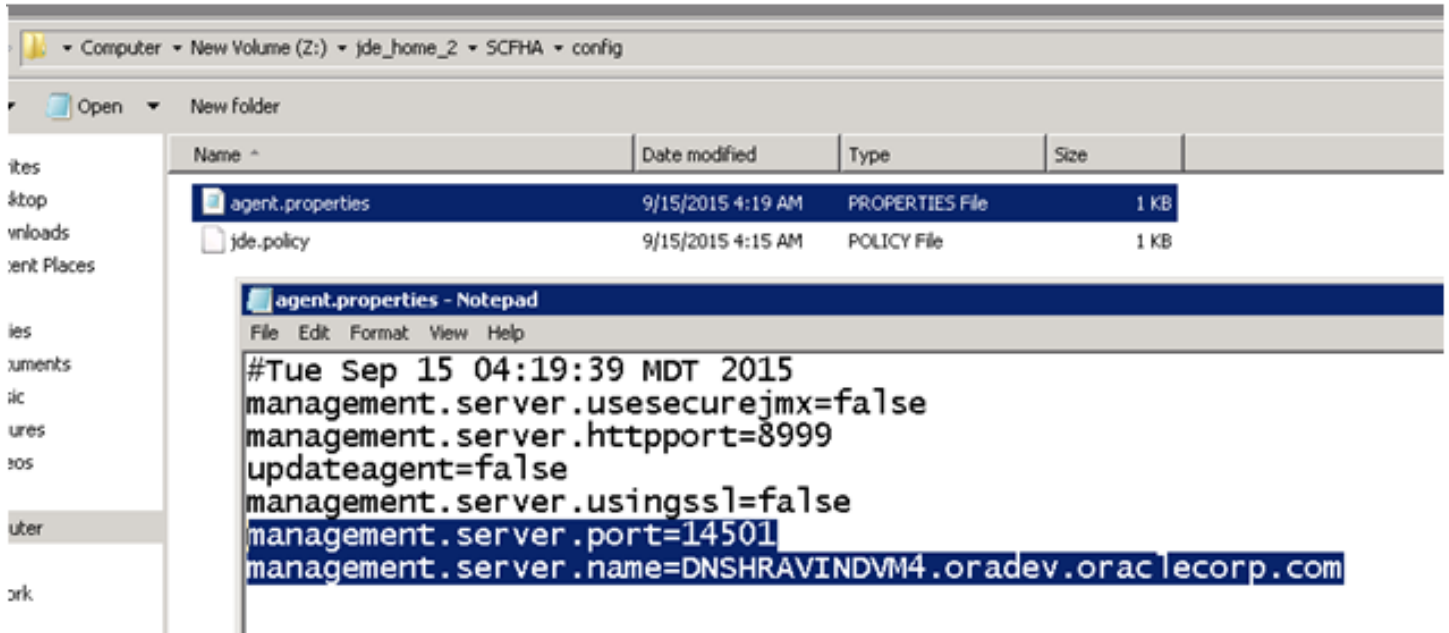


In the `z:\w1ssmc\SCFMC\config\agent.properties` file it is also necessary to ensure following line is present:

```
management.server.usesecurejmx=false
```

After the restoration activity is complete, restart (or start) the WebLogic/WebSphere based Server Manager Console.

If there is a change in the Server Manager Console hostname (that is, if the Server Manager Console is installed onto a different machine) or if there is a change in the JMX Port of the Server Manager Console (default 14501), then it is necessary to update the agent.properties file of all the connected Server Manager Agents (located at \$SCFHA\config\agent.properties file). Refer to the screenshot below:



Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools

The following table shows the matrix of supported application servers and platforms onto which the JD Edwards EnterpriseOne Server Manager Console can be installed and run on JD Edwards EnterpriseOne. Refer to Oracle Certifications for JD Edwards EnterpriseOne for details on determining the supported release levels for each product and platform.

Application Server and JDK	Platform	Notes
Oracle WebLogic Server with Oracle JDK	<ol style="list-style-type: none"> Windows Server 2012 Windows Server 2012 R2 64-bit only Oracle Linux & Red Hat Linux x86 64-bit only Oracle Solaris SPARC x86 not supported 	Requires the pre-installation of WebLogic Server. Unique installers are available per supported platform.

Application Server and JDK	Platform	Notes
	64-bit only	
IBM WebSphere Application Server IBM JDK	Windows Server 2012 Windows Server 2012 R2 64-bit only	Requires the pre-installation of the Websphere Application Server. The IBM AIX and iSeries platform are not supported.

Understanding the Installation, Upgrade, and Update Strategy for JD Edwards EnterpriseOne Tools for Release 9.2

This section describes the installation, upgrade, and update strategy for JD Edwards EnterpriseOne Tools Release 9.2 Update. The strategy shown in the following table is based on the matrix of supported application servers and platforms described in the preceding section of this guide entitled: *Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools*.

Note:

An **Upgrade** is applicable to major releases, such as upgrading from Release 8.98 to Release 9.1. An Upgrade is performed using an installer program.

An **Update** is applicable to revisions within a major release. For example: from Release 9.1.2.1 to Release 9.1.2.2. An Update is performed from within the Server Manager Console itself.

Platform	Application Server	Current Release	Upgrade Release	Update Release	Notes
Windows	OC4J	8.97 through 8.98.4x	9.1.x	n/a	Must Upgrade using the Release 9.1 Update x installer (Upgrade Mode). Future updates possible using standard Update functionality.
Windows	OC4J	9.1.x	n/a	9.2.x	Must Update using existing standard self-update functionality.
Windows Linux Solaris	WebLogic	9.1.2	9.1.x	9.2.x	For a WebLogic server, you must perform a fresh install using the Release 9.2 installer. Future Updates possible using standard Update functionality. There is no Upgrade from one platform or application server to another.

Platform	Application Server	Current Release	Upgrade Release	Update Release	Notes
Windows	WebSphere	9.1.2	9.1.x	9.2.x	<p>For a WebSphere server, you must perform a fresh install using the Release 9.2 installer.</p> <p>Future updates possible using standard Update functionality.</p> <p>There is no Upgrade from one platform or application server to another.</p>

Update Center Components for JD Edwards EnterpriseOne Tools

To verify the support of the matrix of products where the Server Manager Console can be installed and run (as described in the previous section entitled: *Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools*), the following components are available for download from the JD Edwards EnterpriseOne Update Center:

- Server Manager Console Installer 9.2 for Microsoft Windows (the same installer is used for all supported application servers)
- Server Manager Console Installer 9.2 for Linux
- Server Manager Console Installer 9.2 for Solaris
- Server Manager Console Update 9.2 (the same installer is used for all supported platforms)

Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools

To obtain the Server Manager code from Oracle web sites, you have two choices:

- **Oracle JD Edwards Update Center** (see Step 3)
 This method is the recommended method to obtain the most current version tied to a specific JD Edwards EnterpriseOne Tools Release.
- **Oracle Software Delivery** (see Step 4)
 This method is only recommended if you want to obtain the version tied to a major initial release of a major Tools Release, like 9.2.2. and 9.2.3. This site does not contain versions for any other subsequent "dot" releases such as 9.2.3.2 and 9.2.2.3.

1. Create a temporary installation directory on the machine where you want to install the Server Manager Console.
Microsoft Windows

Log on to the Microsoft Windows-based machine onto which you are installing the Server Manager Management Console as a user with Administrator rights. The recommended machine is the JD Edwards EnterpriseOne Deployment Server.

Linux or Solaris

Log on to your Linux or Solaris server.

2. Create a temporary installation directory in any preferred location. The recommend directory is:

Microsoft Windows

`C:\SM_Console`

Linux or Solaris

`/u01/SM_Console`

3. Update Center

Access the Oracle JD Edwards EnterpriseOne Update Center at this link:

<https://updatecenter.oracle.com/apps/WebSearch/updatecenter.jsp>

For **Type** criteria, use the drop-down menu to select: **EnterpriseOne Tools Releases**

For **Search** criteria, choose your JD Edwards EnterpriseOne release and click the Search button. From the displayed list, locate the corresponding Server Manager component for your release and platform.

Note: If you choose to search for only the Server Manager component, the search criteria for **Search for Name** is exactly this case-dependent string: `*Server-Manager*`

For example, the search criteria might look like this:

ORACLE MY ORACLE SUPPORT

Search

Type
EnterpriseOne Tools Releases

Release
All EOne 9.2x Releases

Platform
Linux

Search for Name
Server-Manager

BUG
*

Object
*

Description (*text*)
*

License Agreement ⓘ

→ SEARCH

4. Oracle Software Delivery Cloud

- a. Using your Customer ID credentials, sign in to the Oracle Software Delivery Cloud site at this link:

<https://edelivery.oracle.com>

- b. Use this search criteria:

JD Edwards EnterpriseOne Tools

- c. In the returned results, choose this selection

JD Edwards EnterpriseOne Core Tools and Infrastructure <tools release version>

- d. Click the item or click the **+Add to Cart** button next to the item to add it to the cart.
- e. In the upper right hand section, click the Checkout link.
- f. In the list of Selected Software, deselect all items except this one:

JD Edwards EnterpriseOne Core Tools and Infrastructure <tools release version>

- g. In the Platforms/Languages column, use the pull-down to select your platform.
- h. Click the **Continue** button.
- i. After reviewing the license agreement, click the button to accept the terms and click the **Continue** button.
- j. Deselect all items except for the Server Manager Installer for the platform you selected. For example, if you selected Linux x86-64, the selection will be in a format similar to this:

V980115-01.zip JD Edwards EnterpriseOne 9.2.3.0 Server Manager Installer Linux, 310.1 MB

Note: Do not select the Server Manager Update. This is a package intended for users changing the major level version of Server Manager. For example, from Tools Release 9.1 to 9.2.

- k. Click the **Download** button and follow the prompts to download the installer.
- l. After you finish downloading your item, use your preferred unzip program to extract the contents of the first two downloaded files to the temporary installation directory that you created in Step 2. If you followed the recommendation:

Microsoft Windows

```
C:\SM_Console
```

Note: Extract Option. When extracting, be sure to click in the check box to enable this option: **Use folder names**

Linux or Solaris

```
/u01/SM_Console
```

- m. The example below illustrates the directory structure when the .zip files are extracted into the example temporary installation directory:

Microsoft Windows

```
C:\SM_Console
-----\Disk1
-----\install
-----\stage
-----\Disk2
```

```
-----\stage
```

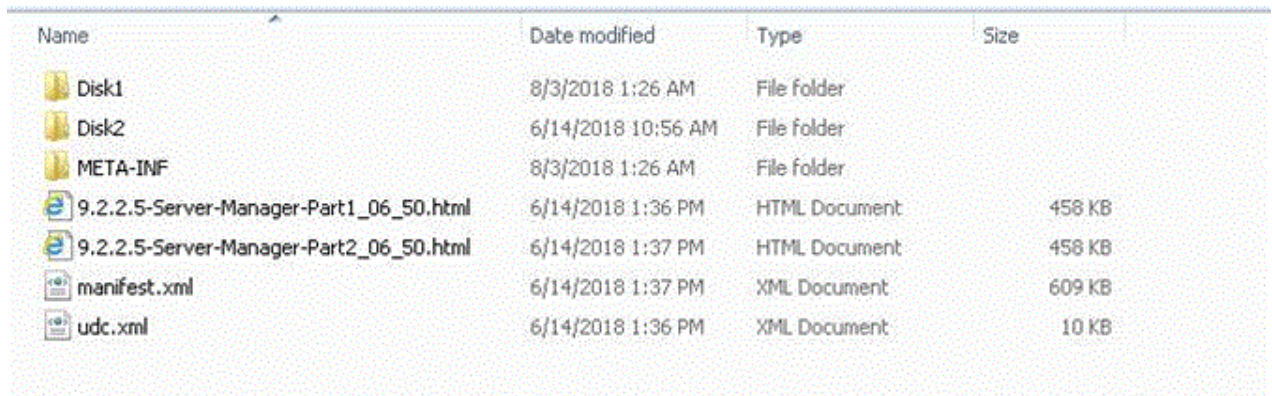
CAUTION: Ensure that the Disk1 and Disk2 directories are present directly under the SM_Console directory.

Linux or Solaris (see **Note** below)

```
/SM_Console  
-----/Disk1  
-----/install  
-----/stage  
-----/Disk2  
-----/stage
```

CAUTION: Ensure that the Disk1 and Disk2 directories are present directly under the SM_Console directory. Note that the Disk2 directory will be present in the unzipped structure even though only one image was downloaded.

The following screen shows an example of the disk structure for the extracted `.par` file for the Solaris version of the Management Console installer:



Name	Date modified	Type	Size
Disk1	8/3/2018 1:26 AM	File folder	
Disk2	6/14/2018 10:56 AM	File folder	
META-INF	8/3/2018 1:26 AM	File folder	
9.2.2.5-Server-Manager-Part1_06_50.html	6/14/2018 1:36 PM	HTML Document	458 KB
9.2.2.5-Server-Manager-Part2_06_50.html	6/14/2018 1:37 PM	HTML Document	458 KB
manifest.xml	6/14/2018 1:37 PM	XML Document	609 KB
udc.xml	6/14/2018 1:36 PM	XML Document	10 KB

Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools

This section assumes this is a new installation of the Server Manager Management Console. The standard procedure after installing the Management Console is to obtain the software components for the agents, deploy the agent installer to the target machine, and run the agent installer on the target machine. It is very important that the version of Server Manager Console uses the same corresponding versions of the agents.

This section describes these topics:

- *Implementing Security for JMX*

- *Installing the Management Console on WebLogic Server*
- *Installing the Management Console on WebSphere Application Server*
- *Troubleshoot the Management Console Installation*

Implementing Security for JMX

The Server Manager Management Console uses the Java Management Extension (JMX) protocol to communicate with deployed Server Manager agents through a socket connection. A new installation of EnterpriseOne Tools 9.2 automatically includes an additional layer of security for JMX. However, if you are upgrading Server Manager to EnterpriseOne Tools Release 9.2, you must manually implement the additional security for JMX after performing the upgrade.

Note: If you are upgrading Server Manager to EnterpriseOne Tools Release 9.2, you must also upgrade any existing agents for your managed instance to the same release as your Server Manager Console prior to enabling JMX security. Otherwise, existing agents will not be able to communicate with the Server Manager Console with JMX security enabled.

JMX Security and Server Manager Install and Configuration

JMX Security is enabled as part of the 9.2+ Server Manager installer for both console and agents on all supported platforms.

The configuration changes added by the Server Manager installer are:

Server Manager Console agent.properties:

```
management.server.useseccurejmx=true
```

Server Manager Agent agent.properties:

```
management.server.useseccurejmx=true
```

```
management.server.usingssl=<Installer code will add true if Admin confirms that Server Manager is using HTTPS in the Server Manager Agent install wizard>
```

```
management.server.httpport=<Installer code will add Server Manager HTTP(S) port number based on what Admin provides in the Server Manager Agent install wizard>
```

JMX Security and Managed EnterpriseOne Target Servers

You will have to deploy 9.2+ tools code in Server Manager managed EnterpriseOne servers (Enterprise Server, HTML Server, AIS Server, RTE Server, BSSV Server, DAD driver, Deployment Server) and restart the managed server.

For a WAS and WLS cluster you will have to deploy 9.2+ tools code in Server Manager managed EnterpriseOne web targets (HTML Server, AIS Server, RTE Server) which will configure the web.xml with a secure JMX setting and restart the managed server.

JMX Security and Server Manager Upgrade to 9.2+ Tools Release

If you are updating Server Manager to EnterpriseOne Tools Release 9.2, you must manually implement the additional security for JMX after performing the update by updating the agent.properties file for the console and all agents connected to the Server Manager Console.

To enable JMX Security for the Server Manager Console:

1. Navigate to the agent.properties file in the base folder for the Server Manager Console.

Typically, this might be named:

```
C:\jde_home_1\SCFMC\config\agent.properties
```

2. Edit the agent.properties file for the console and add the following new setting:

```
management.server.useseccurejmx=true
```

3. Restart the Server Manager Console.

To enable JMX Security for the Server Manager Agents:

1. Navigate to the agent.properties file in the base folder for the Server Manager agent.

Typically, this might be named:

```
C:\jde_home_2\SCFHA\config\agent.properties.
```

2. Edit the agent.properties file for the agent and add the following new settings:

- a. `management.server.useseccurejmx=true`

- b. `management.server.usingssl=<This should be set to true if the Server Manager console URL is using HTTPS, otherwise set it to false>`

- c. `management.server.httpport=<This should be set to the correct HTTP(S) port number for the Server Manager Console URL>`

3. Restart the Server Manager agent.

4. Repeat these steps for each Server Manager agent connected to the Server Manager Console.

After enabling JMX Security for the Server Manager Console and Agents:

1. Restart the Server Manager managed EnterpriseOne servers (Enterprise Server, HTML Server, AIS Server, RTE Server, BSSV Server, DAD driver, Deployment Server) to finalize enabling JMX Security and to publish runtime metrics.
2. For the WebSphere Application Server and the WebLogic Server cluster, you will have to deploy new EnterpriseOne managed code (HTML Server, AIS Server, RTE Server) which will configure the web.xml with secure JMX settings.
3. Restart the Managed Server to work with Server Manager with JMX Security enabled and publish runtime metrics.

JMX Security and Server Manager Upgrade to 9.2+ Tools Release and WLS Fix for ManagementLoginModule_JAR.jar

1. Update the Server Manager Console to 9.2.x Tools release from pre 9.2 Tools release.
2. STOP the AdminServer and all the Managed Server(s) within the Domain, before applying this fix.
3. GET the ManagementLoginModule_JAR.jar from below location:

```
<SM Install location>\stage\ManagementConsole_WAR.ear\ManagementConsole_WAR.war\WEB-INF\lib  
\ManagementLoginModule_JAR.jar
```

4. COPY the ManagementLoginModule_JAR.jar, copied from the above location into the locations listed below:

```
<SM Install location>\lib\ManagementLoginModule_JAR.jar
```

```
<WLS Install location>\user_projects\domains\E1Tools\lib\ManagementLoginModule_JAR.jar
```

5. DELETE the contents of the .tmp directory

```
<WLS Install location>\user_projects\domains\E1Tools\servers\SMC_Server_EOne_Console\tmp\_WL_user
```


6. START the AdminServer. The Managed Server(s) within the Domain can also be started.

JMX Security and JMX clients

The JDE Application pack (12.1.0.3) for Enterprise Manager is modified in the 9.2 tools release to support both secure JMX and non-secure JMX Server Manager for server manager discovery and to collect configuration and runtime metrics for EnterpriseOne targets from Server Manager.

The JDE Concurrent Licensing Monitor tools are modified in the 9.2 tools release to support both the secure JMX and non-secure JMX Server Manager in order to collect configuration and runtime data from the Server Manager or licensing team.

Note: There is no configuration change required to work with secure JMX Server Manager.

JMX Security and pre 9.2 Managed EnterpriseOne Target Servers

If you are using a pre 9.2 (9.1.5.x, 9.1.4.x,...) tools release for managed target servers but are using a 9.2+ Server Manager where secure JMX is enabled by default using the new 9.2+ Server Manager installer, or you have manually enabled secure JMX security after upgrading the Server Manager code to 9.2+, Runtime metrics will NOT work for pre 9.2 managed target servers.

You should be able to work with configuration, log files, start/stop servers and change code on pre 9.2 managed servers with secure JMX enabled in 9.2 + Server Manager.

Installing the Management Console on WebLogic Server

You can install the Server Manager Console on WebLogic Server on Microsoft Windows, Linux, or Solaris platforms.

See Also

Refer to these sites for additional information about configuring and using Oracle WebLogic Server:

- JD Edwards EnterpriseOne HTML Server on Oracle WebLogic Server Reference Guide for UNIX
https://docs.oracle.com/cd/E61420_01/doc.92/e55829.pdf
- Oracle WebLogic Server 10.3.5 Documentation Home
http://docs.oracle.com/cd/E21764_01/wls.htm
- Oracle Fusion Middleware Documentation (for all supported releases of Oracle WebLogic Server)
<https://docs.oracle.com/en/middleware/middleware.html>
- Node Manager Overview Documentation Home
http://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/nodemgr.html
<http://docs.oracle.com/middleware/1212/wls/NODEM/overview.htm>

This section discusses these topics:

- *Prerequisites for WebLogic Server*
- *Running the WebLogic Server Installer for the Server Manager Console*
- *Verifying the Server Manager Console Installation on WebLogic Server*
- *Enable SSL for Server Manager Console on the WebLogic Server*
- *Obtain and Install CA Certificates in Oracle WebLogic Server*
- *Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore*
- *Import the Server Manager Console Certificate into All Java Installations That Are Used by Embedded Agents*
- *Troubleshooting the Server Manager Console Installation on WebLogic Server*

Prerequisites for WebLogic Server

Ensure the following prerequisites are met prior to running the Server Manager Console installer:

- The Server Manager Console installer must be run with the same user who installed and is running WebLogic server. The user running the Server Manager Console installer should have read/write access to the directories pointed by TEMP and TMP Environment Variables. The TEMP and TMP Environment Variables must be configured to point to valid paths.

Note: Linux/Solaris Platforms. The paths pointed to by TEMP and TMP environment variables should refer to the same mount point where the WebLogic Server is installed and where the Server Manager Console is to be installed. For example, the mount point might be `/u01`. If the variable points to a different mount point the Server Manager Console installation may fail with this message: permission denied on scf.properties file.

- The machine on which the Server Manager Console will be installed must have adequate disk space to perform the installation.
- You must create a new and separate WebLogic Server Domain in which you will install the Server Manager Console.
- If there are other managed servers in the Domain in which you are attempting to install the Server Manager Console they must be in a STOPPED state at the time of installation. Only the AdminServer of the domain and the nodemanager associated with the domain should be running at the time of installation (see troubleshooting 5.6.2.4).
- The Server Manager Console cannot be installed into a WebLogic Server Domain where a JD Edwards EnterpriseOne BSSV Instance/Server is already installed. Conversely, a JD Edwards EnterpriseOne BSSV Instance/Server cannot subsequently be installed into the same WebLogic domain where you install the Server Manager Console.
- The nodemanager logical *machine name* must be known to the administrator performing the installation. This is necessary because the installer requires this value as an input. It is important to note that this value must be the logical nodemanager machine name, which is not necessarily the physical server name.
- The `nodemanager.properties` file used by the nodemanager must have this value set to true (the default value is false):

```
StartScriptEnabled=true
```

Note that you must restart the nodemanager in order for any changed values to take effect. The `nodemanager.properties` file is typically located at this location:

Microsoft Windows

WebLogic Server 11g

C:\Oracle\Middleware\wlserver_10.3\common\nodemanager\nodemanager.properties

WebLogic Server 12c

C:\Oracle\Middleware\Oracle_Home\user_projects\domains\\nodemanager\nodemanager.properties

WebLogic Server 14c

C:\Oracle\Middleware\Oracle_Home\user_projects\domains\\nodemanager\nodemanager.properties

Linux and Solaris

WebLogic Server 11g

/u01/Oracle/Middleware/Oracle_Home/wlserver_10.3/common/nodemanager/nodemanager.properties

WebLogic Server 12c

/u01/Oracle/Middleware/Oracle_Home/user_projects/domains/<domain_name>/nodemanager/
nodemanager.properties

WebLogic Server 14c

/u01/Oracle/Middleware/Oracle_Home/user_projects/domains/<domain_name>/nodemanager/
nodemanager.properties

- There must be a valid nodemanager associated with the WebLogic Domain into which the Server Manager Console will be installed as described below:

Microsoft Windows

Ensure the nodemanager is running as a Microsoft Windows service or using the `startNodeManager.cmd` program started from the command prompt.

Linux and Solaris

Ensure the nodemanager is started by using the `startNodeManager.sh` command.

- You can also stop Node Manager using `stopNodeManager.sh` (for UNIX) and `stopNodeManager.cmd` (for Windows) under:

```
<ORACLE_HOME>\user_projects\domains<domain_name>\bin\
```

Other ways to stop Node Manager are as follows:

Microsoft Windows

Stopping the Windows service or by killing the nodemanager process.

Linux and Solaris

Killing the nodemanager process using this command:

```
kill -9 <pid of nodemanager process>
```

- Verify that the nodemanager is reachable to the AdminServer using this process:

- a. Login into WebLogic Server AdminServer console.
 - b. Go to the Environment > Machines tab and select the nodemanager machine to which the Domain is registered.
 - c. Go to the Monitoring tab and verify that **Reachable** is displayed. This value indicates that a valid nodemanager is configured with the WebLogic Server Domain and that it is running.
- An AdminServer must be associated with the WebLogic Domain into which the Server Manager Console is to be installed and it must be running at the time of installation.
 - The administrator performing the installation must know the AdminServer **http/t3 port number** and the **Hostname/IP Address** on which the AdminServer is listening for http/t3 connections. You can find this value from the AdminServer logs or must be known because this value is configured when WebLogic is installed. Currently the https/t3s protocols are not supported for installing Server Manager Console software.
 - The administrator performing the installation will be prompted to input the path to the WebLogic Server directory during the install. The typical values are:

Microsoft Windows

WebLogic Server 11g

`C:\Oracle\Middleware\wlserver_10.3`

WebLogic Server 12c

`C:\Oracle\Middleware\Oracle_Home\wlserver`

WebLogic Server 14c

`C:\Oracle\Middleware\Oracle_Home\wlserver`

Linux and Solaris

WebLogic Server 11g

`/u01/Oracle/Middleware/Oracle_Home/wlserver_10.3`

WebLogic Server 12c

`/u01/Oracle/Middleware/wlserver`

WebLogic Server 14c

`/u01/Oracle/Middleware/wlserver`

- The administrator performing the installation will be prompted to input the Listen port of the AdminServer, the admin userid and password of the AdminServer.

- At the time of the Server Manager Console installation, the AdminServer cannot not be locked for editing. You can confirm this by determining if the "Lock & Edit" button is enabled in the WebLogic Admin Console.

As a double-check, you can verify that no file named `edit.lock` exists in the Domain directory. If the file exists, you should delete it. The typical location is:

Microsoft Windows

```
C:\Oracle\Middleware\user_projects\domains\E1Apps\edit.lock
```

Linux and Solaris

```
/u01/Oracle/Middleware/user_projects/domains/E1Apps/edit.lock
```

- The hosts file must have the entry for localhost (loopback).
- The hosts file should have an entry for the correct IP Address of the machine mapping to the appropriate hostname of the machine.

Microsoft Windows

```
C:\Windows\System32\drivers\etc\hosts
```

Linux and Solaris

```
/etc/hosts
```

- The hostname of the machine should not map to the IP Address 127.0.0.1, because that IP address is typically used for localhost.
- The AdminServer must not have any particular Listen Address configured and it must be left blank. A blank setting specifies that it will listen for connection on all IP addresses available on the machine.

Running the WebLogic Server Installer for the Server Manager Console

To install the Server Manager Console:

1. Log on to the machine onto which you are installing the Server Manager Management Console as a user with privileges as described in the preceding section of this guide entitled: *Prerequisites for WebLogic Server*.
2. Change to the directory in which you extracted the Server Manager Console installer as described in the previous section of this chapter entitled: *Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools*.

3. Depending on your Tools release, launch the OUI installer according to these notes:

Note:

- **For Tools Release 9.2.2.0 and Greater:** A 64-bit JDK or JRE, version 1.8 or later must be installed before starting the Server Manager Console installer.
- **For Tools Releases prior to 9.2.2.0:** A JDK is included in the installer. Therefore, a separate JDK is not required.
- **For Tools Release 9.2.3.3 and Greater:** Microsoft Visual Studio 2017 and 2013 64-bit Redistributables must be installed prior to running the Server Manager Console installer.
- **For Tools Releases prior to 9.2.3.3:** Microsoft Visual Studio 2010 32-bit Redistributables must be installed prior to running the Server Manager Console installer.

Note: One of the following requirements must be met:

- **For Tools Release 9.2.3.3 and Greater:** You must specify the location of the JDK or JRE on the command line. If the location is not specified, the installer will fail immediately.
- **For Tools Release 9.2.2.0 up to but not including 9.2.3.3:** You can specify the location of the JDK or JRE on the command line. If the location is not specified, you will be prompted for it.
- **For Tools Releases prior to 9.2.2.0:** Because a JDK is included in the installer, you will not be prompted for one.

Microsoft Windows

To specify the location of a JDK or JRE on the command line:

- a. Open a Windows Command window with **Run as administrator**.
- b. Change directory (cd) to the directory in which you unzipped the installer. For example, if you followed the recommendation in *Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools* the command would be:

```
cd C:\SM_Agent\Disk1\install
```

- c. Use this command to run `setup.exe` followed by the argument `-jreLoc` and the directory to the JDK or JRE:

```
setup.exe -jreLoc C:\PROGRA~1\Java\JRE18~1.0_1
```

Note: Regarding the above command:

- Include a space after the `-jreLoc` argument.
- The path to the JDK or JRE must be of the Windows short form, which is 8 + 3 format.
- The specified JDK or JRE directory must contain this directory and executable:

```
bin\java.exe
```

To skip specifying the location of a JDK or JRE on the command line:

Do one of the following:

- a. Follow the instructions above to run from a Windows Command window but without the `-jreLoc` argument.
- b. In Windows Explorer, right-click on `setup.exe` in the directory in which you unzipped the installer and select **Run As Administrator**. For example, if you followed the recommendation in *Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools* the file will be located in this directory:

```
C:\SM_Agent\Disk1\install\setup.exe
```

The Windows Command window starts indicating Windows is preparing to launch the Oracle Universal Installer for the Server Manager Management Console.

Linux or Solaris

To specify the location of a JDK or JRE on the command line:

- a. Execute `runInstaller` from the directory in which you unzipped the installer. For example, if you followed the recommendation in Section 3.5, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools," the file will be as below. Follow `runInstaller` with `-jreLoc` and the directory to the JDK or JRE:

```
./SM_Console/Disk1/install/runInstaller -jreLoc /u01/jre1.8.191
```

Note: Regarding the above command:

- o Include a space after the `-jreLoc` argument.
- o The specified JDK or JRE directory must contain this directory and executable:

```
bin\java
```

To skip specifying the location of a JDK or JRE on the command line:

- a. Execute `runInstaller` from the directory in which you unzipped the installer. For example, if you followed the recommendation in *Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools*, the file will be:

```
./SM_Console/Disk1/install/runInstaller
```

All Platforms

The Oracle Universal Installer (OUI) Wizard begins to initialize and prepare the JVM for the JD Edwards EnterpriseOne Management Console installer. This may take a few minutes to completely initialize. When the

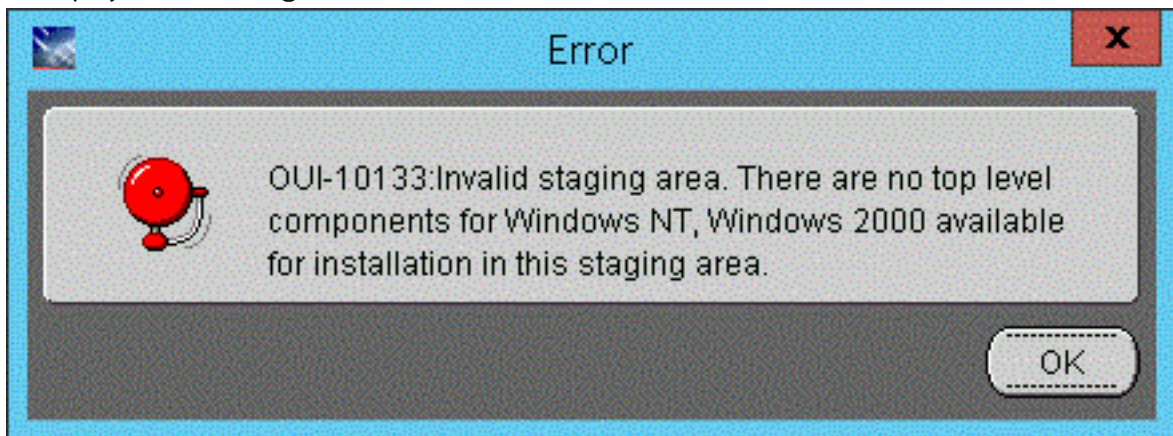
initialization is complete, a new and separate JD Edwards EnterpriseOne Management Console installer window is displayed.

Tools Release 9.2.2.0 up to but not including 9.2.3.3. If you did not specify the location of a JDK or JRE via the `-jreLoc` argument, the installer prompts you to specify the location of that at a command prompt.

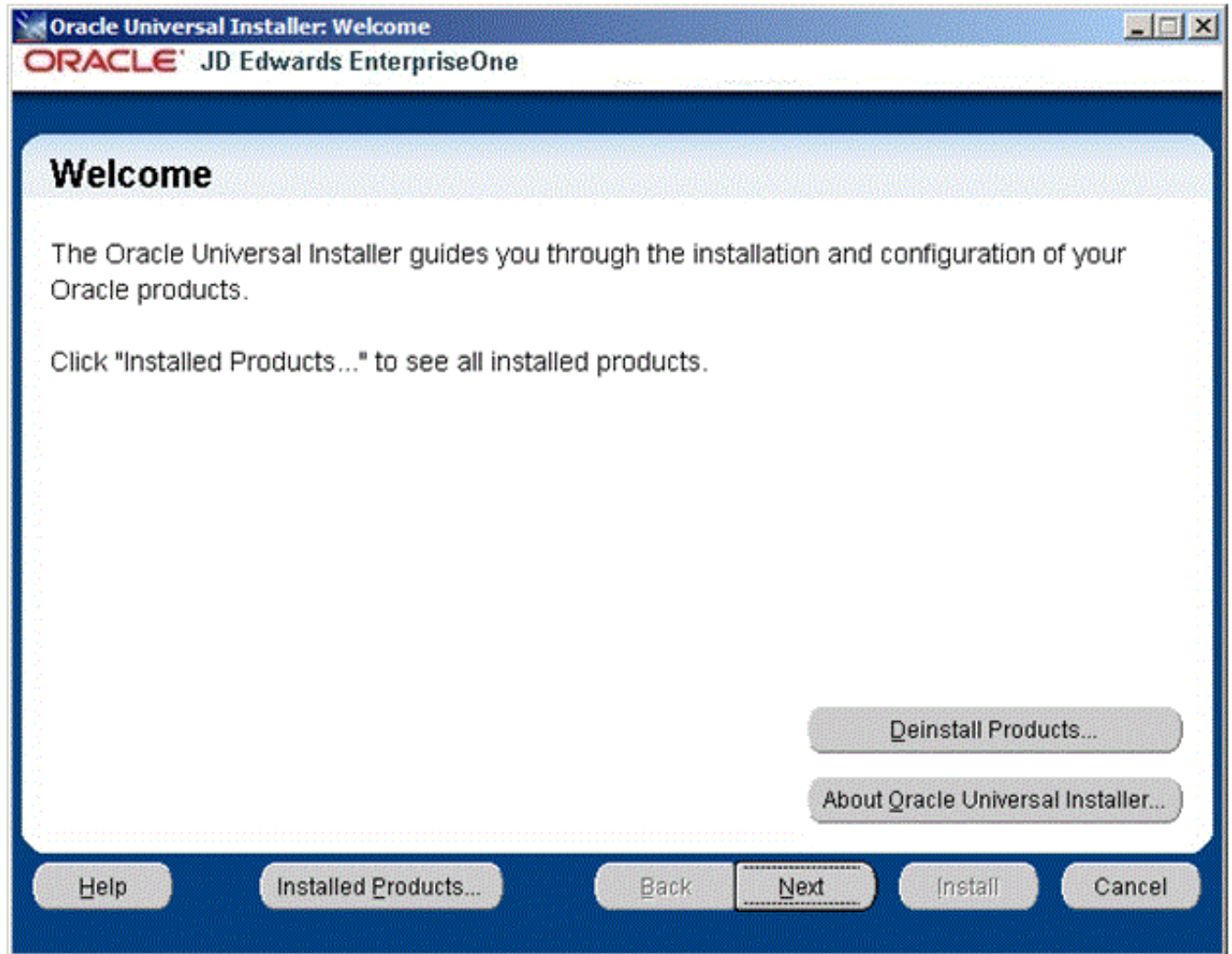
```
$ ./runInstaller
Starting Oracle Universal Installer...

Preparing to launch Oracle Universal Installer from /tmp/OraInstall2017-08-15_09-16-20AM. Please wait ...
Please specify JRE/JDK location ( Ex. /home/jre ), <location>/bin/java should exist :
```

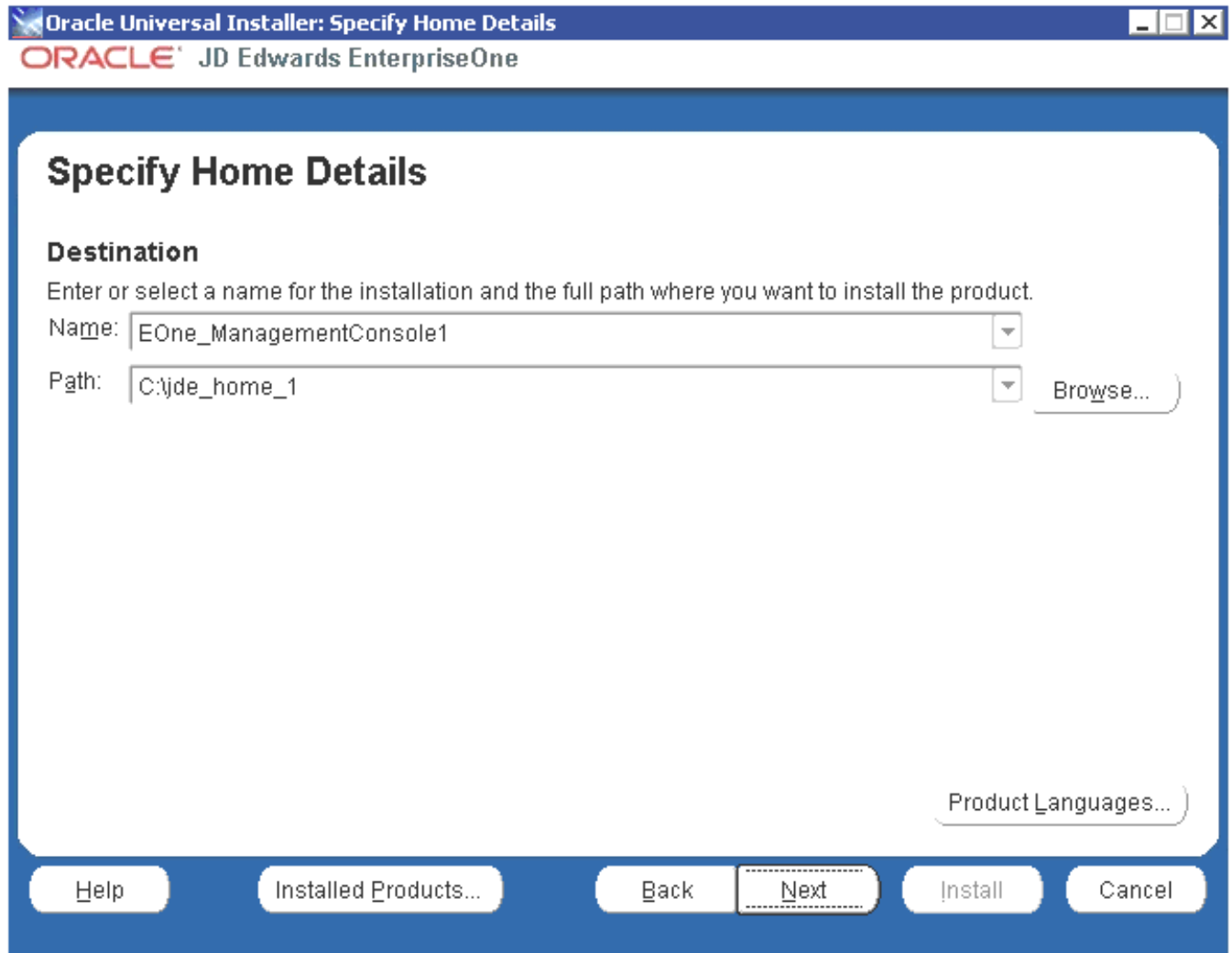
Note: For the 9.2.2.0 installer, as the installer runs, it will fail if the JDK/JRE is not at least Version 1.8. Upon failure it displays the following error:



After the installer validates existence of the JDK in the specified location, the OUI installer user interface appears. All further installer behavior remains the same as previous Tools Releases.



4. On the Welcome screen, click the **Next** button.



5. On Specify Home Details, complete these fields:

o **Name**

Enter a unique name of the Management Console. The default value is:

EOne_ManagementConsole

Note: If there is an existing installation of the Management Console with the default name, the installer will append the default name with a number to make it unique. For example, EOne_ManagementConsole1.

o **Path**

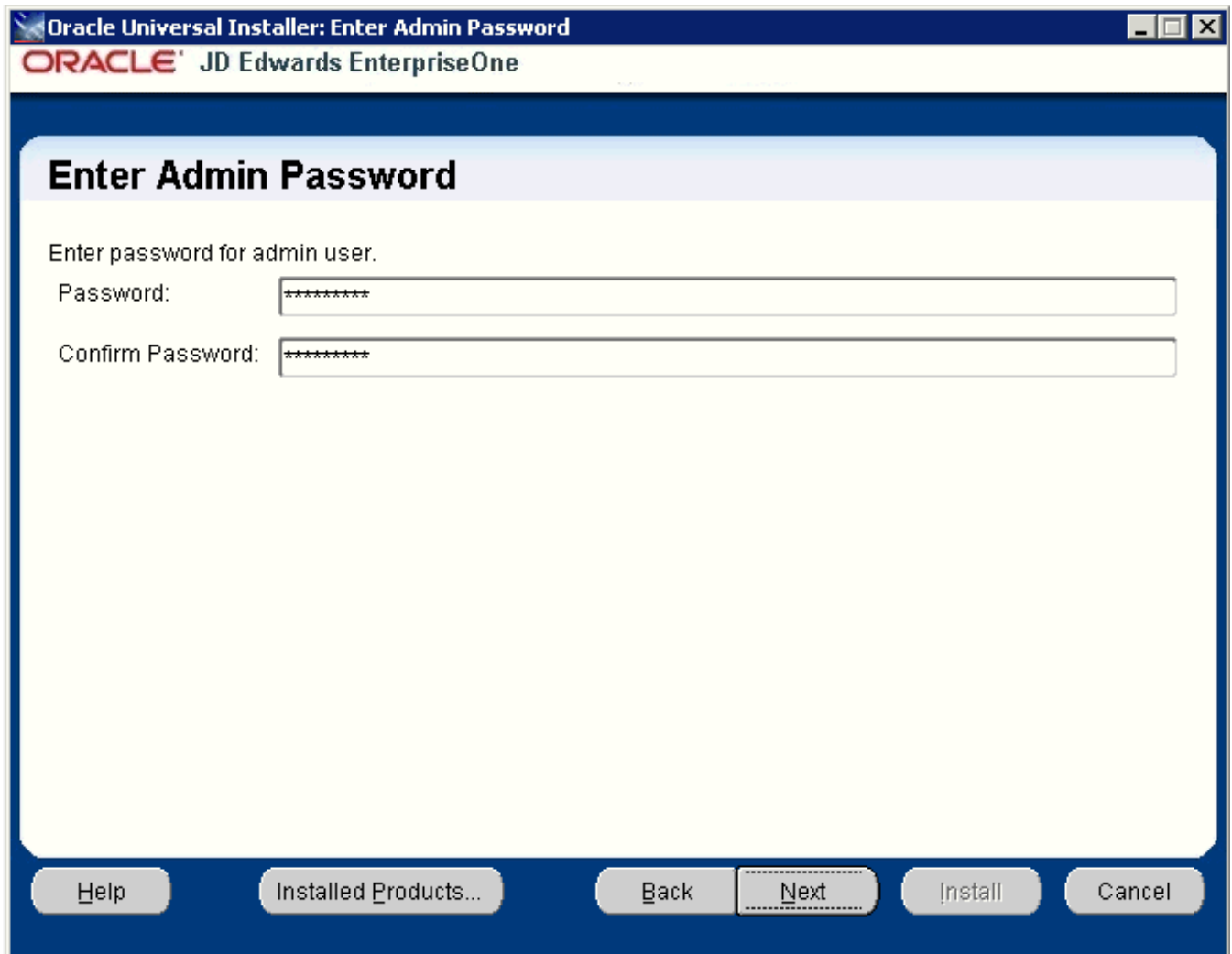
Enter the drive and directory where you want the files installed on your Management Console. The JD Edwards EnterpriseOne Management Console installer automatically detects the root drive location on the machine and by default appends this value:

jde_home

Note: Although jde_home is the default and recommended setting, you can specify any value to replace the default value. If there is an existing installation of the Management Console the default name will be appended with an underscore and a number. For example, JDE_HOME_1.

CAUTION: You cannot specify a directory that already exists.

6. Click the **Next** button.



7. On Enter Admin Password, enter and confirm the password for the jde_admin user.

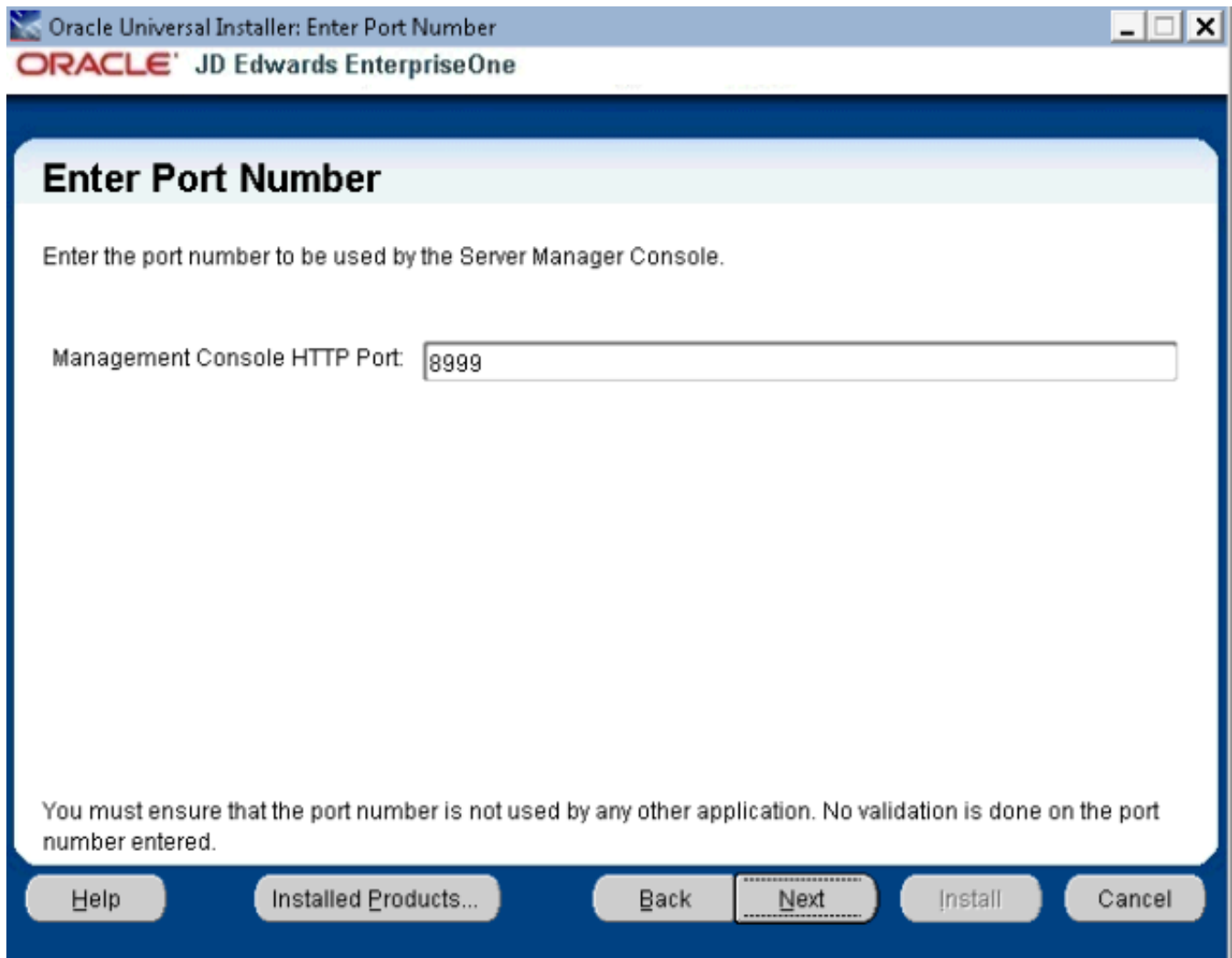
Note: The user name itself cannot be changed from jde_admin. The password must be at least eight (8) characters in length and cannot contain space or blank character values. Values are alphanumeric and these special characters: ! @ # \$ %. At least one (1) special character is required in the password.

Note: The default value for the user named jde_admin is automatically populated by the Management Console installer and cannot be altered. This is the administrative user account that is associated with the Management Console.

CAUTION: Because there is no programmatic way to retrieve a lost or forgotten password, it is critical that you remember and safeguard this password. If the password is forgotten or lost, the only recovery is a complete reinstallation of Server Manager. If you reinstall the Management Console and specify the JMX port the original installation was configured to use, you will retain all your managed homes and associated instances along with the configuration of those instances. However, you will lose this data:

- o Console configuration, which includes database information entered using the Setup Wizard and information regarding security server(s) used to authenticate users.
- o User Configuration, which are the added JD Edwards EnterpriseOne users and defined user groups, including their permissions.
- o Server Groups and associated template configurations.
- o Defined monitors and their associated monitor history.

8. Click the **Next** button.



9. On Enter Port Number, complete this field:

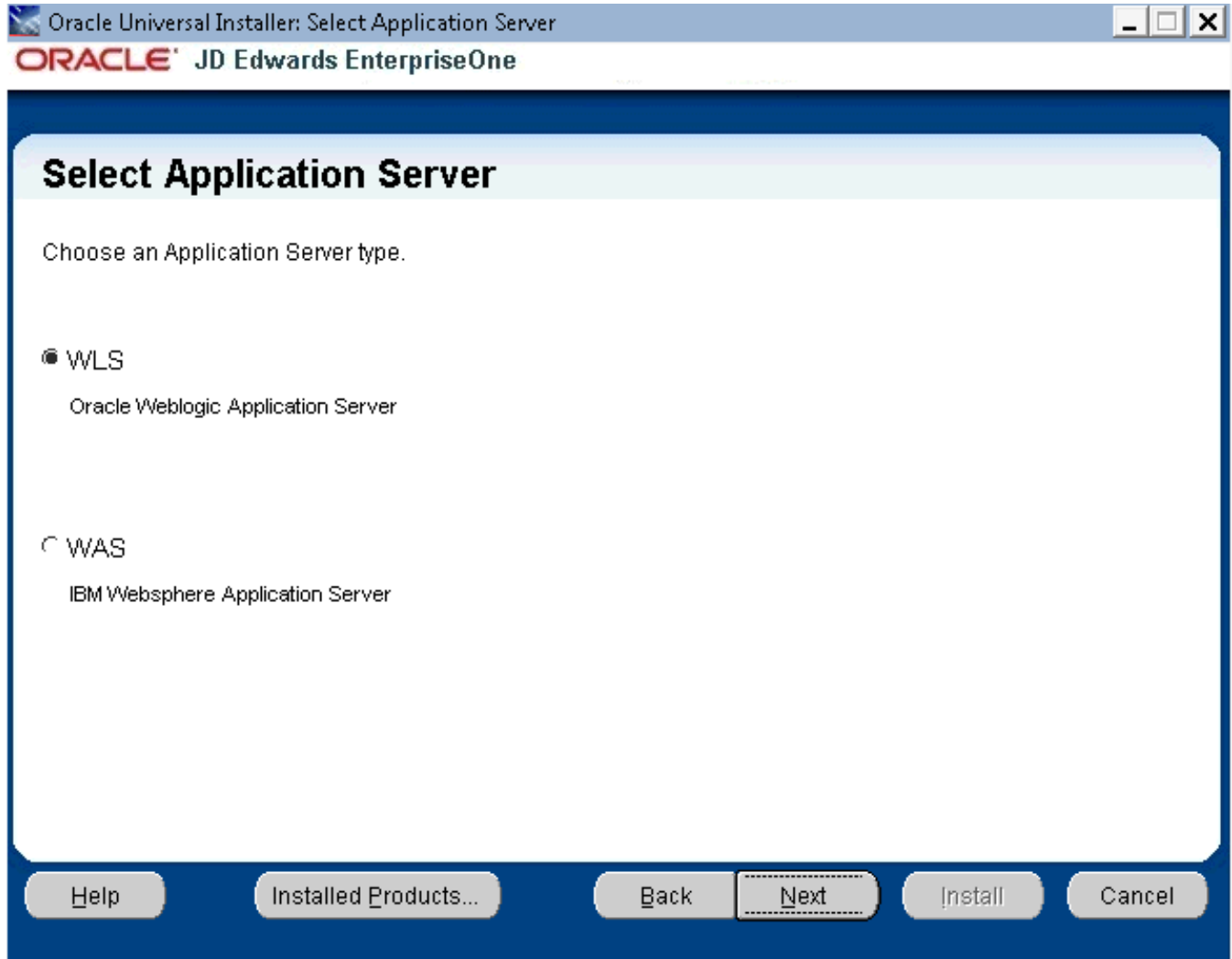
- o **Management Console HTTP Port**

Enter valid unused port number for use by the Management Console.

The default value is 8999.

CAUTION: This port number must be available and cannot be in use by any other application on this machine. Since the installer cannot validate the port, you must be certain that these conditions are met or else the Management Console will not start.

If there is insufficient disk space to complete the installation on the Management Console target machine, the installer displays an error message.



Note: If using Oracle Enterprise Linux, the above screen will not appear. The selection will default to WLS.

10. On Select Application Server, select this radio button:

WLS

Oracle WebLogic Application Server

11. Click the **Next** button.

Oracle Universal Installer: Enter Information for Weblogic server
ORACLE JD Edwards EnterpriseOne

Enter Information for Weblogic server

Enter informations for Weblogic server

Install Directory	<input type="text" value="C:\Oracle\Middleware\wls_server_10.3"/>
Host/IP	<input type="text" value="shravind-idc.peoplesoft.com"/>
Node Manager Machine Name	<input type="text" value="mymachine1"/>
Domain Port	<input type="text" value="7001"/>
Admin User Name	<input type="text" value="weblogic"/>
Admin User Password	<input type="password" value="*****"/>

Enter proper values, no validation is done on these values

Help Installed Products... Back Next Install Cancel

12. On Enter Information for WebLogic Server, complete the following fields:

- o *Install Directory*

Enter the path to the WebLogic installation directory. For example:

Microsoft

WebLogic Server 11g

`C:\Oracle\Middleware\wlserver_10.3`

WebLogic Server 12c

`C:\Oracle\Middleware\Oracle_Home\wlserver`

WebLogic Server 14c

`C:\Oracle\Middleware\Oracle_Home\wlserver`

Linux and Solaris

WebLogic Server 11g

`/u01/Oracle/Middleware/wlserver_10.3`

WebLogic Server 12c

`/u01/Oracle/Middleware/Oracle_Home/wlserver`

WebLogic Server 14c

`/u01/Oracle/Middleware/Oracle_Home/wlserver`

- o *Host/IP*

Enter the hostname or the IP Address at which the WebLogic Admin Server is listening for http/t3 connections. This is usually the hostname/IP Address of the physical machine. For example:

<machine name>us.example.com

- o *Node Manager Machine Name*

The nodemanager machine name is not necessarily the physical machine name, but it can be the same. This is the logical name of the nodemanager machine as displayed in the WebLogic Admin Console.

- o *Domain Port*

Enter the port number on which WebLogic AdminServer is listening for http/t3 connections. This value is configured when you created the WebLogic Domain.

- o *Admin User Name*

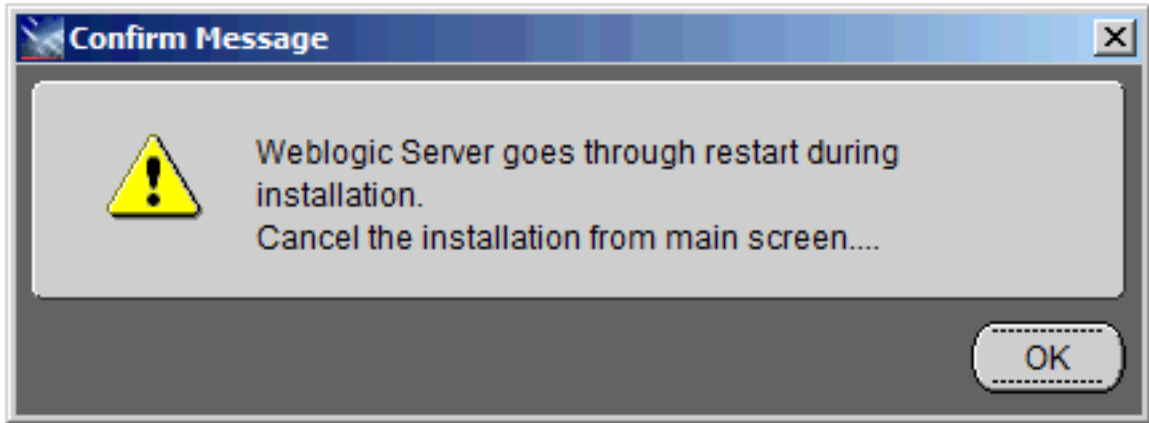
Enter the user name of the WebLogic Server admin account.

- o *Admin User Password*

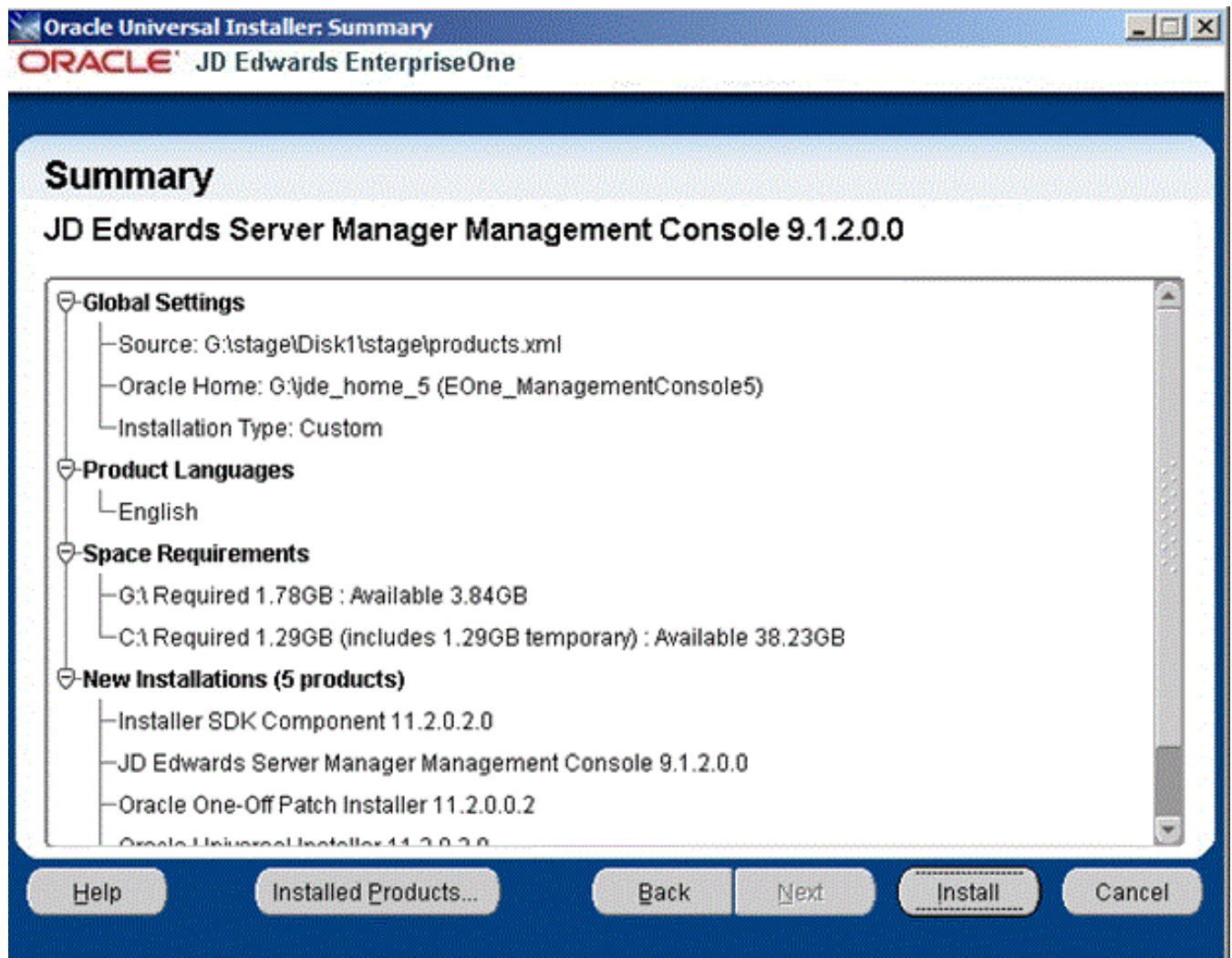
Enter the password for the WebLogic Server admin account.

CAUTION: The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items. If you enter invalid values, you will have to re-run the installer with the correct values.

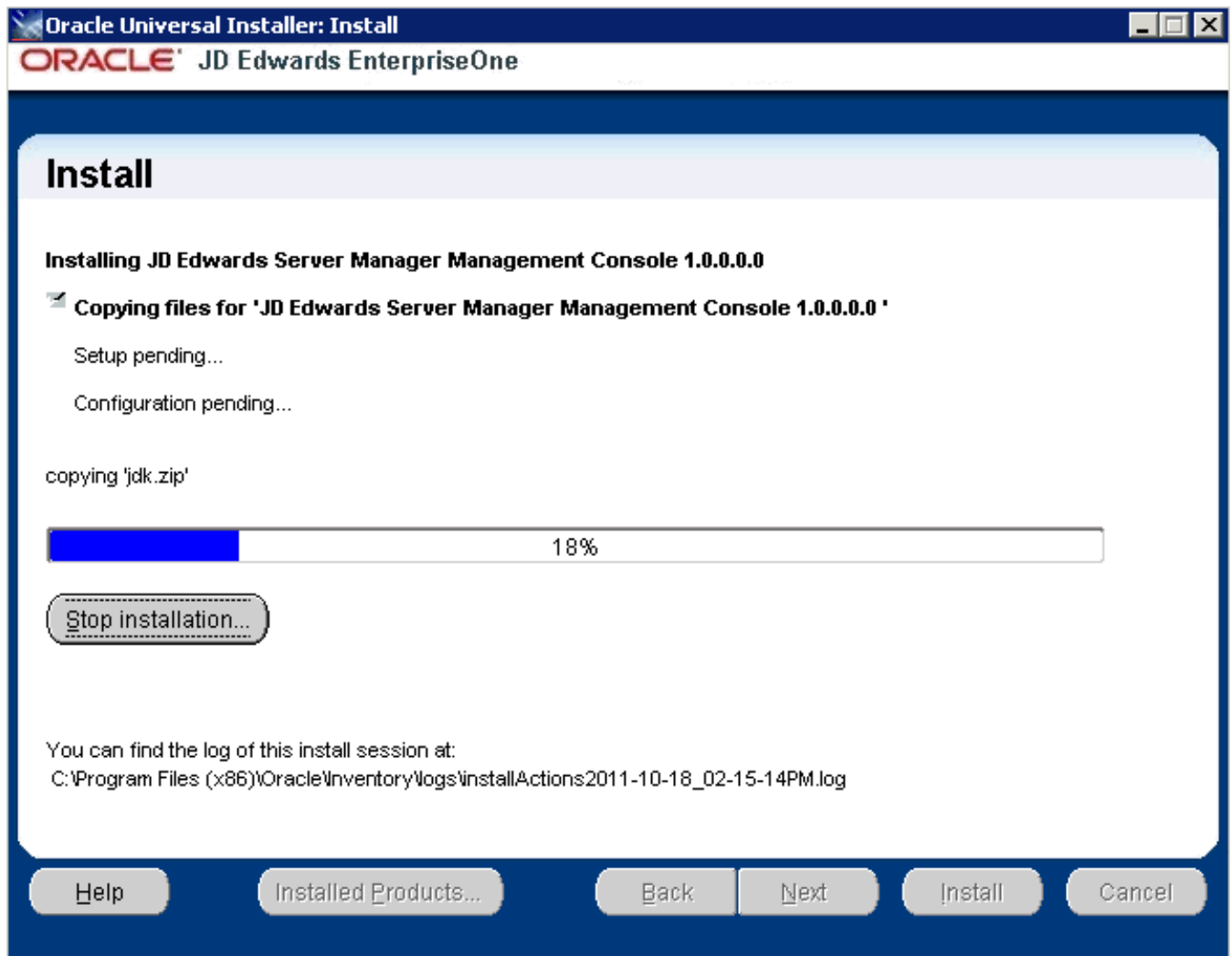
13. Click the **Next** button.



14. A popup dialog is displayed with the message that the AdminServer will be restarted during the installation. Click **OK** to continue or click **Cancel** in the next Summary panel to abort the installation if you do not wish to have the AdminServer restarted at this time.

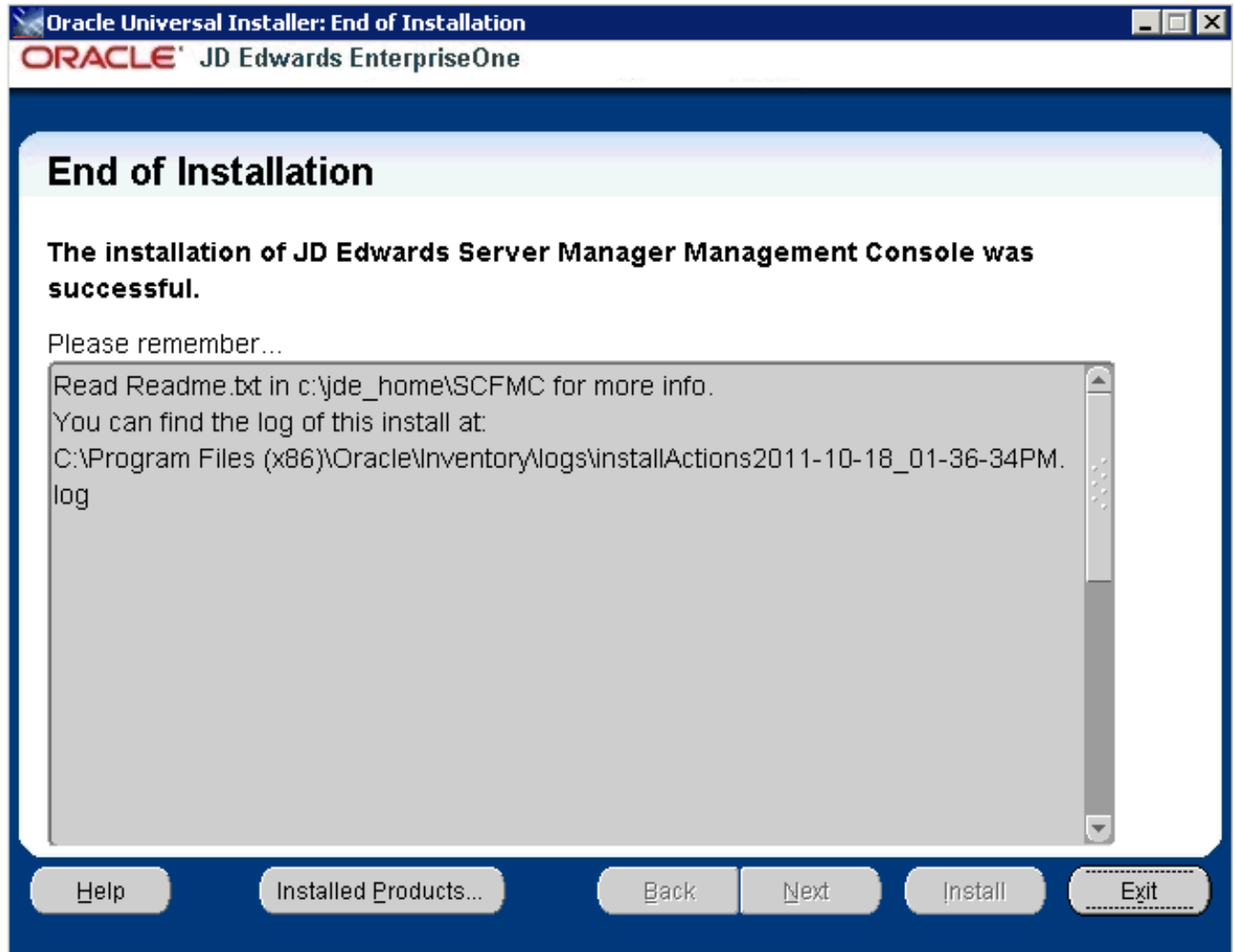


15. On Summary, verify your selections and click the **Install** button to begin the installation.



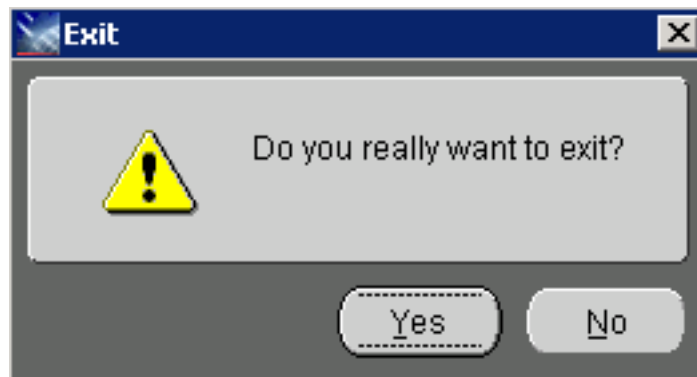
The Install progress screen is displayed. Note that this screen displays the location of the log of this installation. For example:

`C:\Program Files (x86)\Oracle\Inventory\logs\installActions2011-10-18-02-15-14PM.log`



16. On End of Installation, verify the installation was successful. The “Please remember ...” section also provides the installation log location.

17. Click **Exit** to exit the Oracle Universal Installer for the Server Manager Management Console.



18. On the Exit dialog, click the **Yes** button.

Verifying the Server Manager Console Installation on WebLogic Server

To verify the Server Manager Console Installation on WebLogic Server:

1. Verify the `jmxremote_optional.jar` and `ManagementLogonModule_JAR.jar` files are in this directory:

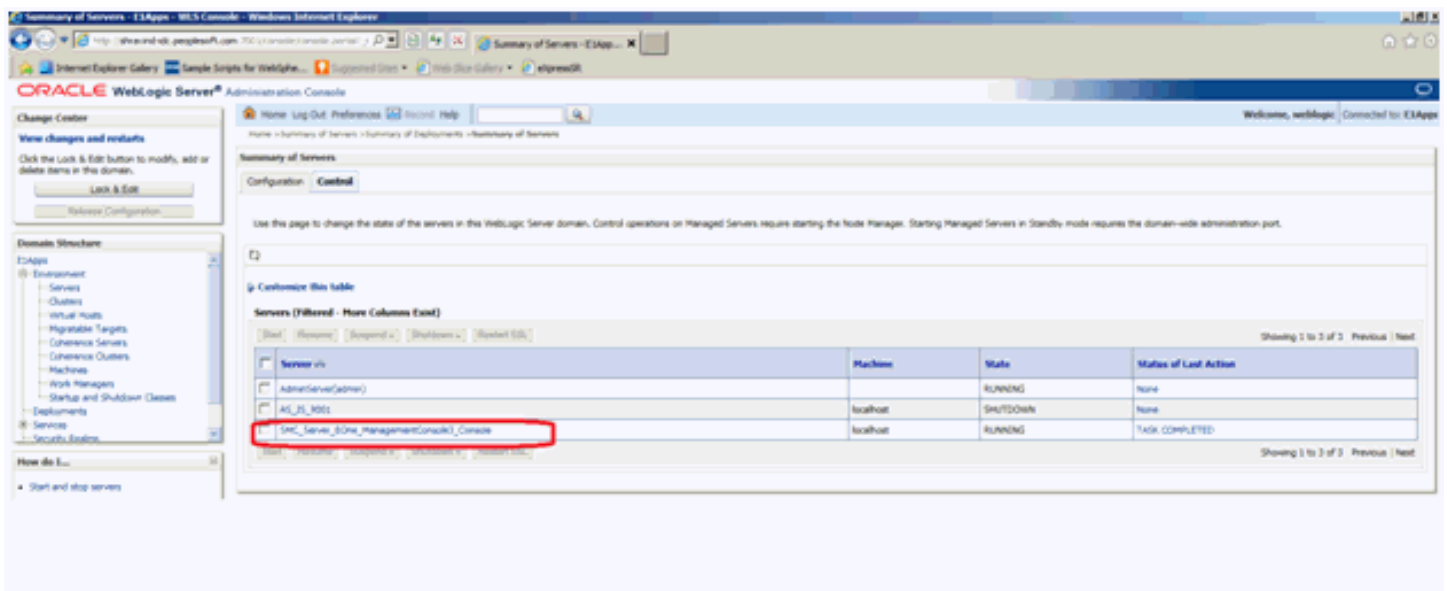
Microsoft Windows

`%DomainDir%\lib`

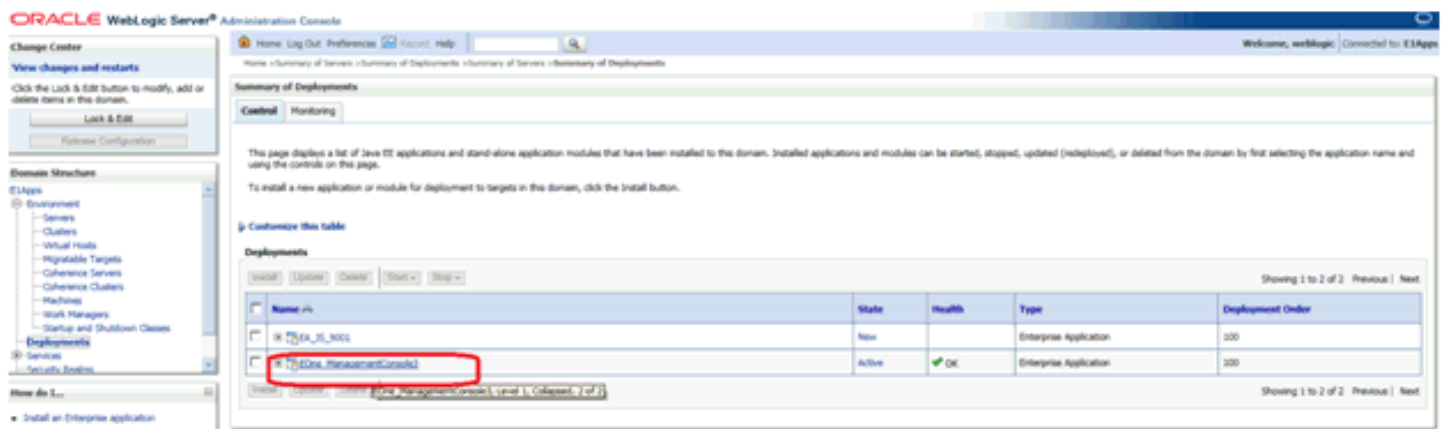
Linux or Solaris

`$DomainDir/lib`

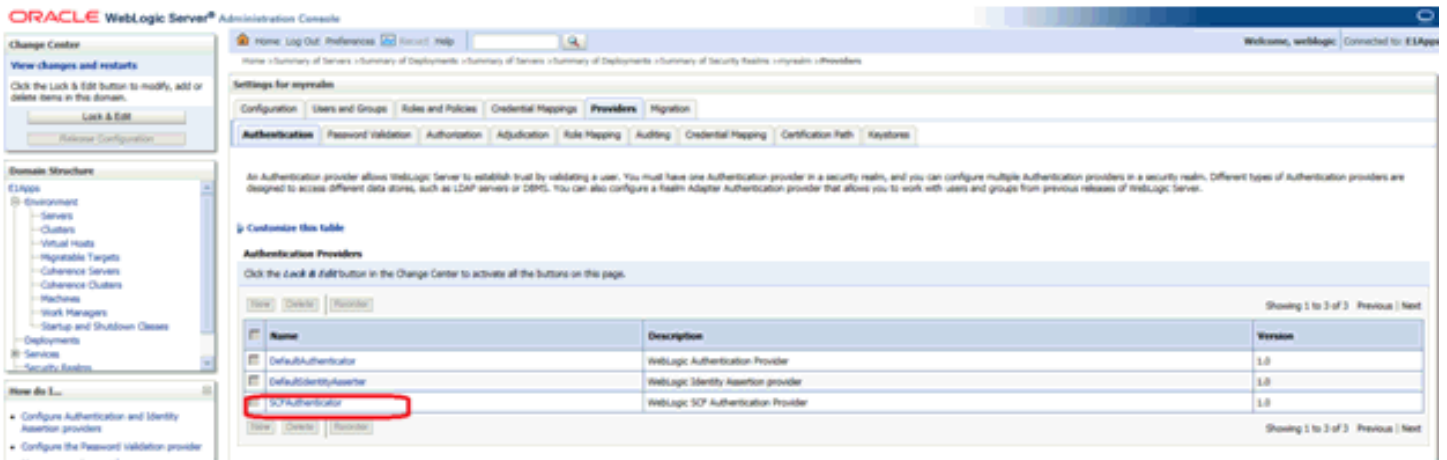
- Go to the WebLogic Admin Server console and navigate to Environment > Servers. Verify that the Server Manager Console installer created a new J2EE Server and that the state of that server is RUNNING. The following screen shows an example.



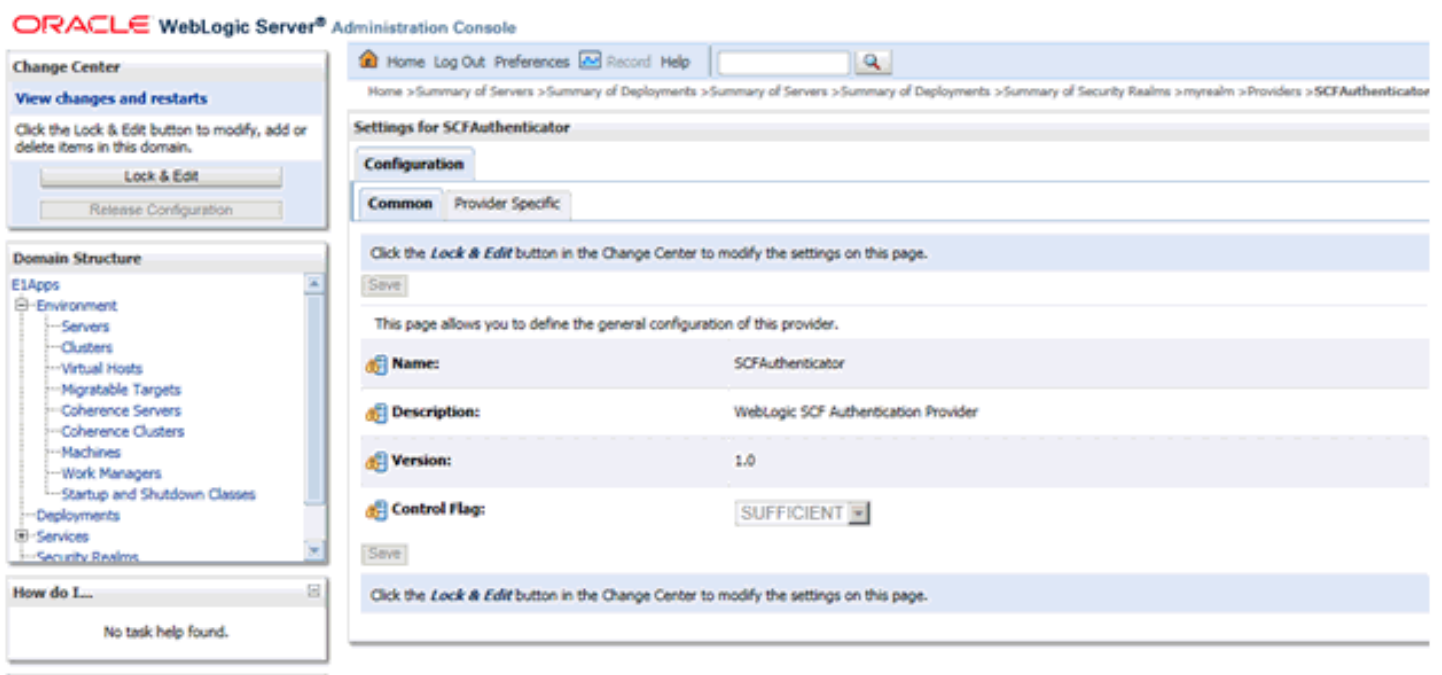
- Go to Deployments and verify that the Server Manager Console is installed. The following screen shows an example.



- Go to Security Realms > myrealm > Providers and verify that the SCFAuthenticator is configured. The following screen shows an example.



- Go to the Configuration tab and verify that both the SCFAuthenticator and DefaultAuthenticator have Control Flags that are set to SUFFICIENT. The following screen shows an example.



6. Verify that after the initial installation of the Server Manager Console, an administrator can sign on to the Server Manager Console using the `jde_admin` user and password specified during the installation. Access the Server Manager Console using this URL:

`http://servername:port/manage`

where `server_name` is the name of the Server Manager machine on which the Server Manager Console is installed, and

where `port` is the port that you specified for the Server Manager Console when you ran the Server Manager Console installer.

For example:

`http://server:8999/manage/`

ORACLE JD Edwards EnterpriseOne Server Manager



Enable SSL for Server Manager Console on the WebLogic Server

Note: The certificate and the keystore files that are used to configure the TLS settings with Server Manager Console must be used for configuring the SSL setting as well.

To enable SSL for the Server Manager Console on the WebLogic Server:

1. Access the WebLogic Admin Console in the browser for the WebLogic domain in which the Server Manager Console is installed. A sample URL would be: `https://denpbds11.example.com:7001/console`
2. Login to the WebLogic Admin Console using WebLogic Administrative Credentials.

3. Navigate to Environments -> Servers.
4. Click on the Server Manager Console J2ee server (in the example below it will be SMC_Server_E1WLSSMC_Console).
5. Click **Lock and Edit** (if this option is available).
6. Ensure you are in the General -> Configuration tab.
7. Select the **SSL Listen Port Enabled** check box.
8. Change the SSL Listen Port to something different than the existing HTTP Server Port for the Server Manager Console. (In the example below, the HTTP Port is 8999 and the HTTPS/SSL Port has been set to 9000.

The screenshot displays the Oracle WebLogic Server Administration Console interface. The main content area shows the configuration for the server instance 'SMC_Server_E1WLSSMC_Console'. The 'General' tab is selected, and the 'Configuration' sub-tab is active. The configuration table includes the following settings:

Property	Value	Description
Name	SMC_Server_E1WLSSMC_Console	An alphanumeric name for this server instance.
Template	(No value specified)	Get the base server.
Machine	localhost	The WebLogic Server host computer (machine) on which this server is running.
Cluster	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs.
Listen Address		The IP address or DNS name this server uses to listen for incoming connections.
Listen Port Enabled	<input checked="" type="checkbox"/>	Specifies whether this server can be reached through the default Listen Port.
Listen Port	8999	The default TCP port that this server uses to listen for regular connections.
SSL Listen Port Enabled	<input checked="" type="checkbox"/>	Indicates whether the server can be reached through the default SSL Listen Port.
SSL Listen Port	9000	The TCP/IP port at which this server listens for SSL connections.
Client Cert Proxy Enabled	<input type="checkbox"/>	Specifies whether the HttpClusterServlet proxies the client certificates.
Java Compiler	javac	The Java compiler to use for all applications hosted on this server.
Diagnostic Volume	Low	Specifies the volume of diagnostic data that is automatically generated. The WLDLF diagnostic volume setting does not affect explicitly configured diagnostic volume. controls the volume of events generated for Flight Recorder.

9. Click **Save**.

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Home > Summary of Servers > Summary of Machines > localhost > Summary of Environment > Summary of Servers > SMC_Server_E1WLSSMC_Console

Messages
 Settings updated successfully.

Settings for SMC_Server_E1WLSSMC_Console

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload H

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

Name: SMC_Server_E1WLSSMC_Console

Template: (No value specified) [Change](#)

Machine: localhost

Cluster: (Stand-Alone)

Listen Address:

Listen Port Enabled

Listen Port:

SSL Listen Port Enabled

SSL Listen Port:

Client Cert Proxy Enabled

Java Compiler:

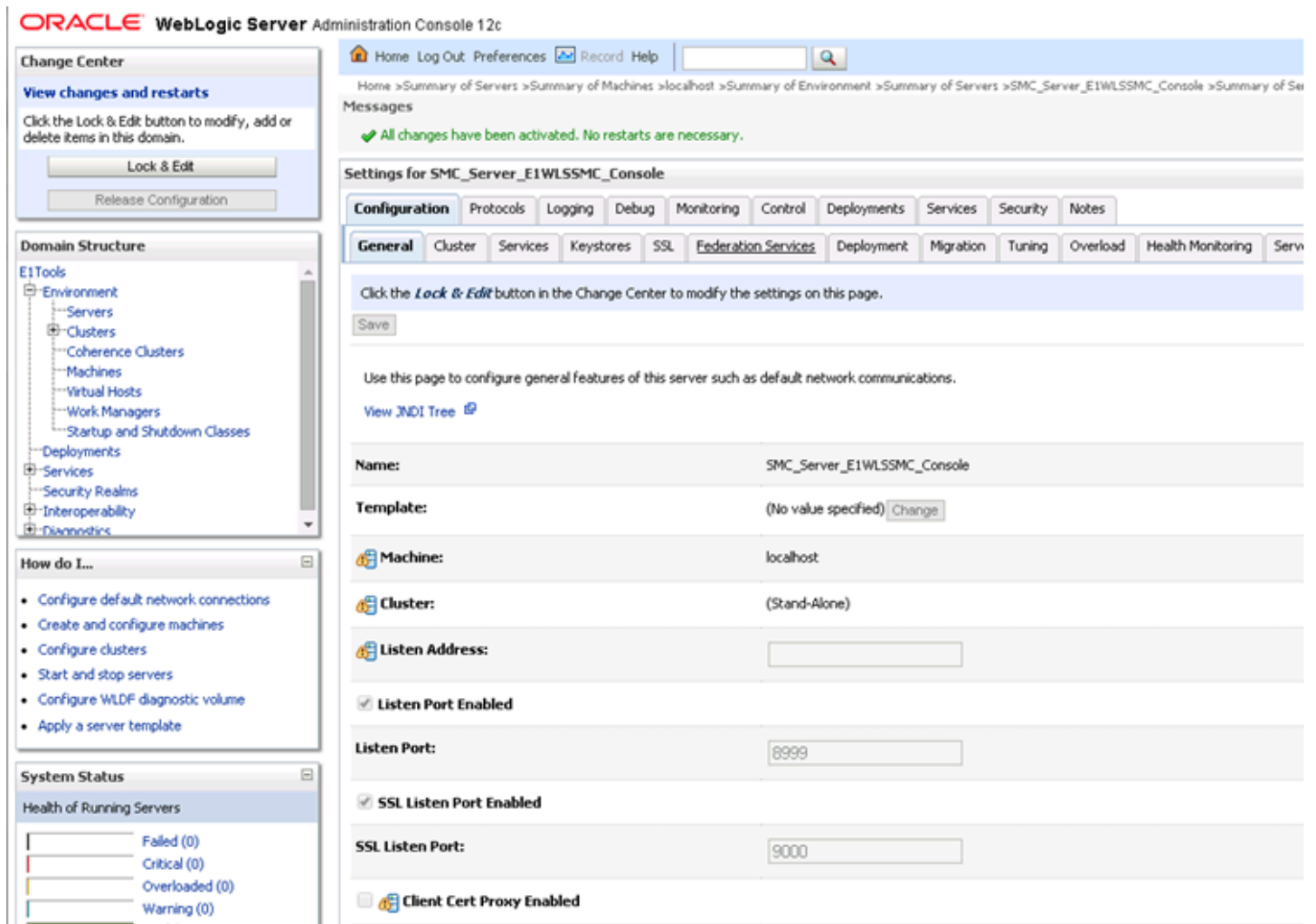
Change Center
 View changes and restarts
 Pending changes exist. They must be activated to take effect.
 Activate Changes
 Undo All Changes

Domain Structure
 E1Tools
 Environment
 Servers
 Clusters
 Coherence Clusters
 Machines
 Virtual Hosts
 Work Managers
 Startup and Shutdown Classes
 Deployments
 Services
 Security Realms
 Interoperability
 Diagnostics

How do I...
 Configure default network connections
 Create and configure machines
 Configure clusters
 Start and stop servers
 Configure WLDf diagnostic volume
 Apply a server template

System Status
 Health of Running Servers
 Failed (0)
 Critical (0)
 Overloaded (0)
 Warning (0)
 OK (?)

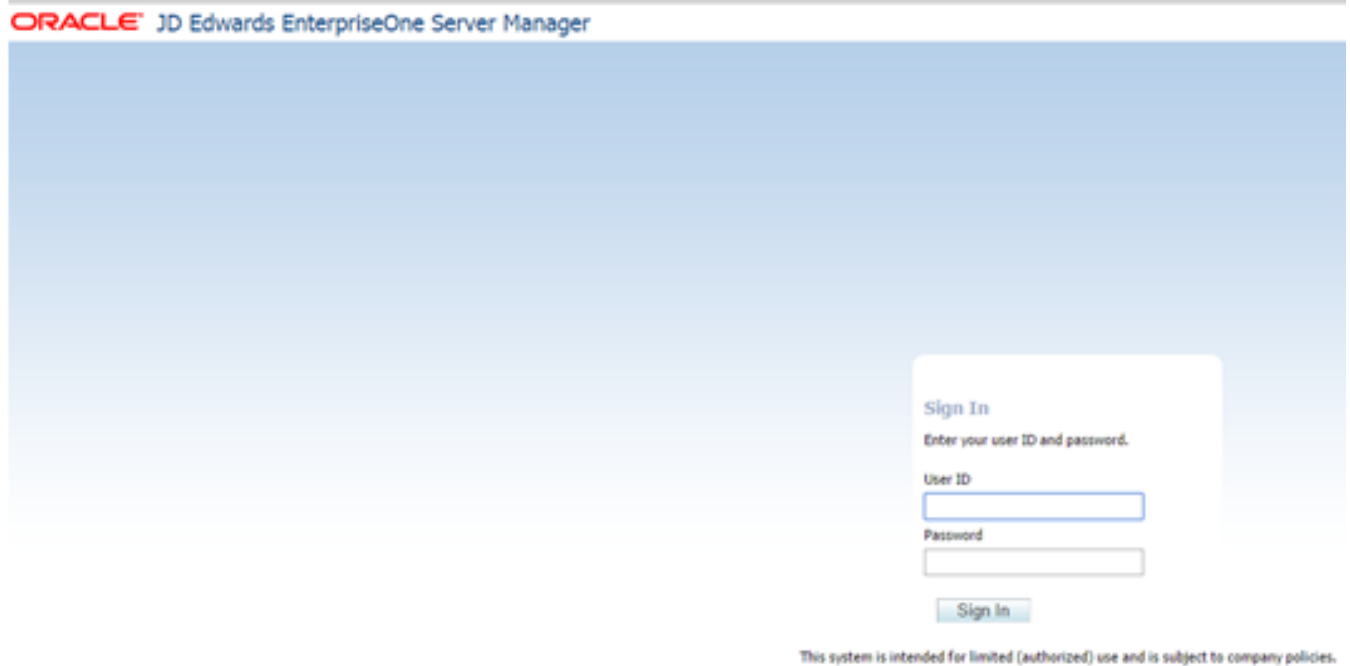
10. Click **Activate Changes**.



11. Based on the message displayed, it may or may not be required to restart the Server Manager Console j2ee server.
12. If required, stop and start the Server Manager Console J2ee server.

- Next, access the Server Manager Console in the browser using an HTTPS/SSL based URL (`https://<Server_Manager_Console_HostName>:<SSL_Listen_Port>/manage/home`). In this example the URL is `https://denpbds11.example.com:9000/manage/home`

Note: If you are not able to access the Server Manager Console at this point, see **Troubleshooting Access to the Server Manager Console** below.



- Go to *Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore* and perform the steps.

Troubleshooting Access to the Server Manager Console

If Server Manager self-update does not work as expected to update the Server Manager Console from 9.2.2.1 to a higher Tools release. This process may not function as expected if the Admin Server of the Domain in which Server Manager Console is installed is not configured with SSL. To verify this potential issue, check the Server Manager Console Weblogic J2EE Server `.out` log for the existence of a message similar to this:

```
Oct 12, 2017 11:56:37 PM com.jdedwards.mgmt.agent.ElAgent
  lookupAdminServerDetailsFromConfigXml
INFO: Entering lookupAdminServerDetailsFromConfigXml
Oct 12, 2017 11:56:37 PM com.jdedwards.mgmt.agent.ElAgentUtils getServerType
INFO: Management Server is running on WLS
Oct 12, 2017 11:56:37 PM com.jdedwards.mgmt.agent.ElAgent
  lookupAdminServerDetailsFromConfigXml
INFO: Parsing the config.xml file 'C:\WLS12212\user_projects\domains\base_domain\config
\config.xml'.
Oct 12, 2017 11:56:37 PM com.jdedwards.mgmt.agent.ElAgent
  lookupAdminServerDetailsFromConfigXml
WARNING: Error parsing config.xml at location 'C:\WLS12212\user_projects\domains
\base_domain\config\config.xml'.
```

```
<Oct 12, 2017, 11:56:37,963 PM MDT> <Warning> <com.jdedwards.mgmt.agent.ElAgent>
<BEA-000000> <Error parsing config.xml at location 'C:\WLS12212\user_projects\domains
\base_domain\config\config.xml'.>
Oct 12, 2017 11:56:37 PM com.jdedwards.mgmt.agent.ElAgent
lookupAdminServerDetailsFromConfigXml
WARNING: Exception: null
<Oct 12, 2017, 11:56:37,963 PM MDT> <Warning> <com.jdedwards.mgmt.agent.ElAgent>
<BEA-000000> <Exception: null>
Oct 12, 2017 11:56:37 PM com.jdedwards.mgmt.targets.mgmtconsole.ManagementConsole
postRegister
WARNING: Unable to create the StandaloneOC4J/StandaloneWLS/StandaloneWAS object:
java.lang.NullPointerException
    at com.jdedwards.mgmt.targets.owl.StandaloneWLS.<init>(Unknown Source)
    at com.jdedwards.mgmt.targets.mgmtconsole.ManagementConsole.postRegister (Unknown
Source)
```

Resolution:

Use the following procedure to resolve this issue:

1. Logon to the Weblogic Admin Console
2. Set the option for **SSL Listen Port** as **Enabled**.
3. Save the changes.
4. Now reverse the setting for **SSL Listen Port** to set it as **Disabled**.

This action adds the `<enabled>false</enabled>` entry into the `config.xml` file for the Admin Server, which allows the self-updating of Tools Release 9.2.2.1 to function as expected.

Obtain and Install CA Certificates in Oracle WebLogic Server

The deployment of JD Edwards EnterpriseOne Server Manager Console and Server Manager agents includes temporary self-signed Certificate Authority (CA) certificates. Self Signed Certificates are not inherently trusted by the JDK / JRE / Java distributions and are not recommended for Production environments. Because self-signed 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, Symantec Corporation, or Thawte.

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 (<https://ssltools.websecurity.symantec.com/checker>).
5. Submit the CSR to the Certificate Authority such as Entrust or Symantec Corporation.
6. Logged in as the WebLogic Administrator, you must manually modify of Oracle WebLogic Server to use the new Keystore.

Tip: For additional details on working with CA certificates on your Oracle WebLogic Server, refer to this guide: *Fusion Middleware Administering Security for Oracle WebLogic Server 12.1.3* at this link: https://docs.oracle.com/middleware/1213/wls/SECMG/ssl_overview.htm#SECMG718

Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore

To import the Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore:

CAUTION: You **must** perform these steps for all Server Manager Agent JDKs.

1. Export the Server Manager Console Certificate to a file using these steps:
 - a. From the browser click the lock icon on the left hand side of the URL of the HTTPS/SSL based Server Manager Console URL.
 - b. Click on **Certificate Information**.
 - c. Go to details tab and select the **Copy to File** option.
 - d. Click **Next**.
 - e. Select DER encoded binary X.509 (.CER) format.
 - f. Click **Next**.
 - g. Enter file information.
 - h. I have given the name as SMC_Certificate.cer.
 - i. Click **Next**.
 - j. Click **Finish**.
 - k. You will get a message saying "Export is Successful".
 - l. You can view the Certificate in the path given in the above step.
2. This Certificate needs to be imported into the Truststore/Keystore of each of the Server Manager Agents (cacerts file of X:\jde_home_1\SCFHA\jdk\jre\lib\security\cacerts file).
3. Before performing the import, backup the cacerts file located at X:\jde_home_1\SCFHA\jdk\jre\lib\security\cacerts file.

- Below is the command to import the Certificate file on Windows Platform. A similar step needs to be done for the Linux/UNIX/AS400 platforms and also for Server Manager Agents installed on these platforms. Import the Certificate using the command below. When prompted for whether you trust the Certificate, answer **Yes**.

```
X:\jde_home_1\SCFHA\jdk\jre\bin\keytool -import -alias smc_cert -file C:\SMC_Certificate.cer -keystore
```

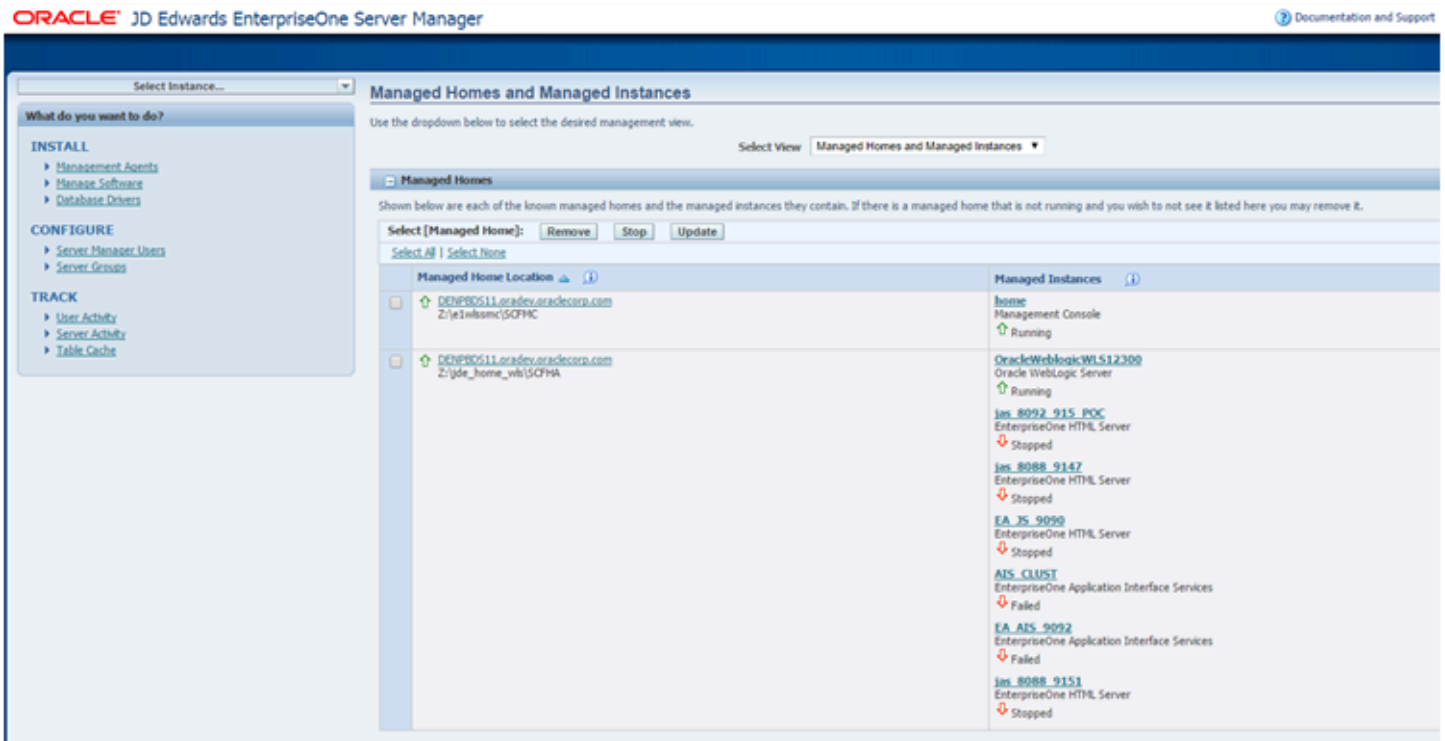
```
X:\jde_home_1\SCFHA\jdk\jre\lib\security\cacerts -storepass password
```

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\shravind.ORADEU>Z:\jde_home_4\SCFHA\jdk\jre\bin\keytool -import -alias
smc_cert -file C:\SMC_Certificate.cer -keystore Z:\jde_home_4\SCFHA\jdk\jre\lib\
security\cacerts -storepass changeit
Owner: CN=DENPBDS11.oradev.oraclecorp.com, OU=DENPBDS11Node07Cell, OU=DENPBDS11N
ode09, O=IBM, C=US
Issuer: CN=DENPBDS11.oradev.oraclecorp.com, OU=Root Certificate, OU=DENPBDS11Nod
e07Cell, OU=DENPBDS11Node09, O=IBM, C=US
Serial number: 46d2afd04b86
Valid from: 5/12/15 11:18 PM until: 5/11/16 11:18 PM
Certificate fingerprints:
    MD5: D3:27:30:2C:AE:7A:A9:9E:6F:BC:A6:DD:4C:AC:CE:90
    SHA1: 9E:BF:C6:06:BA:A9:EE:D6:CB:B0:92:15:C3:D5:E4:49:D0:AD:D0:FA
Trust this certificate? [no]: yes
Certificate was added to keystore
C:\Users\shravind.ORADEU>_
```

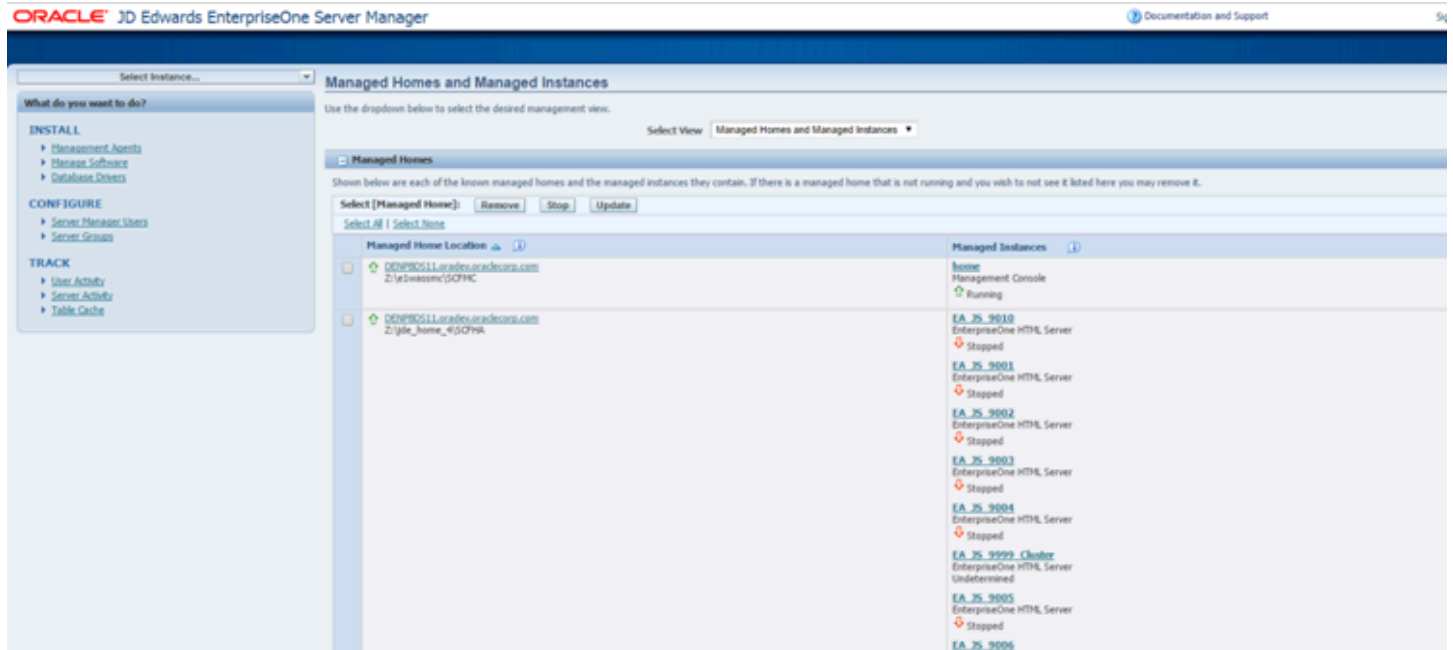
- After this step, restart the Server Manager Agent. This step needs to be done on each of the Server Manager Agent machines. Without this step the Server Manager Agent may not be able to communicate with the Server Manager Console.

- Next, login into the Server Manager Console and ensure that above Server Manager Agent is showing up with a Running Status.

On WLS:



On WAS:



This completes the configuration required for running the Server Manager Console on WebLogic/WebSphere with HTTPS/SSL Enabled and completes the importing of the Certificate on the Server Manager Agents.

Hostname Mismatch Errors

If the hostname in the Certificate generated by WebSphere or WebLogic does not exactly match the Fully Qualified Hostname of the Server Manager Console machine, then you will see the type of errors listed below in the Server Manager Agent stderr.log/e1agent.logs.

In this case a valid Self Signed Certificate will need to be created using the keytool utility and imported into the WebLogic Custom Truststore and Custom Keystore, and WebLogic will need to be configured to use the Custom Truststore and Custom Keystore. Similarly on WebSphere, a Self Signed Certificate will need to be created and will need to be imported. trust.p12 and key.p12 files and will need to be set as the default Certificate using the iKeyMan.bat/.sh utility. This Self Signed Certificate will also need to be imported in the cacerts file of the Server Manager Agents.

```
javax.net.ssl.SSLException: hostname in certificate didn't match: <10.139.162.143> !=
<denpbd11.example.com> at org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:227)
at org.apache.http.conn.ssl.BrowserCompatHostnameVerifier.verify(BrowserCompatHostnameVerifier.java:54)
at org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:147)
at org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:128) at
org.apache.http.conn.ssl.SSLSocketFactory.connectSocket(SSLSocketFactory.java:437) at
org.apache.http.impl.conn.DefaultClientConnectionOperator.openConnection(DefaultClientConnectionOperator.java:180)
at org.apache.http.impl.conn.ManagedClientConnectionImpl.open(ManagedClientConnectionImpl.java:294)
at org.apache.http.impl.client.DefaultRequestDirector.tryConnect(DefaultRequestDirector.java:643)
```

```
at org.apache.http.impl.client.DefaultRequestDirector.execute(DefaultRequestDirector.java:479)
at org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:906)
at org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:805) at
org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:784) at
com.jdedwards.mgmt.agent.UserPasswordCallBack._getUserCredentials(UserPasswordCallBack.java:40)
at com.jdedwards.mgmt.agent.UserPasswordCallBack.<init>(UserPasswordCallBack.java:31) at
com.jdedwards.mgmt.agent.EIAgent$ManagementServerDaemonThread.run(EIAgent.java:2259) at
java.lang.Thread.run(Thread.java:722)
```

Import the Server Manager Console Certificate into All Java Installations That Are Used by Embedded Agents

CAUTION: As is true for the preceding procedure, you **must** perform these steps for all Server Manager Agent JDKs.

Using the principles shown preceding procedure, you **must** also import the Server Manager Console certificate into all Java installations that are used by embedded agents to communicate with the Server Manager Console. Specifically, the certificate needs to be imported for each of the following:

- JDK used by WebLogic or WebSphere
- JRE used by the Enterprise Server kernel processes.

This is either the JRE specified in:

- The JDE system directory. For example:

```
<platform pack install location>/jdedwardspack/e910/system/jre/
```

- The value of `InProcessJVMHome` in the `JDE.INI` file.

Example: Importing the certificate into the JDK used by the embedded agent on the Enterprise Server:

- If a value is assigned to `InProcessJVMHome` in the `JDE.INI` file on the Enterprise Server, you should import the certificate into the `cacerts` file of the JRE corresponding to the value of `InProcessJVMHome`. You can adapt instructions below to use the path to this JRE.
- If no value is assigned to `InProcessJVMHome` in the `JDE.INI` file, you should import the certificate into the `cacerts` file of the JRE in the JDE system directory. For example, the directory might be named:

```
<platform pack install location>/jdedwardspack/e910/system/jre/
```

Below is an example command line to import a certificate (enter as a single contiguous line):

```
/opt/jdedwardspack/e920/system/jre/bin/keytool -import -trustcacerts -keystore /opt/jdedwardspack/e920/system/jre/lib/security/cacerts -storepass PASSWORD -noprompt -alias mynewcert -file
```

The above commands results in the new certificate being created as shown below:

```
/opt/jde_home_ent/SCFHA/jdk/jre/bin/mynewcertificate.cer
```

This example assumes the following:

- Certificate password is **PASSWORD**

- Path to the JRE is:

```
/opt/jdedwardsppack/e920/system/jre
```

- Path to the .cer file is:

```
/opt/jde_home_ent/SCFHA/jdk/jre/bin/mynewcertificate.cer
```

Using the above example, for your installation you should edit the values accordingly.

Troubleshooting the Server Manager Console Installation on WebLogic Server

To troubleshoot the Server Manager Console Installation on WebLogic Server:

1. Verify that all the prerequisites are met as listed in the section of this guide entitled: *Prerequisites for WebLogic Server*.
2. Locate and inspect the contents of the .out and .err log files located in these directories:

Microsoft Windows Platform

```
C:\<Server_Manager_Console_Home>\SCFMC\data\*.dat files
```

where <Server_Manager_Console_Home> is the Server Manager Console installation directory. For example:

```
C:\jde_home_1\SCFMC\data
```

Linux/Solaris Platforms

```
<Server_Manager_Console_Home>/SCFMC/data/*.dat files
```

where <Server_Manager_Console_Home> is the Server Manager Console installation directory. For example:

```
/u01/jde_home_1/SCFMC/data
```

3. Locate and inspect the contents of the Server Manager Console installer-related log files for errors. These logs are typically located in following locations:

Note: The location of these logs and the log file name are displayed on in the lower portion of the installer screens during the installation process.

```
C:\Program Files\Oracle\Inventory\logs
```

4. Locate and inspect the contents of the application server log files for errors. These logs are typically located in following locations:

Microsoft Windows

```
C:\Oracle\Middleware\user_projects\domains\E1Apps\servers\AdminServer\logs
```

```
C:\Oracle\Middleware\user_projects\domains\E1Apps\servers\SMC_Server_xxxx\logs
```

```
C:\Oracle\Middleware\wlserver_10.3\common\nodemanager\logs
```

Linux or Solaris

```
/u01/Oracle/Middleware/user_projects/domains/E1Apps/servers/AdminServer/logs
```

```
/u01/Oracle/Middleware/user_projects/domains/E1Apps/servers/SMC_Server_xxxx/logs
```

```
/u01/Oracle/Middleware/wlserver_10.3/common/nodemanager/logs
```

5. You might encounter this message: [Management:141245]Schema Validation Error in /config.xml if any managed servers are running.

Installing the Management Console on WebSphere Application Server

You can install the Server Manager Console on WebSphere Application Server on Microsoft Windows platforms.

See Also

Refer to this document for additional information about configuring the IBM WebSphere Application Server with JD Edwards EnterpriseOne:

- JD Edwards EnterpriseOne HTML Server on WebSphere Reference Guide

https://docs.oracle.com/cd/E61420_01/doc.92/e55810.pdf

Refer to the IBM resources for IBM WebSphere Application Server 7, or 8.5.5.0, or 9.0 Infocenter.

This section discusses these topics:

- *Starting and Stopping the Server Manager Console on WebSphere on the Microsoft Windows Platform*
- *General Hostname/IP Address Configuration Prerequisites*
- *Running the WebSphere Application Server Installer for the Server Manager Console*
- *Verifying the Server Manager Console Installation on WebSphere Application Server*
- *Enable SSL for Server Manager Console on the WebSphere Application Server*
- *Import the Server Manager Console Certificate into All Java Installations That Are Used by Embedded Agents*
- *Troubleshooting the Server Manager Console Installation on WebSphere Application Server*

Starting and Stopping the Server Manager Console on WebSphere on the Microsoft Windows Platform

For Tools Release 9.1 Update 2, the supported WebSphere version is 7.0.

For Tools Release 9.1 Update 2.3 onwards, WebSphere version 8.5.5.0 is also supported.

For Tools Release 9.2 Update 1 onwards, WebSphere version 9.0 is also supported.

When installing Server Manager Console on any version of WebSphere on Microsoft Windows, it is important to note that the installer does not configure the Server Manager Console as a Windows Service. Therefore, you must manually start and stop the Server Manager Console using the IBM utility called `startServer.bat`. This is also true for other JD Edwards EnterpriseOne components such as HTML Server, RTE Server, and BSSV Server.

To use the `startServer.bat` utility:

1. These instructions assume the Server Manager Console was installed into WebSphere with these properties:

- o **Installation Directory**

- C:\IBM\WebSphere\AppServer

- o **Profile to which the Server Manager Console is Installed**

- AppSrv01

- o **Name of the J2EE Container**

- SMC_Server_ManagementConsole1

2. Open a Microsoft Windows Command Prompt as an Administrator.

3. Use this command to start the Server Manager Console:

```
C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\startServer.bat SMC_Server_ManagementConsole1
```

4. Use this command to stop the Server Manager Console:

```
C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\stopServer.bat SMC_Server_ManagementConsole1
```

General Hostname/IP Address Configuration Prerequisites

This section lists the configuration prerequisites for the hostname and IP address:

- The hosts file must have the entry for localhost (loopback).
- The hosts file should have an entry for the correct IP Address of the machine mapping to the appropriate hostname of the machine.
- The hostname of the machine should not map to the IP Address 127.0.0.1, because that IP address is typically used for localhost.

Running the WebSphere Application Server Installer for the Server Manager Console

To install the Server Manager Console:

1. Log on to the machine onto which you are installing the Server Manager Management Console.
2. Change to the directory in which you extracted the Server Manager Console installer as described in the previous section of this chapter entitled: *Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools*.
3. Launch the OUI installer as follows:

Microsoft Windows

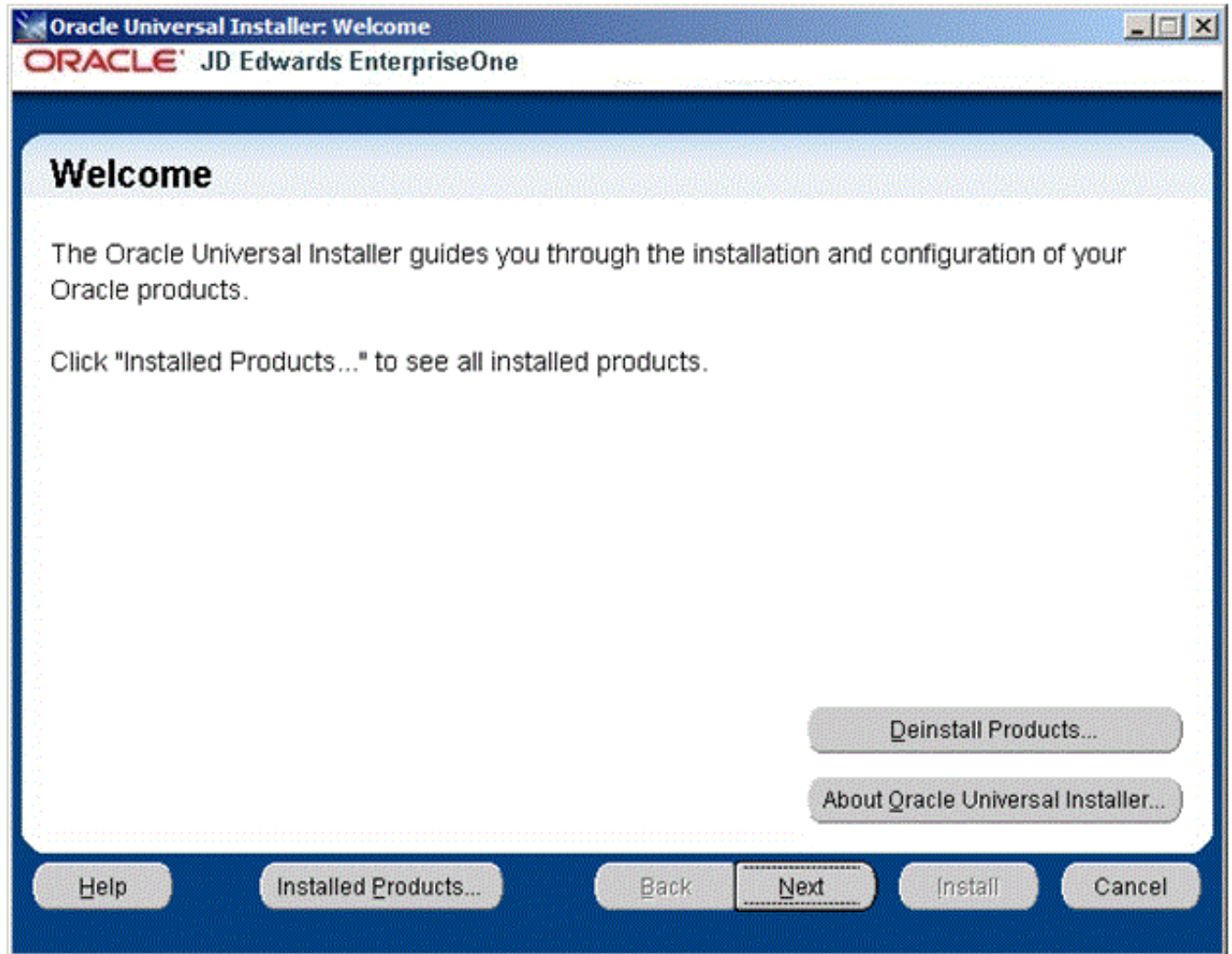
Using "Run As Administrator", run `setup.exe` from the directory in which you unzipped the installer. For example, if you followed the recommendation in *Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools*:

```
C:\SM_Console\Disk1\install
```

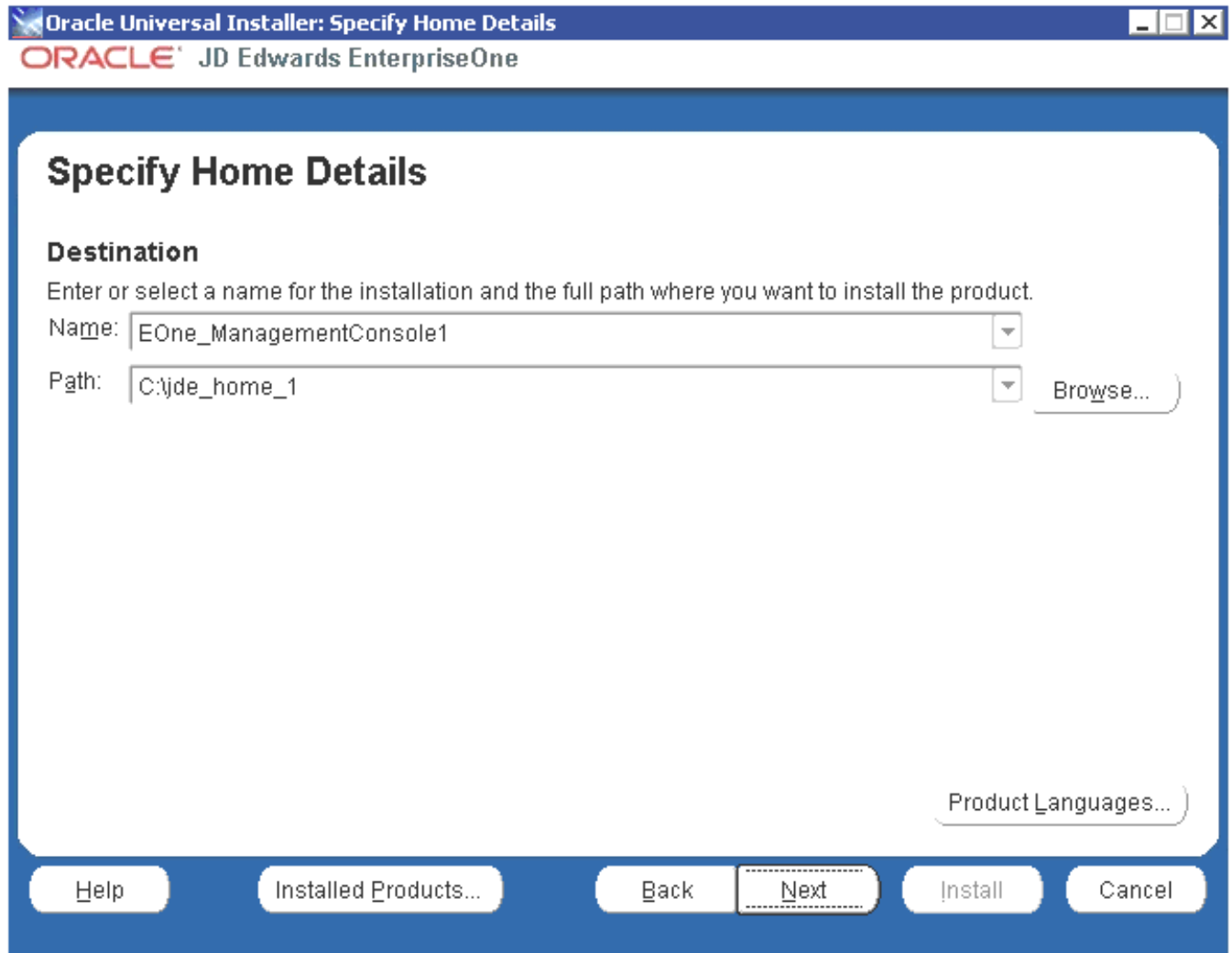
The Windows Command window starts indicating Windows is preparing to launch the Oracle Universal Installer for the Server Manager Management Console.

All Platforms

The Oracle Universal Installer (OUI) Wizard begins to initialize and prepare the JVM for the JD Edwards EnterpriseOne Management Console installer. This may take a few minutes to completely initialize. When the initialization is complete, a new and separate JD Edwards EnterpriseOne Management Console installer window is displayed.



4. On Welcome, click the **Next** button.



5. On Specify Home Details, complete these fields:

o *Name*

Enter a unique name of the Management Console. The default value is:

EOne_ManagementConsole

Note: If there is an existing installation of the Management Console with the default name, the installer will append the default name with a number to make it unique. For example, EOne_ManagementConsole1.

o *Path*

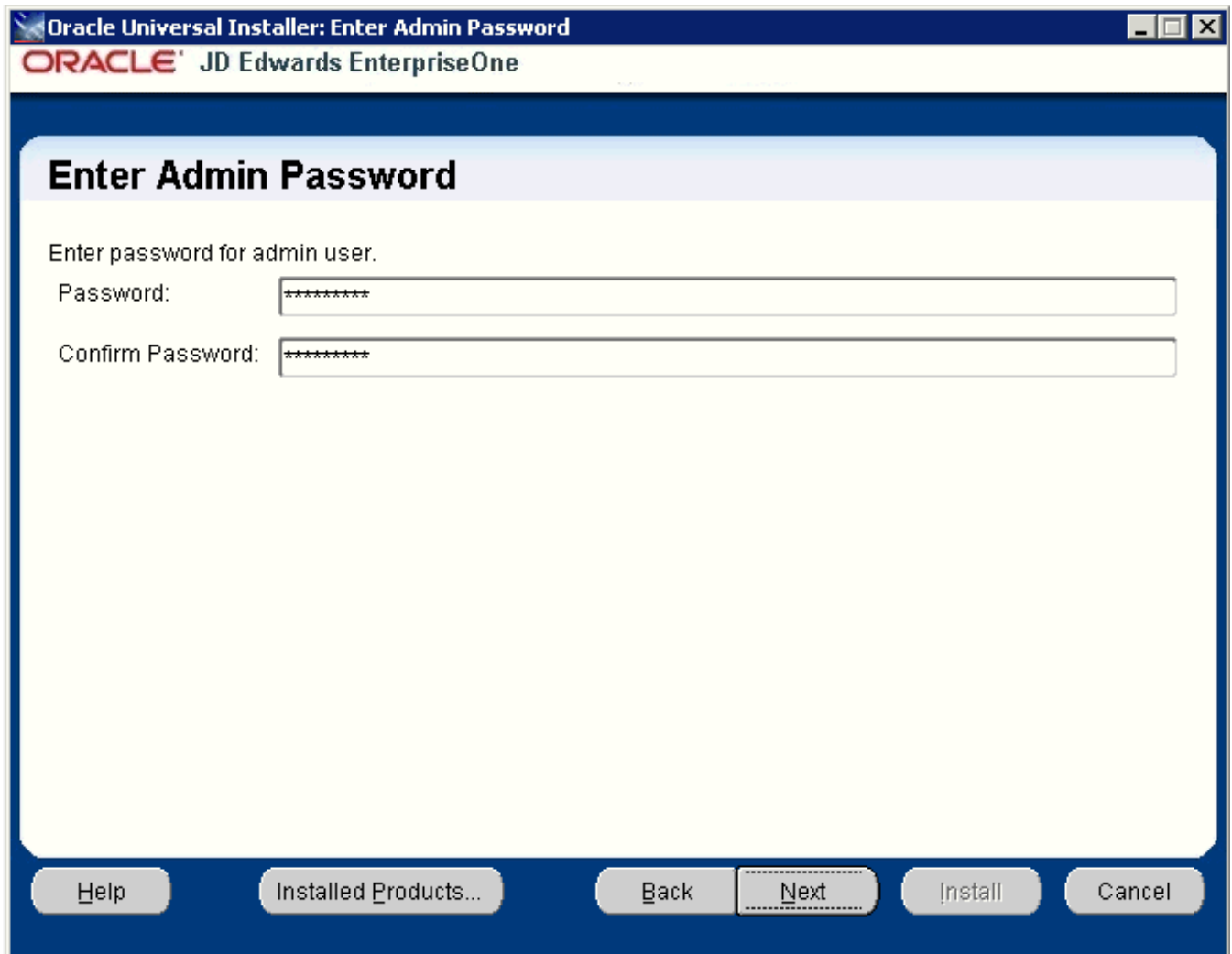
Enter the drive and directory where you want the files installed on your Management Console. The JD Edwards EnterpriseOne Management Console installer automatically detects the root drive location on the machine and by default appends this value:

jde_home

Note: Although jde_home is the default and recommended setting, you can specify any value to replace the default value. If there is an existing installation of the Management Console the default name will be appended with an underscore and a number. For example, JDE_HOME_1.

CAUTION: You cannot specify a directory that already exists.

6. Click the **Next** button.



7. On Enter Admin Password, enter and confirm the password for the jde_admin user.

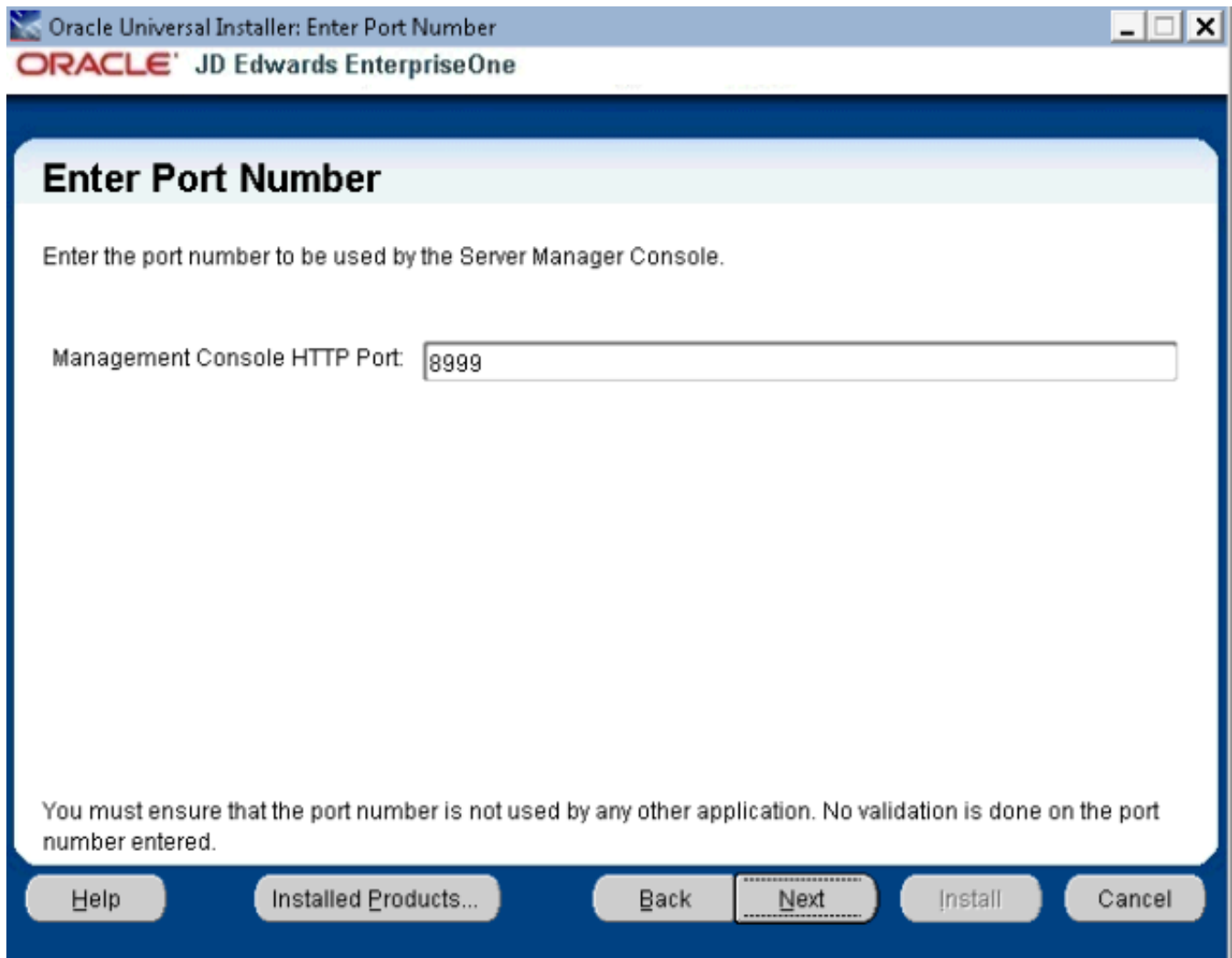
Note: The user name itself cannot be changed from jde_admin. The password must be at least eight (8) characters in length and cannot contain space or blank character values. Values are alphanumeric and these special characters: ! @ # \$ %. At least one (1) special character is required in the password.

Note: The default value for the user named jde_admin is automatically populated by the Management Console installer and cannot be altered. This is the administrative user account that is associated with the Management Console.

CAUTION: Because there is no programmatic way to retrieve a lost or forgotten password, it is critical that you remember and safeguard this password. If the password is forgotten or lost, the only recovery is a complete reinstallation of Server Manager. If you reinstall the Management Console and specify the JMX port the original installation was configured to use, you will retain all your managed homes and associated instances along with the configuration of those instances. However, you will lose this data:

- Console configuration, which includes database information entered using the Setup Wizard and information regarding security server(s) used to authenticate users.
- User Configuration, which are the added JD Edwards EnterpriseOne users and defined user groups, including their permissions.
- Server Groups and associated template configurations.
- Defined monitors and their associated monitor history.

8. Click the **Next** button.



9. On Enter Port Number, complete this field:

- o **Management Console HTTP Port**

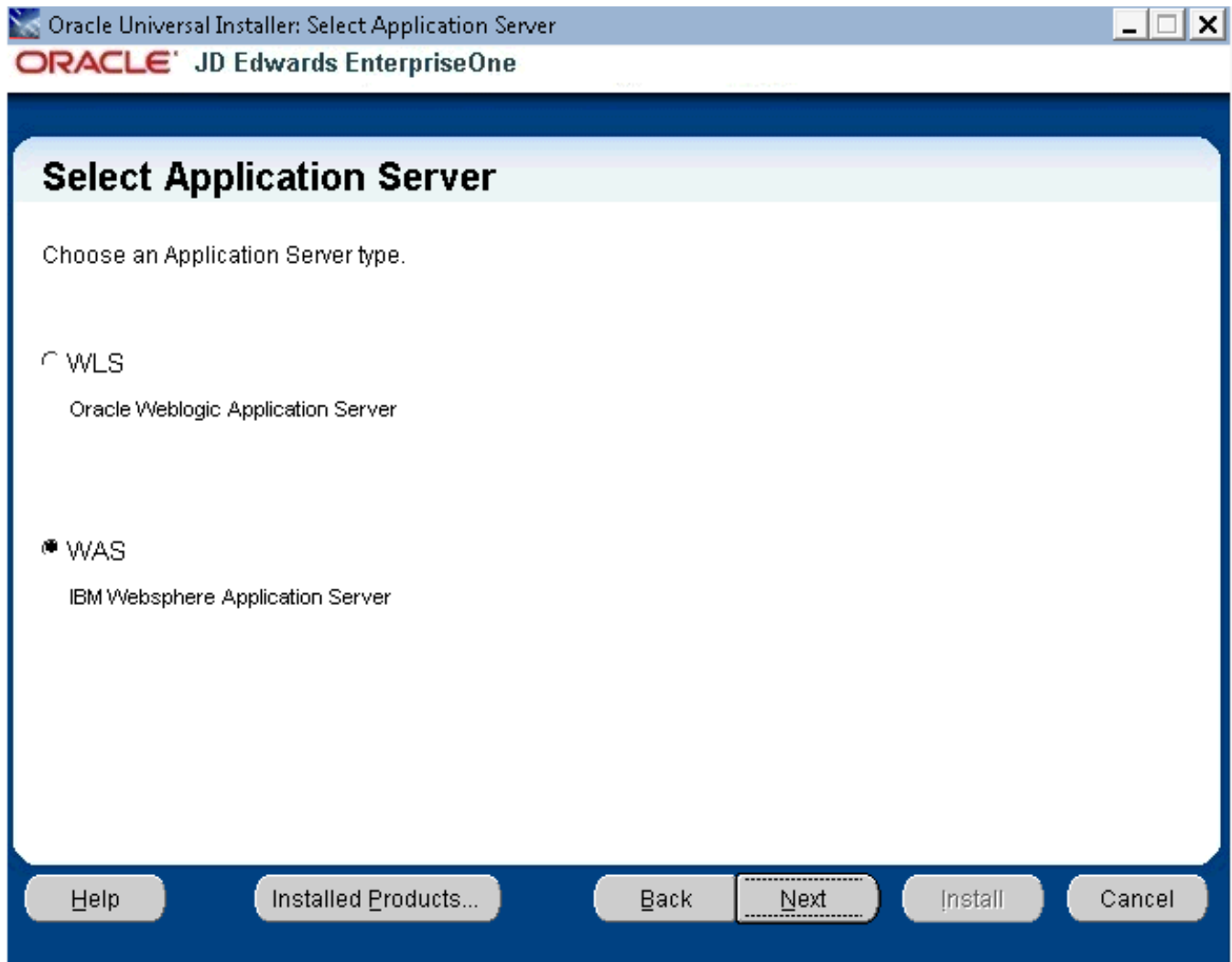
Enter valid unused port number for use by the Management Console.

The default value is 8999.

CAUTION: This port number must be available and cannot be in use by any other application on this machine. Since the installer cannot validate the port, you must be certain that these conditions are met or else the Management Console will not start.

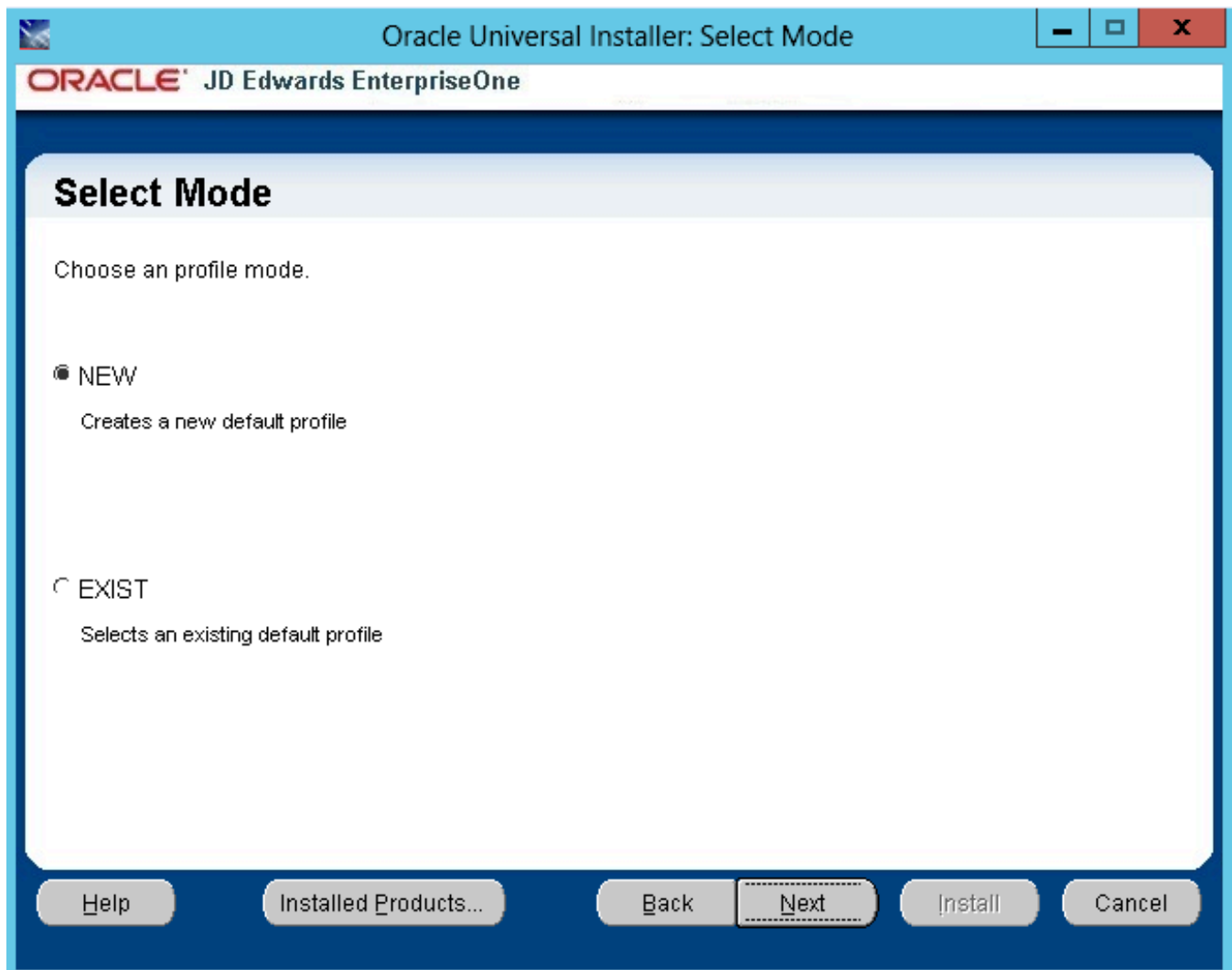
If there is insufficient disk space to complete the installation on the Management Console target machine, the installer displays an error message.

10. Click the **Next** button.



11. On Select Application Server, select the **WAS** radio button for the IBM WebSphere Application Server.

12. Click the **Next** button.

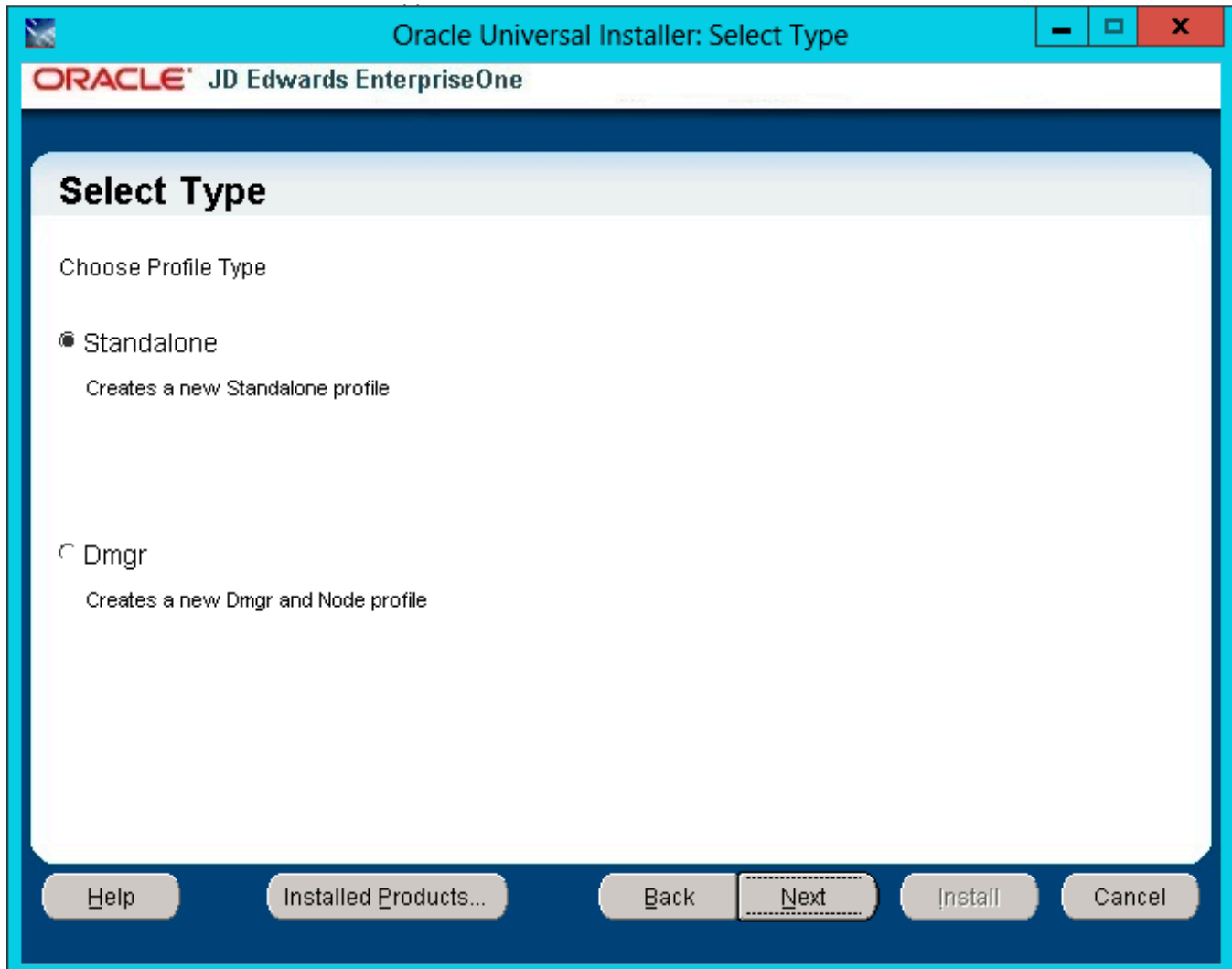


13. On Select Mode, select either:
 - o **NEW** - to create a new default profile.
 - o **EXIST** - to use an existing default profile.
14. Click the **Next** button.

15. The flow of screens will depend on which mode has been selected.

NEW

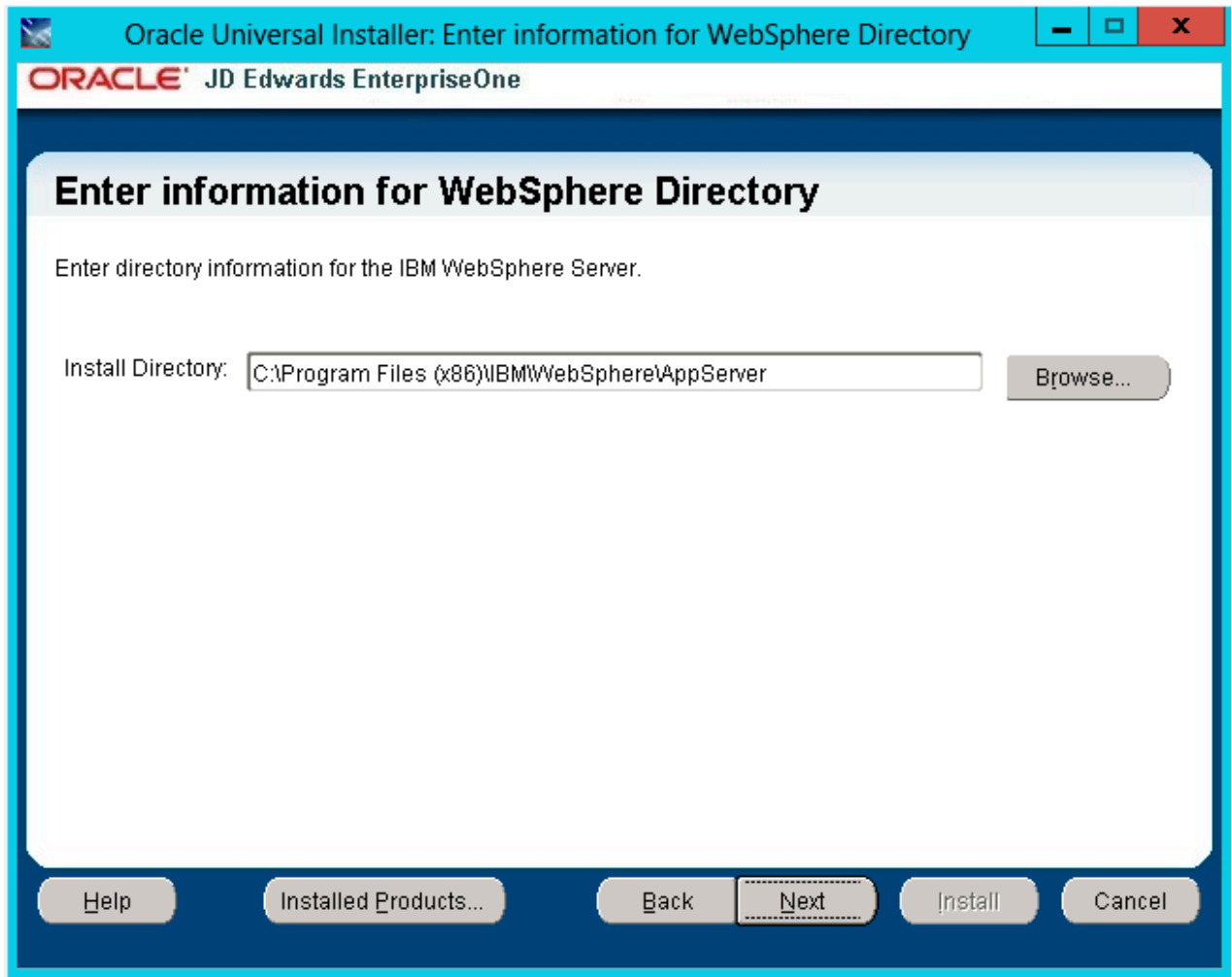
If New mode has been selected, you will first be prompted to select a Profile Type:



- a. On Select Type, select either:

Standalone - creates a new Standalone profile which will have an administration server.

- Dmgr** - creates a new Dmgr and Node profile. Dmgr will have a dmgr and a node. Dmgr will manage the administration work of the node.
- b. Click the **Next** button.



- c. On "Enter information for WebSphere Directory", if the Install Directory field is not automatically populated with the WebSphere folder path, then enter the WebSphere folder path.
- d. Click the **Next** button.

Oracle Universal Installer: Enter Admin UserID and Password information for ...

ORACLE JD Edwards EnterpriseOne

Enter Admin UserID and Password information for WebSphere

Enter Admin UserID and Password information for the IBM WebSphere Server Profile.

Admin User Name:

Admin User Password:

Help Installed Products... Back **Next** Install Cancel

- e. On the “Enter Admin UserID and Password Information for WebSphere” form, enter:

Admin User Name

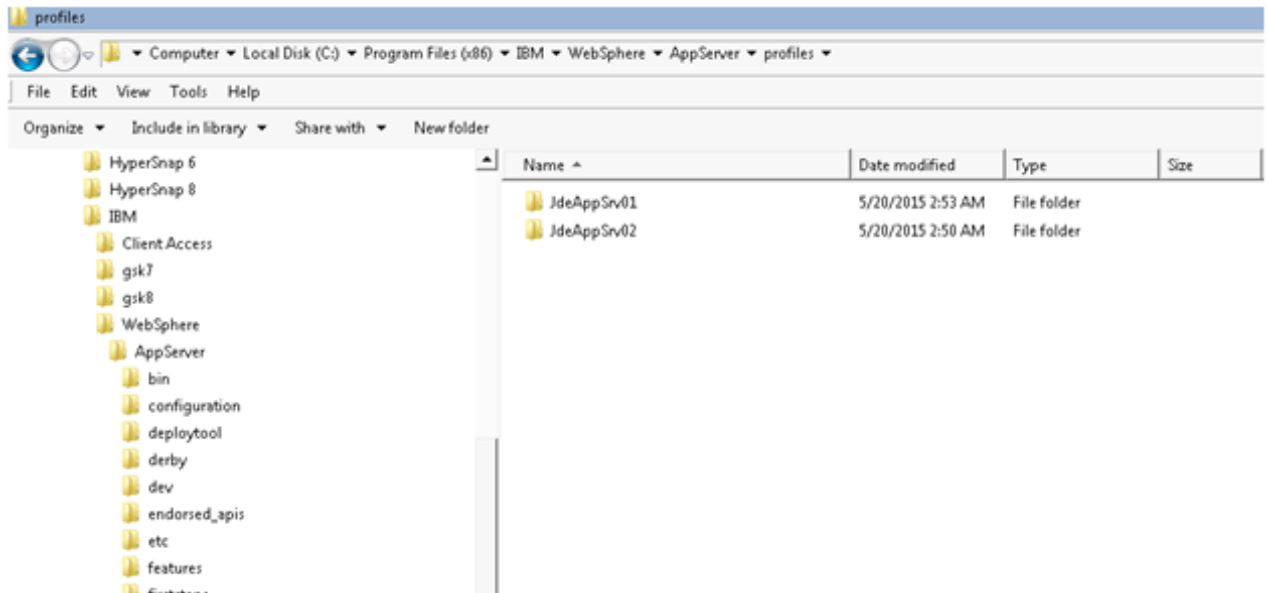
Enter the user name of the WebSphere admin account.

Admin User Password

Enter the password for the WebSphere admin account.

- f. Click the **Next** button.
- g. A Summary screen will be displayed. Proceed to Step 18 to continue.

Note that any created profiles will appear in the WAS profile directory below:



EXIST

If EXIST mode has been selected:

- a. Click the **Next** button.
- b. Proceed to step 16 to continue.

16. On Enter Information for WebLogic Server, complete the following fields:

- o *Install Directory*

Enter the path to the WebSphere installation directory (**AppServer**). For example:

```
C:\IBM\WebSphere\AppServer
```

- o *Host/IP*

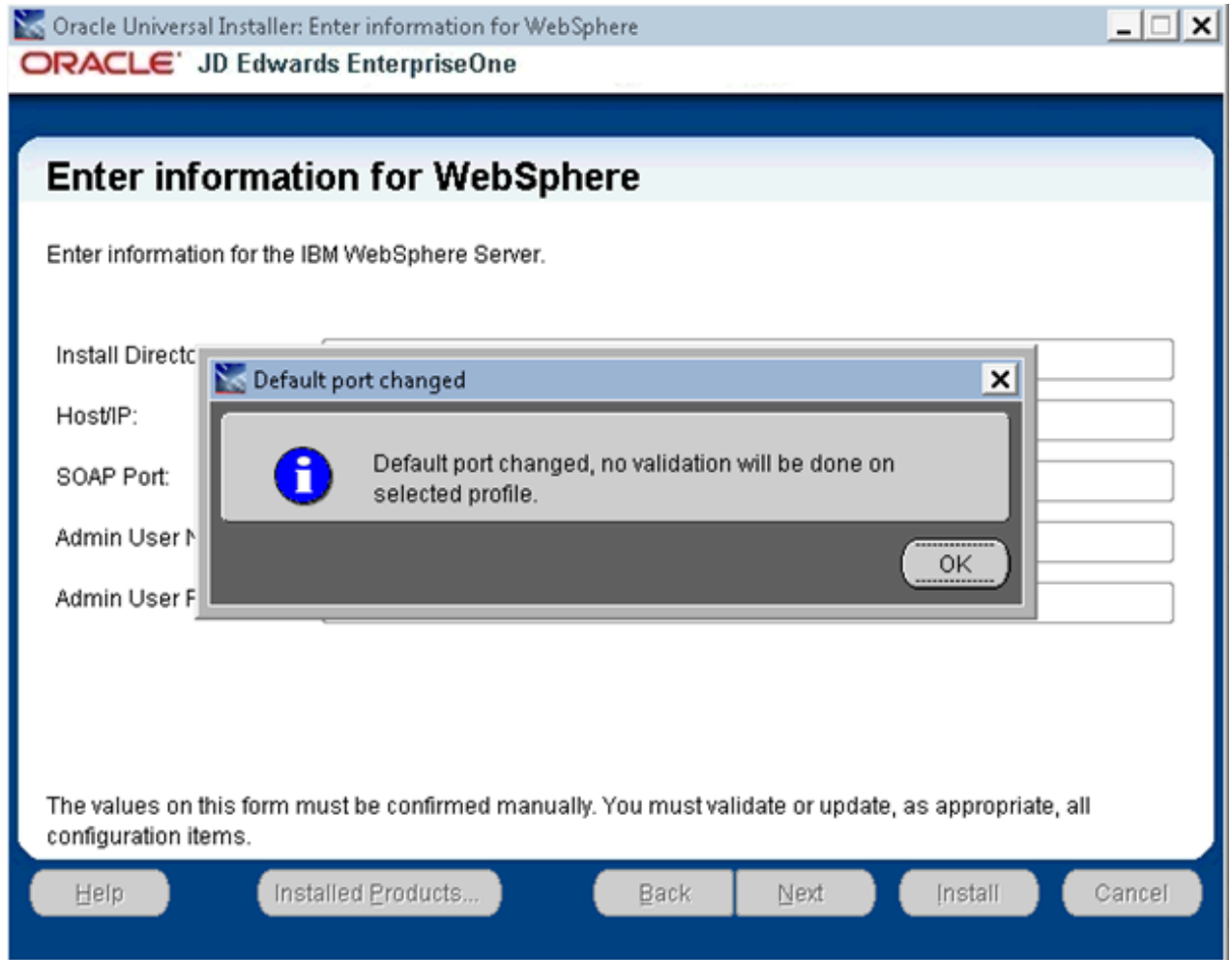
Enter the hostname or the IP Address at which the WebSphere server1 (or Deployment Manager) is listening for SOAP connections. This is usually the hostname/IP Address of the physical machine. For example:

```
<machine name>us.example.com
```

- o *SOAP Port*

Enter the port number on which the server1 (or Deployment Manager) is listening for SOAP Connections. For a particular profile, you can obtain this value from this location:

```
C:\IBM\WebSphere\AppServer\profiles\<profile_name>\logs>AboutThisProfile.txt
```



Sometimes, if the installer is not able to find the default profile path and the associated SOAP Port, it will display "<SOAP Port>", or if it finds a default soap port and the user changes it, the above error will be displayed. If "<SOAP Port>" is populated, that means that there is no default profile or that there is no

profile based on `c:\Program Files (x86)\IBM\WebSphere\AppServer\properties\profileRegistry.xml` file. A profile should be created in order to proceed.

- *Admin User Name*

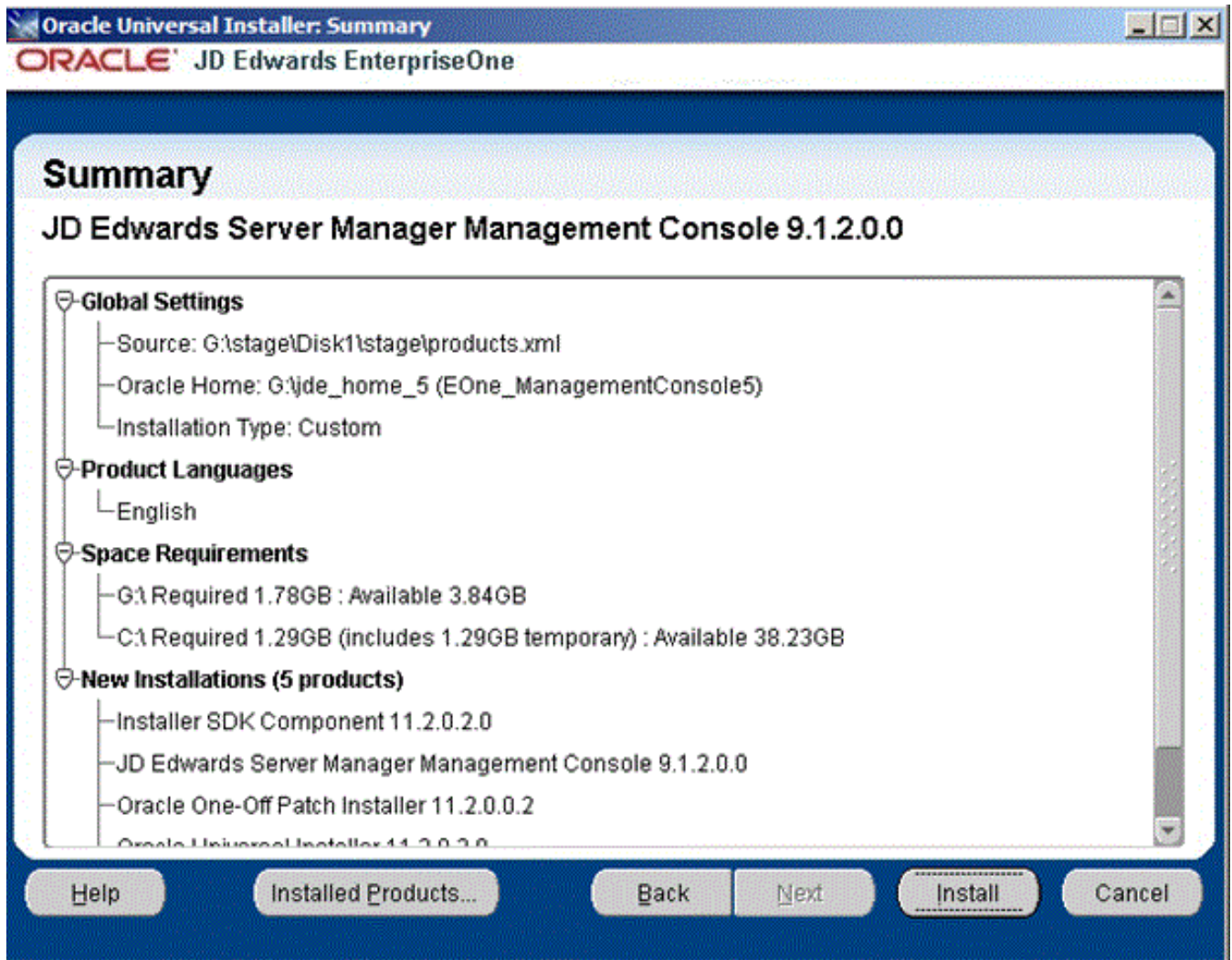
Enter the user name of the WebSphere admin account.

- *Admin User Password*

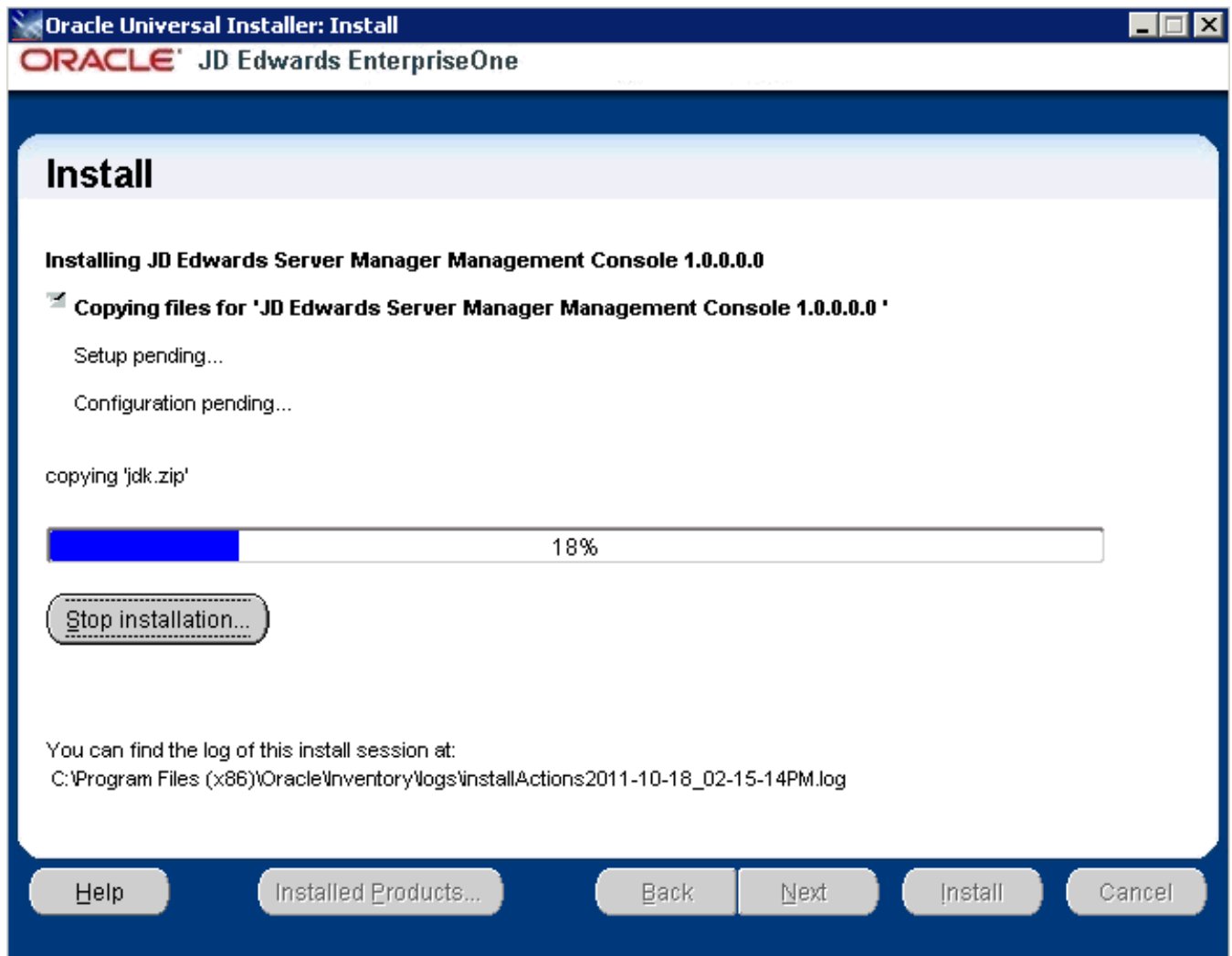
Enter the password for the WebSphere admin account.

CAUTION: The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items. If you enter invalid values, you will have to re-run the installer with the correct values.

17. Click the **Next** button.



18. On Summary, verify your selections and click the **Install** button to begin the installation.

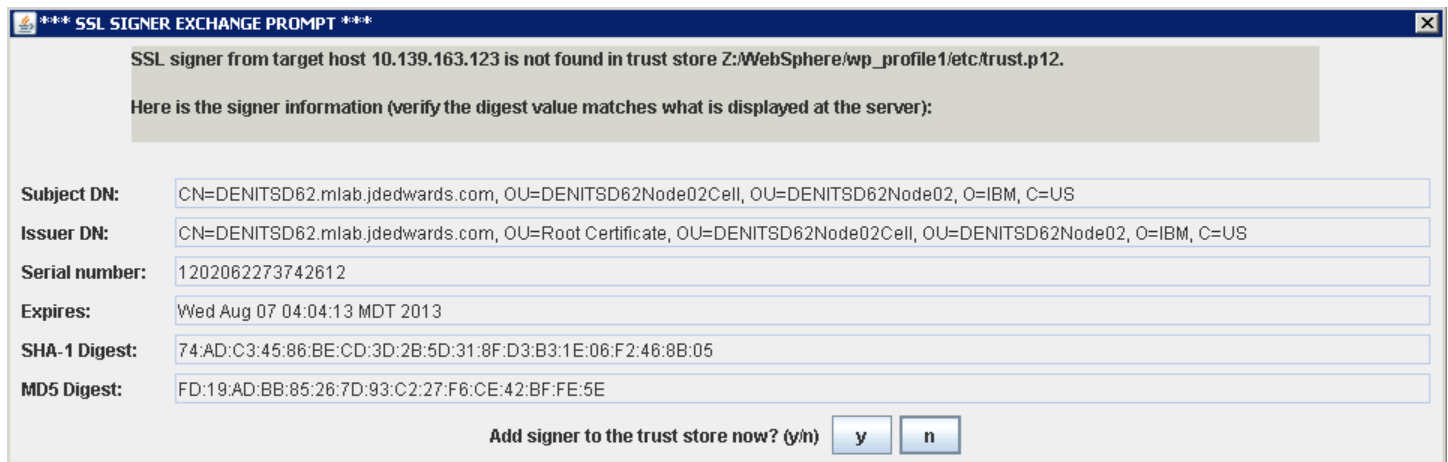


The Install progress screen is displayed. Note that this screen displays the location of the log of this installation. For example:

```
C:\Program Files (x86)\Oracle\Inventory\logs\installActions2011-10-18-02-15-14PM.log
```

Important: When installing the Server Manager Console on WebSphere on the Microsoft Windows platform with a non default profile (that is a profile which is not configured as a default profile during the profile creation time), the wsadmin scripting interface will prompt the administrator to add the signer to the default trust store.

In this case, the admin **must** select “y” option in order to proceed with the installation. If you select “n”, all wsadmin activities will fail. If the preceding conditions in this note are true, the below applet, entitled: “SSL Signer Exchange Prompt”, pops up during the installation process:



Troubleshooting Installations for WebSphere running on Microsoft Windows: If you do not select “y” on the above applet prompt entitled: “SSL Signer Exchange Prompt”, the Server Manager Console installation will fail. Such failure is indicated by the logs as shown in this example:

```
CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN
"CN=DENITSD62.mlab.jdedwards.com, OU=DENITSD62Node02Cell, OU=DENITSD62Node02,
O=IBM, C=US" was sent from target host:port "10.139.163.123:8881". The
signer may need to be added to local trust store "Z:/WebSphere/wp_profile1/
etc/trust.p12" located in SSL configuration alias "DefaultSSLSettings" loaded
from SSL configuration file "file:Z:\WebSphere\wp_profile1\properties/
ssl.client.props". The extended error message from the SSL handshake exception
is: "PKIX path building failed: java.security.cert.CertPathBuilderException:
PKIXCertPathBuilderImpl could not build a valid CertPath.; internal cause is:

java.security.cert.CertPathValidatorException: The certificate issued by
CN=DENITSD62.mlab.jdedwards.com, OU=Root Certificate, OU=DENITSD62Node02Cell,
OU=DENITSD62Node02, O=IBM, C=US is not trusted; internal cause is:

java.security.cert.CertPathValidatorException: Certificate chaining error".
CWPKI0040I: An SSL handshake failure occurred from a secure client. The server's
SSL signer has to be added to the client's trust store. A retrieveSigners utility
is provided to download signers from the server but requires administrative
permission. Check with your administrator to have this utility run to
setup the secure environment before running the client. Alternatively, the
com.ibm.ssl.enableSignerExchangePrompt can be enabled in ssl.client.props for
```

"DefaultSSLSettings" in order to allow acceptance of the signer during the connection attempt.

```
WASX7023E: Error creating "SOAP" connection to host
"DENITSD62.mlab.jdedwards.com"; exception information:
com.ibm.websphere.management.exception.ConnectorNotAvailableException:
[SOAPException: faultCode=SOAP-ENV:Client; msg=Error opening socket:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: PKIX path building
failed: java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl could
not build a valid CertPath.; internal cause is:

java.security.cert.CertPathValidatorException: The certificate issued by
CN=DENITSD62.mlab.jdedwards.com, OU=Root Certificate, OU=DENITSD62Node02Cell,
OU=DENITSD62Node02, O=IBM, C=US is not trusted; internal cause is:

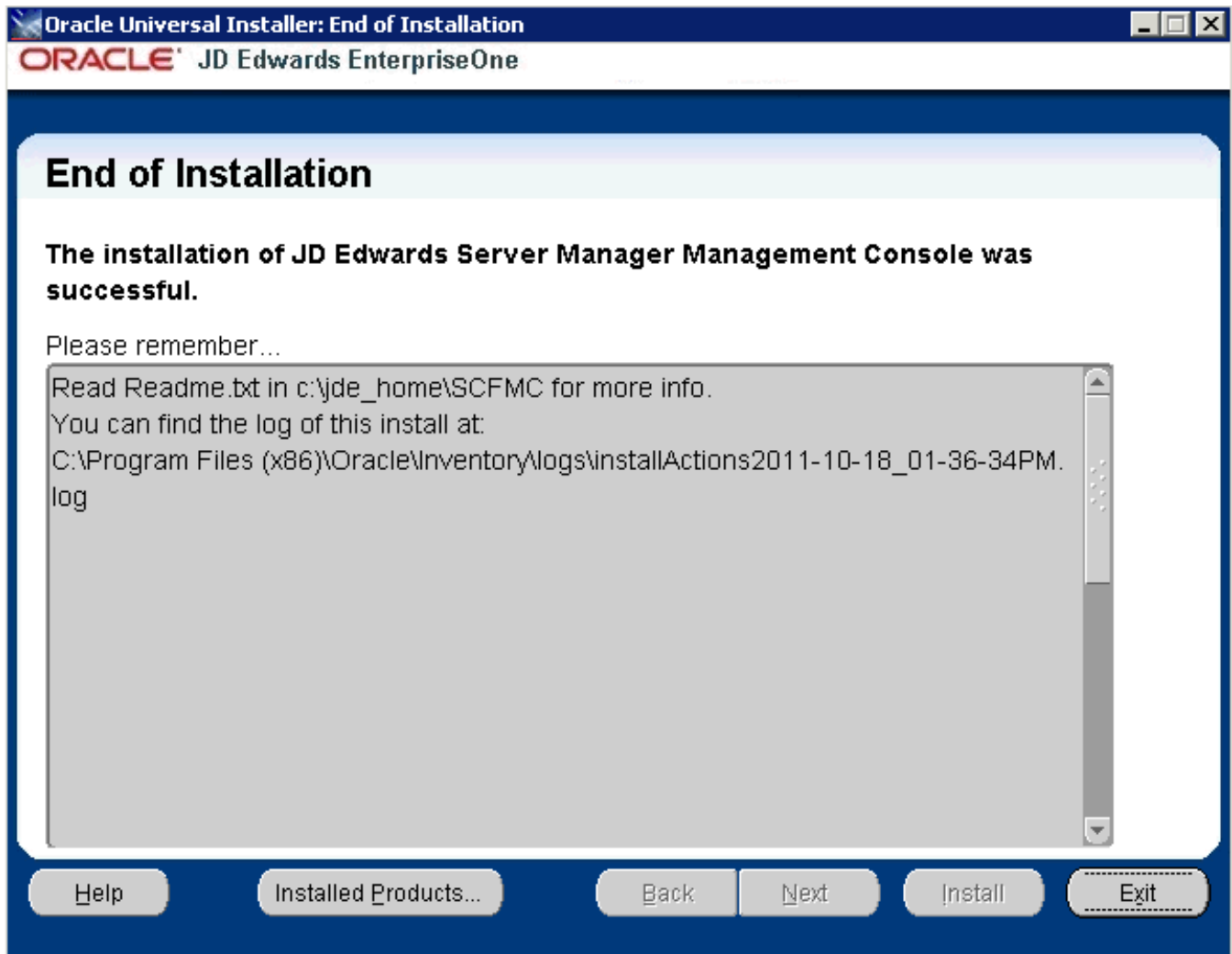
java.security.cert.CertPathValidatorException: Certificate chaining error;
targetException=java.lang.IllegalArgumentException: Error opening socket:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: PKIX path building
failed: java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl could
not build a valid CertPath.; internal cause is:

java.security.cert.CertPathValidatorException: The certificate issued by
CN=DENITSD62.mlab.jdedwards.com, OU=Root Certificate, OU=DENITSD62Node02Cell,
OU=DENITSD62Node02, O=IBM, C=US is not trusted; internal cause is:

java.security.cert.CertPathValidatorException: Certificate chaining error]
WASX7213I: This scripting client is not connected to a server process; please refer
to the log file Z:\WebSphere\wp_profile1\logs\wsadmin.traceout for additional
information.
```

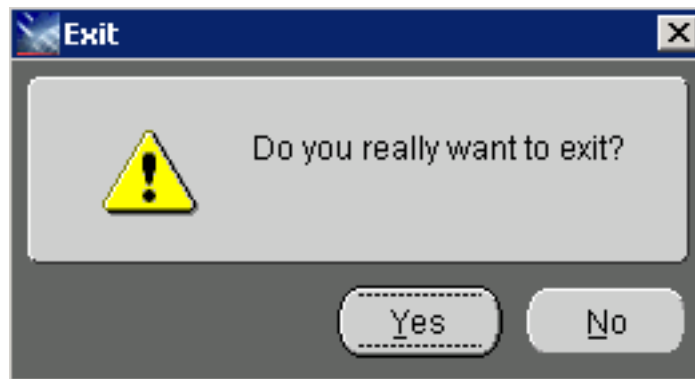
WASX8011W: AdminTask object is not available.

For all other installations using WebSphere on platforms other than Microsoft Windows, the following End of Installation screen is displayed.



19. On End of Installation, verify the installation was successful. The "Please remember ..." section also provides the installation log location.

20. Click **Exit** to exit the Oracle Universal Installer for the Server Manager Management Console.



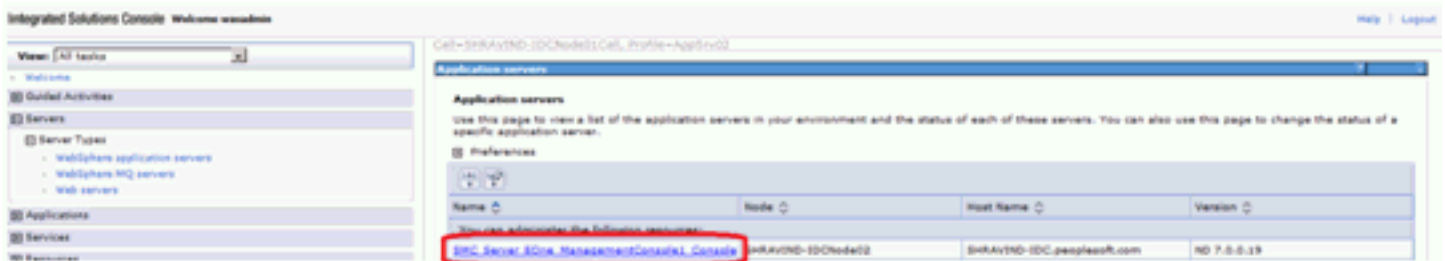
21. On the Exit dialog, click the **Yes** button.
22. The Administrator should refer to the `readme.txt` file in the provided in this directory:

`$ORACLE_HOME\SCFMC\`

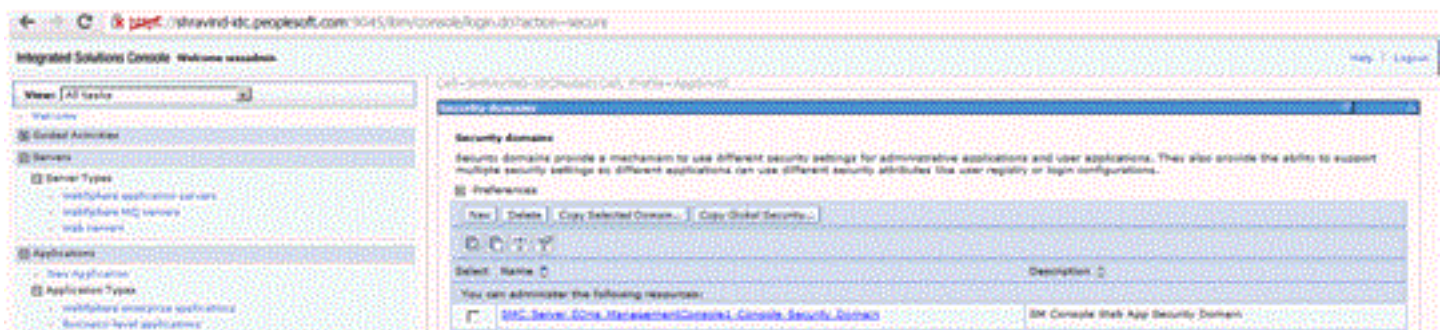
Verifying the Server Manager Console Installation on WebSphere Application Server

To verify the Server Manager Console installation on WebSphere Application Server:

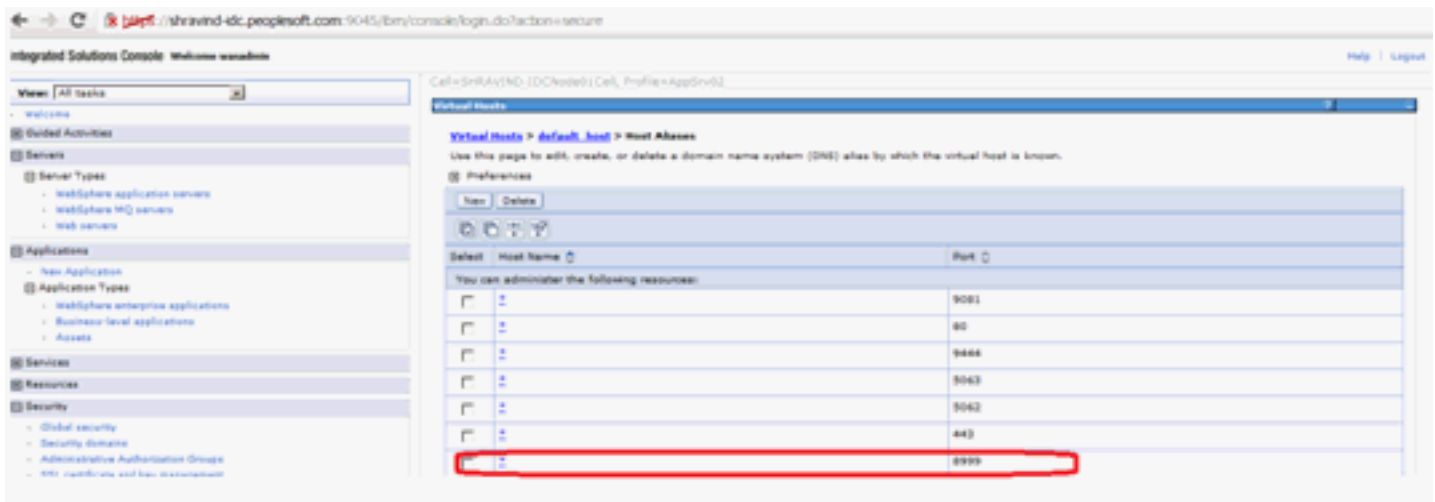
1. Login into the WebSphere Server Admin Console.
2. Go to Servers > Server Types > WebSphere Application Servers.
3. Verify a new J2EE Server is created for the Server Manager Console. The following screen shows an example.



4. Go to Security > Security Domains and verify that the Security Domain has been created. The following screen shows an example.



- Go to Virtual Hosts > default_host > Host Aliases and verify that there is a host alias entry created with the HTTP Port number that you specified during the installation of the Server Manager Console. The following screen shows an example.

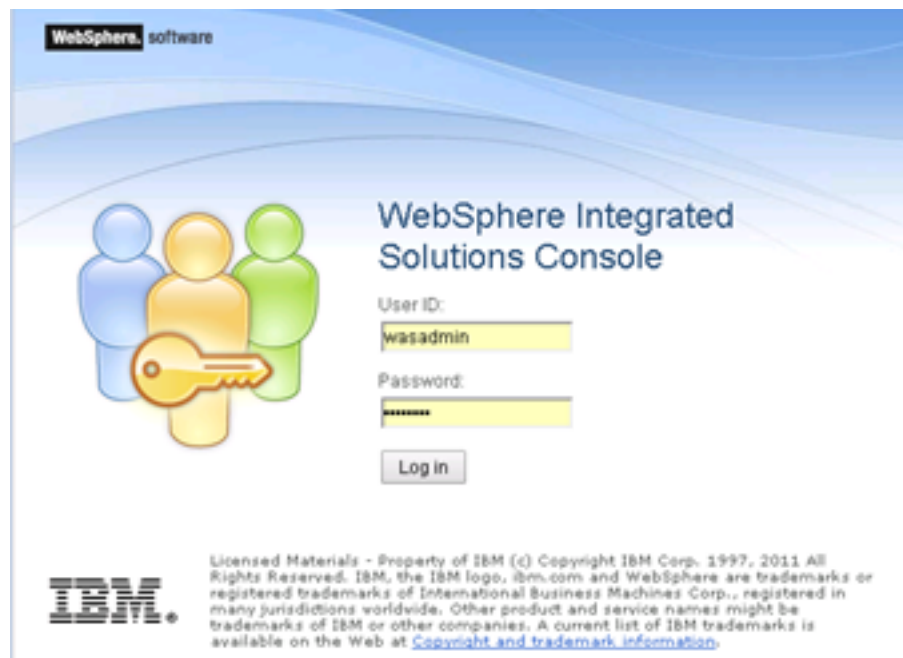


- Verify that the successful installation has automatically started the Server Manager Console.

Enable SSL for Server Manager Console on the WebSphere Application Server

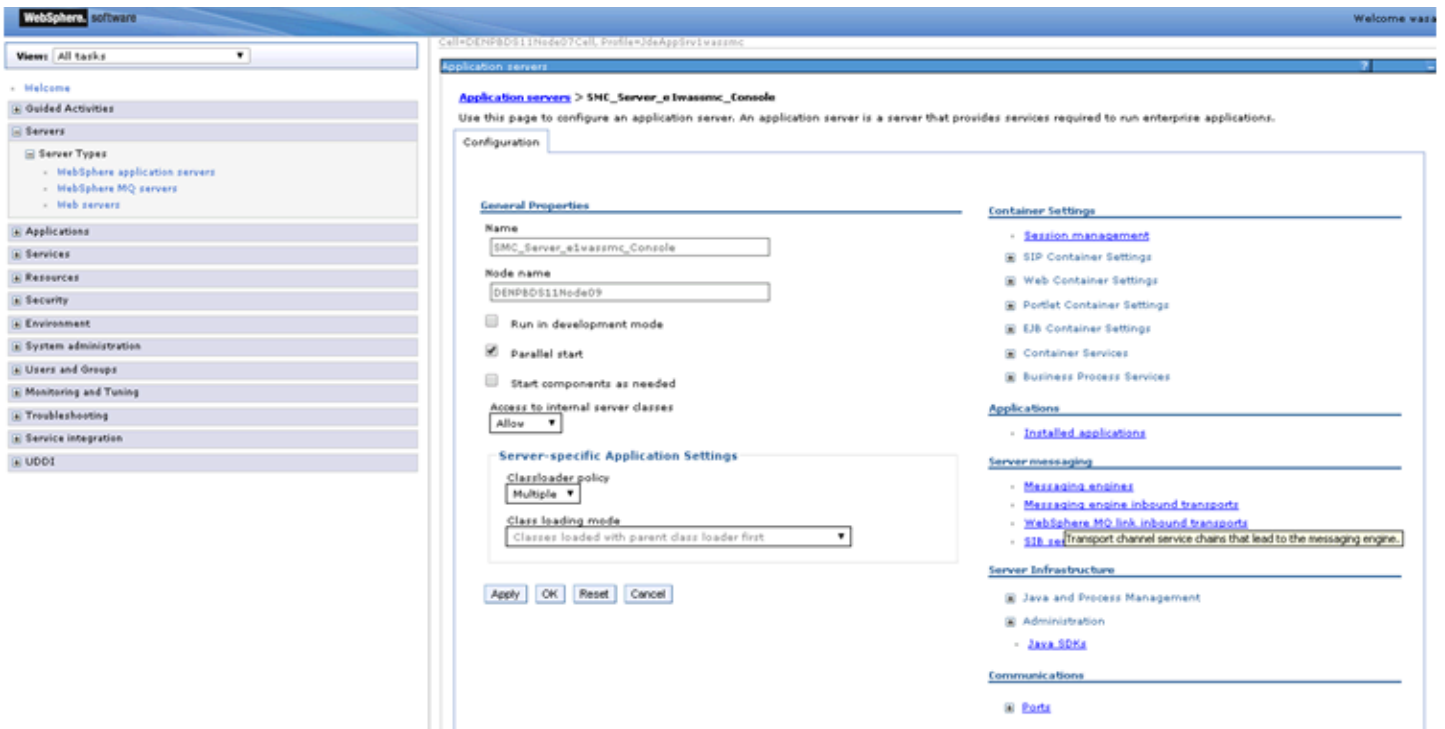
Note: The certificate and the keystore files that are used to configure the TLS settings with Server Manager Console must be used for configuring the SSL setting as well.

- Access the WebSphere Admin Console in the browser for the profile in which the Server Manager Console is installed. A sample URL would be: `https://denpbds11.example.com:9146/ibm/console`



- Login to the WebSphere Admin Console using the WebSphere Administrative credentials.
- Navigate to Servers -> Server Types -> WebSphere Application Servers.

- Click on the Server Manager Console J2ee server (in the example below it is the SMC_Server_e1wasmc_Console).



- Expand the Ports tab on the lower right hand side and write down the WC_defaulthost_secure port number. This is the port which we will use to access the Server Manager Console over HTTPS/SSL. In this example, the WC_defaulthost is the port number over which we will access Server Manager over HTTP.

- In this example the WC_defaulthost_secure parameter is set to 9519 while the WC_defaulthost is set to 8999.

Communications

Ports

Port Name	Port	Details
BOOTSTRAP_ADDRESS	2838	
SOAP_CONNECTOR_ADDRESS	8909	
ORB_LISTENER_ADDRESS	9150	
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS	9516	
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS	9517	
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS	9518	
WC_adminhost	9151	
WC_defaulthost	8999	
DCS_UNICAST_ADDRESS	9383	
WC_adminhost_secure	9153	
WC_defaulthost_secure	9519	
SIP_DEFAULTHOST	5114	
SIP_DEFAULTHOST_SECURE	5115	
OVERLAY_UDP_LISTENER_ADDRESS	11045	
OVERLAY_TCP_LISTENER_ADDRESS	11046	
IPC_CONNECTOR_ADDRESS	9657	
SIB_ENDPOINT_ADDRESS	7332	
SIB_ENDPOINT_SECURE_ADDRESS	7333	
SIB_MQ_ENDPOINT_ADDRESS	5612	
SIB_MQ_ENDPOINT_SECURE_ADDRESS	5613	

- Next, navigate to Environment -> Virtual hosts -> default_host -> Host Aliases.
- Select **New** and add a host alias with Host Name set to * and the Port set to the entry noted for WC_defaulthost_secure (in this example it is 9519).

9. Click **OK**.
10. Click **Save**.
11. Restart the Server Manager Console J2ee container (in this example, SMC_Server_e1wassmc_Console) from the command prompt using these commands:

```
Z:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\JdeAppSrv1wassmc\bin>stopServer.bat
SMC_Server_e1wassmc_Console
```

```
Z:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\JdeAppSrv1wassmc\bin>startServer.bat
SMC_Server_e1wassmc_Console
```

12. Next, access the Server Manager Console in the browser using an HTTPS/SSL based URL (`https://<Server_Manager_Console_HostName>:<WC_defaulthost_secure_port>/manage/home`). In this example the URL is: `https://denpbds11.example.com:9519/manage/home`



13. Go to *Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore* and perform the steps.

Import the Server Manager Console Certificate into All Java Installations That Are Used by Embedded Agents

You **must** also import the Server Manager Console certificate into all Java installations that are used by embedded agents to communicate with the Server Manager Console. For instructions, refer to the following sections of this guide:

- *Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore*
- *Import the Server Manager Console Certificate into All Java Installations That Are Used by Embedded Agents*

Troubleshooting the Server Manager Console Installation on WebSphere Application Server

To troubleshoot the Server Manager Console installation on WebSphere Application Server:

1. Locate and inspect the contents of the `.out` and `.err` log files located in these directories:

Microsoft Windows

```
C:\<Server_Manager_Console_Home>\SCFMC\data
```

where `<Server_Manager_Console_Home>` is the Server Manager Console installation directory. For example:

```
C:\jde_home_1\SCFMC\data
```

2. Locate and inspect the contents of the Server Manager Console installer-related log files for errors. These logs are typically located in following locations:

Note: The location of these logs and the log file name are displayed on in the lower portion of the installer screens during the installation process.

Microsoft Windows

`C:\Program Files (x86)\Oracle\Inventory\logs`

Linux or Solaris

`/u01/app/oracle/oraInventory/logs`

3. Locate and inspect the contents of the application server log files for errors. These logs are typically located in following locations:

`C:\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\logs`

`C:\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\SMC_Server_###\logs`

`C:\IBM\WebSphere\AppServer\profiles\DMGR01\logs\dmgr\logs`

`C:\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\ffdc`

Please note the following bug numbers and special instructions with regard to the Server Manager Console installed on WebSphere:

BUG 14369731 - FOR SMC ON WAS 8.5 MANAGEMENT AGENTS SHOWING STOPPED IN HOME PAGE AFTER LOGIN

Issue/ Resolution:

This issue is specifically for a Server Manager Console installed on WAS 8.5 (typically not applicable to Server Manager Console on WAS 7.x). The issue is caused because the JMX ports being used by the Server Manager Console (14501/14502 by default) are not freed during the self-update process and as a result, when the Server Manager Console application is updated and starts up it is unable to bind to the same JMX ports. Thus, the Server Manager Console now binds to the next free set of ports available. Because the Server Manager Agents connected to the Server Manager Console are not aware of this, they still attempt to connect to the old Server Manager Console port (14501 by default). As a result they show a status of stopped as the Server Manager Console and Server Manager Agents are not able to communicate. This is being investigated as to whether this is an EnterpriseOne Server Manager bug or a IBM WebSphere issue.

The resolution is to restart the Server Manager Console J2EE server after the self-update using these steps:

1. Stop the Server Manager Console WAS J2EE container using:

`Z:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\stopServer.bat <server_name>`

2. Start the Server Manager Console J2EE server from the command line using:

`Z:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\startServer.bat <server_name>`

After applying these steps the Server Manager Agents connected to the Server Manager Console should show the correct statuses.

Troubleshooting the Tools Build Promotion Failing Error

If you see the following exception in the Server Manager Console J2EE container log while performing the self-update operation:

```

Jun 01, 2018 2:37:48 PM GenericConnectorServer ClientCreation.run
WARNING: Failed to open connection: javax.net.ssl.SSLHandshakeException:
Received fatal alert: handshake_failure
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.Alerts.getSSLException(Alerts.java:154)
...
<Jun 1, 2018 2:37:48,083 PM UTC> <Warning> <javax.management.remote.generic>
<BEA-000000> <Failed to open connection: javax.net.ssl.SSLHandshakeException:
Received fatal alert: handshake_failure
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.Alerts.getSSLException(Alerts.java:154)
...
Truncated. see log file for complete stacktrace
>
Jun 01, 2018 2:37:48 PM com.jdedwards.mgmt.targets.mgmtconsole.ManagementConsole
changeComponentWithUserName WARNING: Unable to change the management console tools
release; unable to
perform remote authentication with wls admin server
<Jun 1, 2018 2:37:48,086 PM UTC> <Warning>
<com.jdedwards.mgmt.targets.mgmtconsole.ManagementConsole> <BEA-000000>
<Unable to change the management console tools release; unable to perform
remote authentication with wls admin server>
Jun 01, 2018 2:37:48 PM org.apache.commons.modeler.BaseModelMBean invoke
SEVERE: Exception invoking method changeComponentWithUserName
  
```

Use the following procedure to resolve the issue and to update the Server Manager Console to the Tools release 9.2.2.6 (or higher):

1. Download the Server Manager Console for Tools update for release 9.2.2.6 from the Update Center.
2. Extract the ManagementLoginModule_JAR.jar file from the par file.
3. Stop the Server Manager Console and the Admin Server (and any other running Managed Servers) from the Weblogic Domain on which the Server Manager Console is being installed.
4. Overwrite the X:\\$MIDDLEWARE_HOME\user_projects\domains\base_domain\lib directory file with the extracted ManagementLoginModule_JAR.jar file.
5. Start the Admin Server and the Server Manager Console (and other Managed Servers if required).

For more information, see [BUG 28122456 - SERVER MANAGER ON 9.2.2.5 BUILD - TOOLS PROMOTION IS FAILING](#)

Note: Customers who perform fresh installations of the Server Manager Console from Tools release 9.2.2.6 (or higher) will not run into this issue since the ManagementLoginModule_JAR.jar file containing the fix will be copied to X:\\$MIDDLEWARE_HOME\user_projects\domains\base_domain\lib directory

Troubleshoot the Management Console Installation

Note: Starting with JD Edwards EnterpriseOne Tools Release 9.2.4.3, there is no support for connecting to Server Manager Console and Server Manager Agent(s) using jconsole, any other JMX Client, or using a Java Debugger.

This section discusses these topics:

- [Installer Fails to Complete](#)

- *Management Console Will Not Start*
- *Management Console Will Not Save Configuration Settings*

Installer Fails to Complete

If the Management Console installer fails to complete, an exception screen is displayed. For details, examine the log file located in the `oracle\Inventory\logs` directory.

Tip:

The log file location is displayed on the End of Installation screen for the Management Console installer. Refer to the section of this guide entitled: *Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools*.

For example, the complete path and log file name might be:

```
C:\Program Files (x86)\Oracle\Inventory\logs\installActions2011-10-18-02-15-14PM.log
```

Management Console Will Not Start

The HTTP port number must be available and cannot be in use by any other application on this machine. Since the installer cannot validate the port, you must be certain that these conditions are met or else the *Management Console* will not start.

Management Console Will Not Save Configuration Settings

If the *Management Console* generates an error when you try to save configuration settings, verify that the JMX port that the *Management Console* is using is not being used by another application. To view what port is currently set as the JMX port and to change it, use the *Management Agent Port Assignments* section on the *Management Agents* page of the *Management Console*.

For example:

The screenshot shows a configuration window titled "Management Agent Port Assignments". It contains a text box for "Management Server JMX Port" with the value "15501" and a text box for "Management Agent Starting Port" with the value "15502". There is a "Save" button at the bottom right. Below the form, there are two informational messages with checkmarks:

- ✓ Modification of the management server JMX port should be performed prior to installing any managed agents. Changing the port while there are deployed management agents will cause unpredictable and undesirable results.
- ✓ Remote agents currently connected to the management console will not be affected by changes to the agent starting port. New connections to the management console will utilize the changed value.

Accessing a Secure Profile from Server Manager

There is now an option to either use the existing **DummyClientTrustFile.jks** and **DummyClientKeyFile.jks** files or use a custom **TrustStore** and **KeyStore** file which is more secure and is recommended by IBM. Prior to the JD Edwards EnterpriseOne 9.2 Tools Release, Server Manager always used DummyClientTrustFile.jks and DummyClientKeyFile.jks, which were located in the respective profile `WASInstall>/AppServer/profiles/<profile>/etc` location.

Using the Existing DummyClientTrustFile.jks and DummyClientKeyFile.jks files

When you are registering a brand new WAS Instance from the Server Manager Console, you can keep the TrustStore File, TrustStore File Password, KeyStore File, and KeyStore File Password as blank.

The screenshot shows a registration wizard with four steps: Instance Type, Instance Properties (active), Confirmation, and Finish. The 'Instance Properties' section contains several input fields. A red rectangular box highlights the following fields: 'TrustStore File', 'TrustStore File Password', 'KeyStore File', and 'KeyStore File Password'. The other fields, 'Instance Name' and 'Application Server Install Location', are visible but not highlighted.

If you have already registered a WAS Instance and would like to use the default DummyClientTrustFile.jks and DummyClientKeyFile.jks files from the `<profile>/etc` folder like the pre 9.2 Tools Release, then you will need to:

1. Open the registered WAS instance page.
2. In the **Instance Properties** section (top right), blank out or clear the **TrustStore File** and **KeyStore File** fields.
3. Click the **Save** button next to these fields.

The screenshot shows the 'IBM WebSphere' console with two tabs: 'General' and 'Instance Properties'. The 'Instance Properties' tab is active. It shows fields for 'Application Server Install Location', 'Instance Name', 'TrustStore File', 'TrustStore File Password', 'KeyStore File', and 'KeyStore File Password'. A red rectangular box highlights the 'TrustStore File' and 'KeyStore File' fields, which contain the paths 'C:\temp\wastrust.jks' and 'C:\temp\waskey.jks' respectively. Each of these fields has a 'Save' button next to it.

4. Restart the Server Manager Agent.

Server Manager will now start using the default DummyClientTrustFile.jks and DummyClientKeyFile.jks files from the `<WASInstall>/AppServer/profiles/<profile>/etc` folder, as it would in the pre 9.2 Server Manager.

Using a Custom TrustStore and KeyStore File

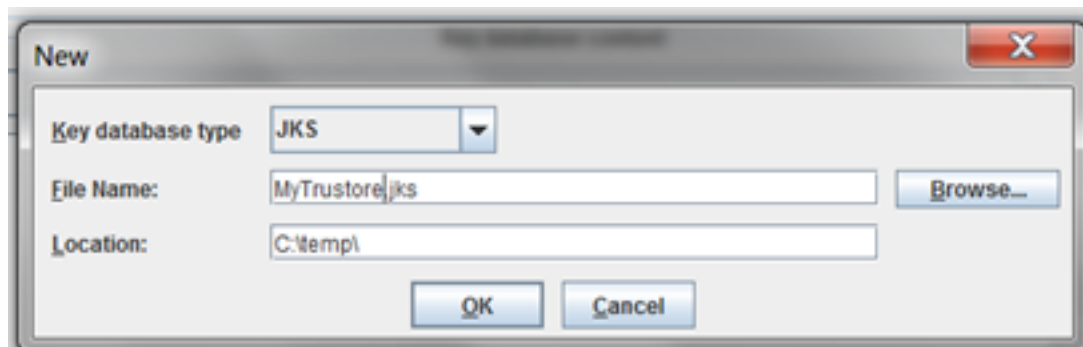
Before we proceed further, it is assumed that a secure profile has already been created and the required changes have been made to the **soap.client.props** file. We also assume that you have the IBM IKEYMAN GUI based utility available. The IKEYMAN utility is installed by default when you install IBM Websphere or IBM HTTPServer.

Note: Server Manager supports only one set of TrustStore and KeyStore files for the whole WAS Instance. So, if you have multiple Secure Profiles created, you will need to import the TrustStore and KeyStore certificates from each of these profiles to one single TrustStore and KeyStore file.

Importing the TrustStore Certificate

To import a TrustStore certificate:

1. Start the IKEYMAN GUI utility.
2. Create a new TrustStore Database File by selecting **Key Database File**, and then select **New**.
3. In the new dialog box select:
 - o **Key database type** = JKS
 - o **Filename** = give any name
 - o **Location** = any location where the new Key Database file will be generated.
4. Click **OK**. The password dialog box will popup.



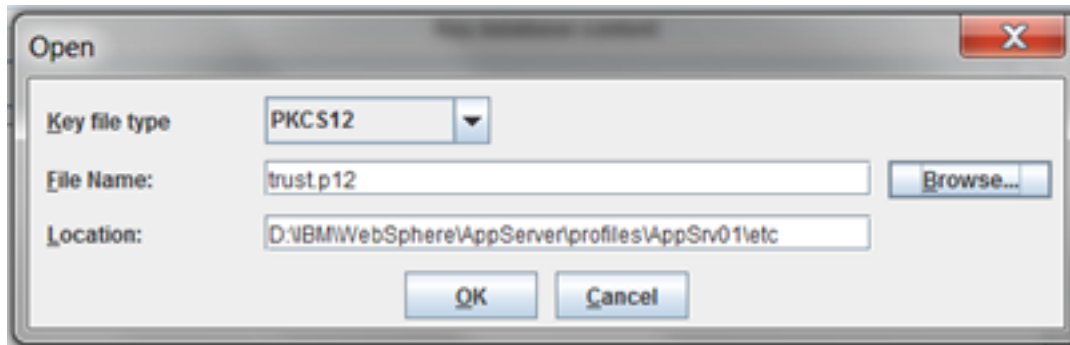
5. In the password dialog box, provide a password for the TrustStore database file that is being created and click **OK**.

Note: Be sure to write down this password to have it available to provide to the Server Manager Console later when configuring the TrustStore and KeyStore Files for the secure profile.

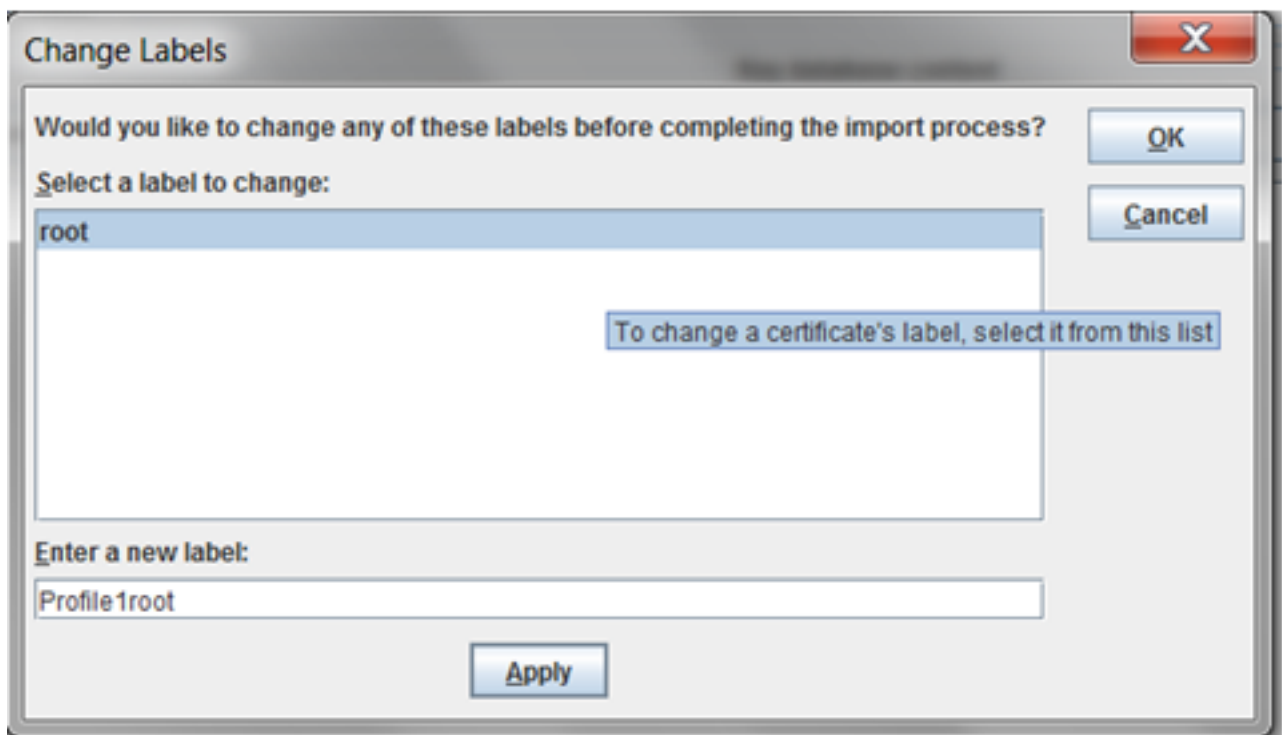
Now we will import the TrustStore file from the WAS Secure Profile location. To import the TrustStore file:

1. Click **Import** to bring up the **Open** dialog box to import the trust.p12 file from the WAS Secure Profile's etc folder.
2. In the **Key file type** field, select **PKCS12**.

3. For the **File Name** field, click **Browse** and select the **trust.p12** file from your <WASInstall>/AppServer/profiles/<profile>/etc folder.

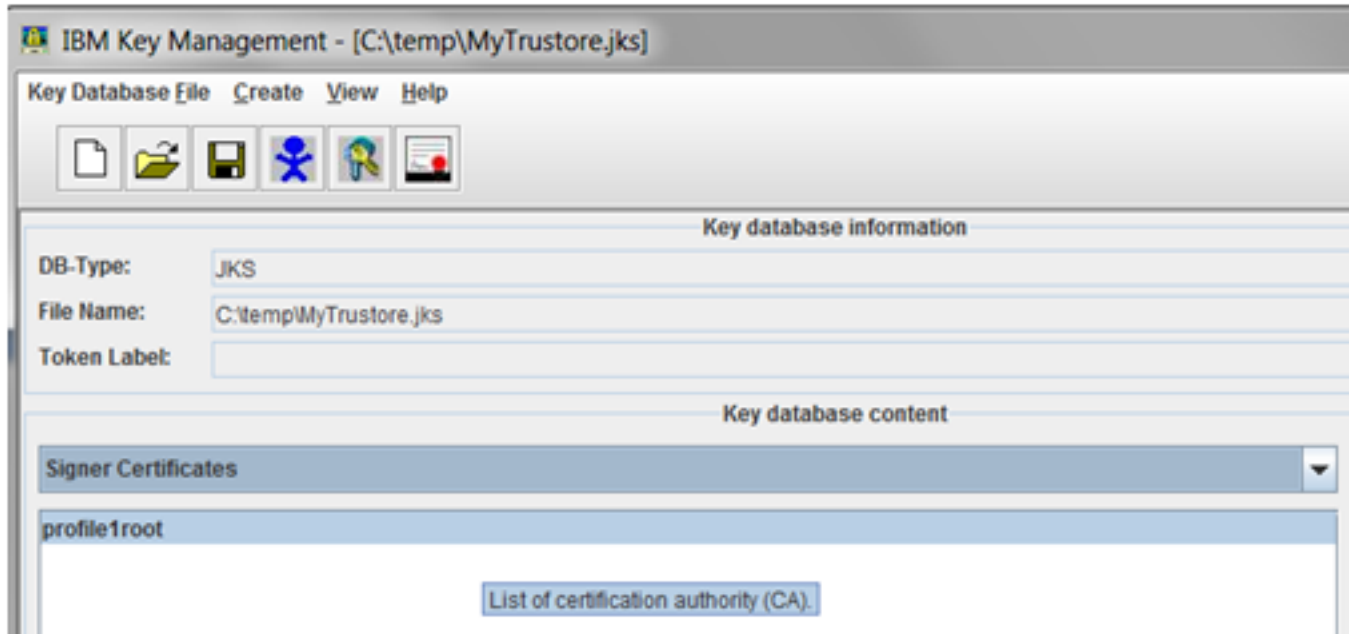


4. Click **OK**.
5. When prompted for a password, use **WebAS**, which is the default password for all of the profile's TrustStore and KeyStore files.
6. Click **OK**. This will bring up the **Change Labels** dialog box.
7. Select **root** from **Select a label to change**, and enter a new label name like **Profile1root** to make sure every certificate that is imported from different profiles has a unique name associated with it.



8. Click **Apply**.
9. Click **OK** to save.

The TrustStore that you have imported in the above steps will now be listed under the IKEYMAN **Signer Certificates**.



If you do not see the imported certificates under the **Signer Certificates** section, then the import did not work and you need to redo these steps for *Importing the TrustStore Certificate* from the beginning.

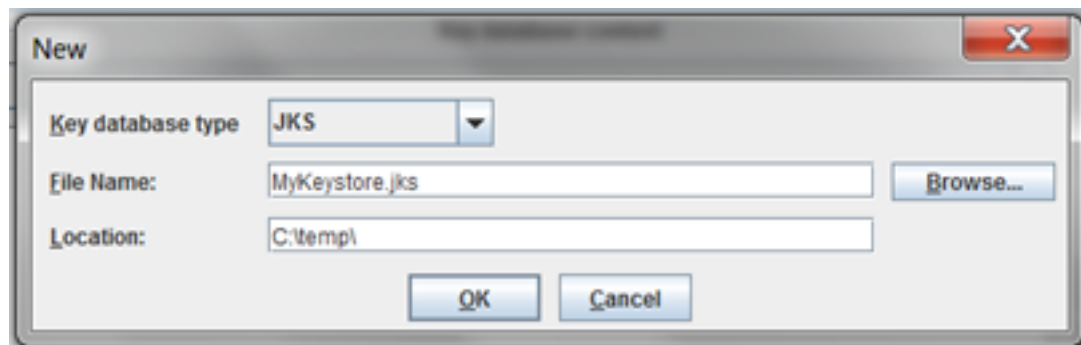
If you are using multiple Secure Profiles, you will need to import the TrustStore keys from each of these profiles to the same JKS database file. The instructions remain the same.

Close the newly created TrustStore Database by selecting **Key Database File**, and then select **Close**.

Importing the KeyStore Certificate

We will now create a KeyStore File and will import the KeyStore from the WAS Secure Profile. To import the KeyStore Certificate:

1. Create a new KeyStore Database File by selecting **Key Database File**, and then select **New**.
2. In the new dialog box select:
 - o **Key database type** = JKS
 - o **Filename** = give any name
 - o **Location** = any location where the new Key Database file will be generated.
3. Click **OK**. The password dialog box will popup.

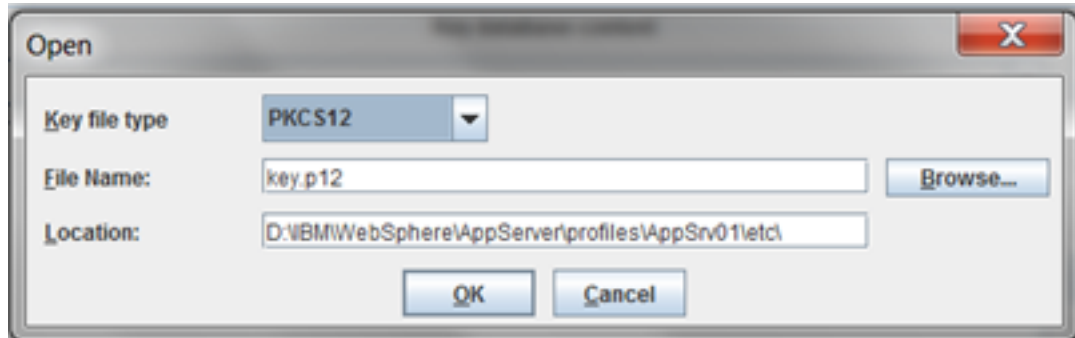


In the password dialog box, provide a password for the KeyStore database file that is being created and click **OK**.

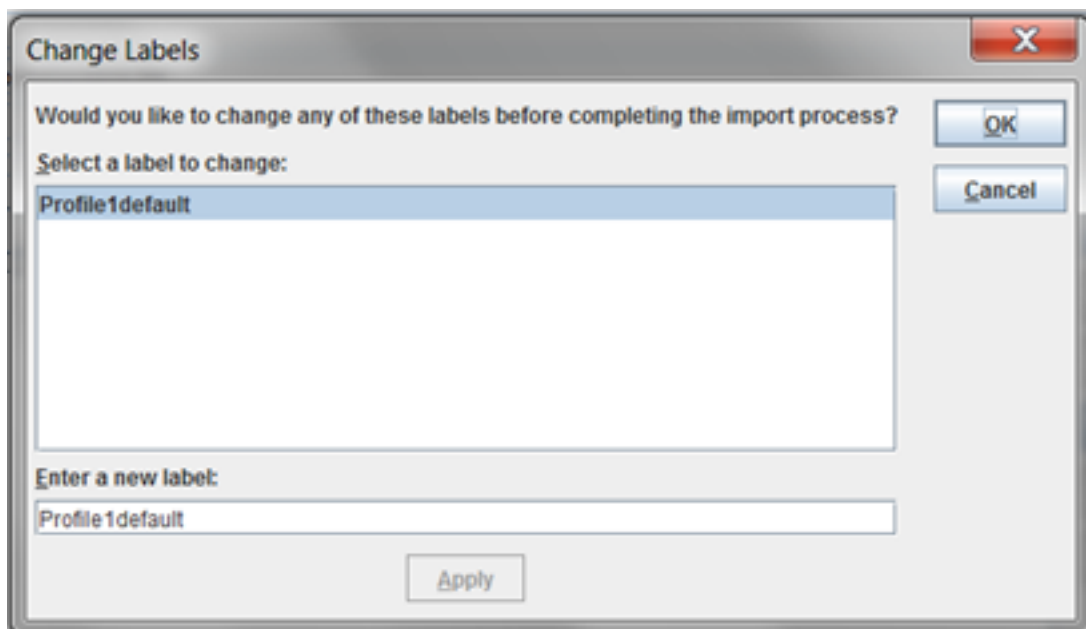
Note: Be sure to write down this password to have it available to provide to the Server Manager Console later when configuring the TrustStore and KeyStore Files for the secure profile.

Now we will import the KeyStore file from the WAS Secure Profile location. To import the KeyStore file:

1. Click **Import** to bring up the **Open** dialog box to import the trust.p12 file from the WAS Secure Profile's etc folder.
2. For the **Key file type** field, select **PKCS12**.
3. For the **File Name** field, click **Browse** and select the **trust.p12** file from your <WASInstall>/AppServer/profiles/<profile>/etc folder.

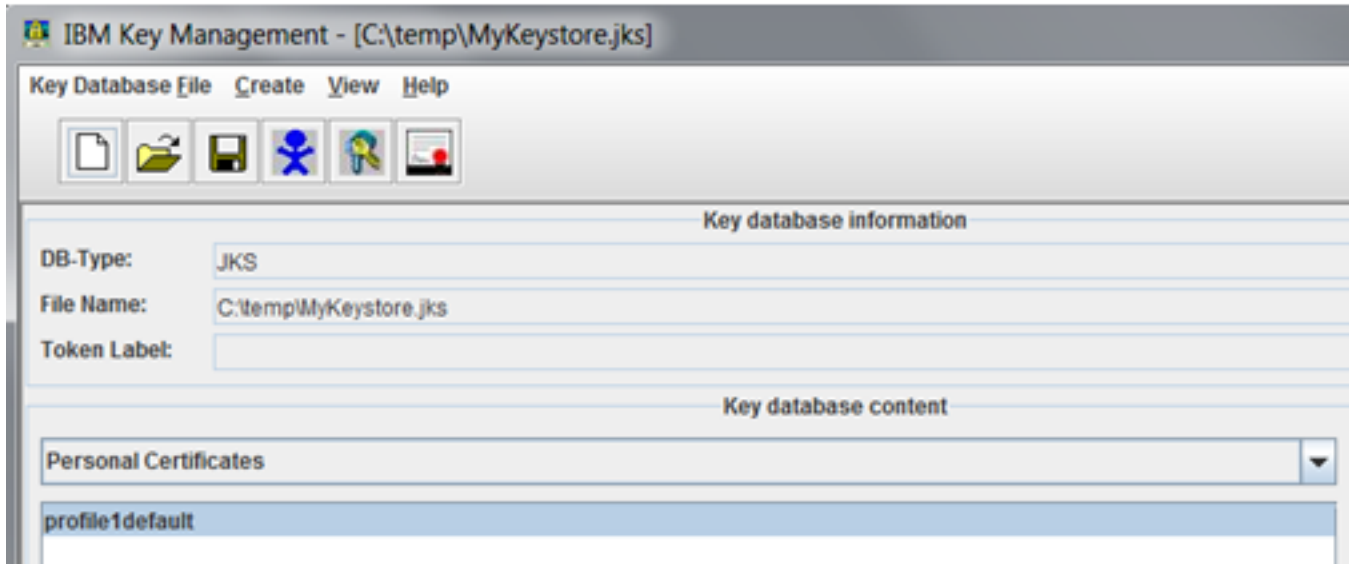


4. Click **OK**.
5. When prompted for a password, use **WebAS**, which is the default password for all of the profile's TrustStore and KeyStore files.
6. Click **OK**. This will bring up the **Change Labels** dialog box.
7. Select **default** from **Select a label to change** and enter a new label name like **Profile1default** to make sure every certificate that is imported from different profiles has a unique name associated with it.



8. Click **Apply**.
9. Click **OK** to save.

The KeyStore you have imported in the above steps will now be listed under the IKEYMAN **Personal Certificates**.



If you do not see the imported certificates under the **Signer Certificates** section, then the import did not work and you will need to redo these steps for *Importing the KeyStore Certificate* from the beginning.

If you are using multiple Secure Profiles, you will need to import KeyStore keys from each of these profiles to the same JKS database file. The instructions remain the same.

Close the newly created KeyStore Database by selecting **Key Database File**, and then select **Close**.

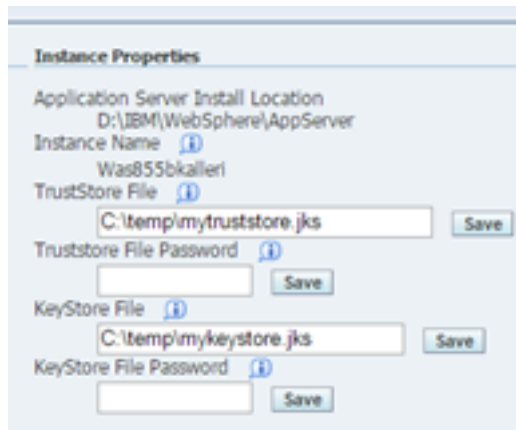
Configuring the Server Manager Console to Use Custom TrustStore and KeyStore Files

It is assumed that you have already created your own TrustStore and KeyStore files by following the previous steps. In this section we will configure the Server Manager Console to use the custom TrustStore and KeyStore files we have previously created. Make sure you copy these TrustStore and KeyStore files to a location on the host machine which is accessible for the Server Manager Agent which is managing the WAS you have registered. These files should be accessible to the Server Manager Agent which is managing the WAS instance. So, you will need to provide proper access to the file location depending on your Server Manager Agent host for OS Windows/UNIX/AS400.

If you have already registered a WAS Instance and would like to use the custom TrustStore and KeyStore files:

1. Open the registered WAS instance page.

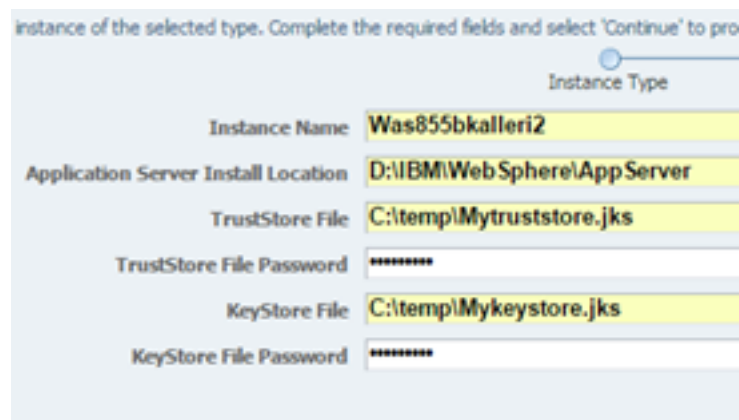
2. In the **Instance Properties** section (top right), enter the details below for each editable field:
 - o **TrustStore File** - enter the complete path to the TrustStore File, including the filename, and click **Save**.
 - o **TrustStore File Password** - enter the password used when the TrustStore file was created and click **Save**.
 - o **KeyStore File** - enter the complete path to the KeyStore File, including the filename, and click **Save**.
 - o **KeyStore File Password** - enter the password you have used while creating the KeyStore file, and click **Save**.



3. Restart the Server Manager Agent.

If you are registering a brand new WAS Instance and would like to use custom TrustStore and KeyStore files:

1. Navigate to the **Create/Register A Managed Instance** page.
2. In the **Instance Properties** section, enter the details below for each editable field:
 - o **Instance Name** - provide a valid/unique Instance name for the WAS instance.
 - o **Application Server Install Location** - provide the location of your WAS Application Server Install.
 - o **TrustStore File** - list the complete path to the TrustStore File, including the filename.
 - o **TrustStore File Password** - enter the password used when creating the TrustStore file.
 - o **KeyStore File** - list the complete path to the KeyStore File.
 - o **KeyStore File Password** - enter the password used when creating the KeyStore file.



3. Click **Continue**.

Complete the Management Console Setup Wizard

This section discusses:

- *Access the Management Console*
- *Run the Management Console Setup Wizard*

Access the Management Console

After the initial installation of the *Management Console*, an administrator can sign on to the *Management Console* using the `jde_admin` user and password specified during the installation. Access the *Management Console* using this URL:

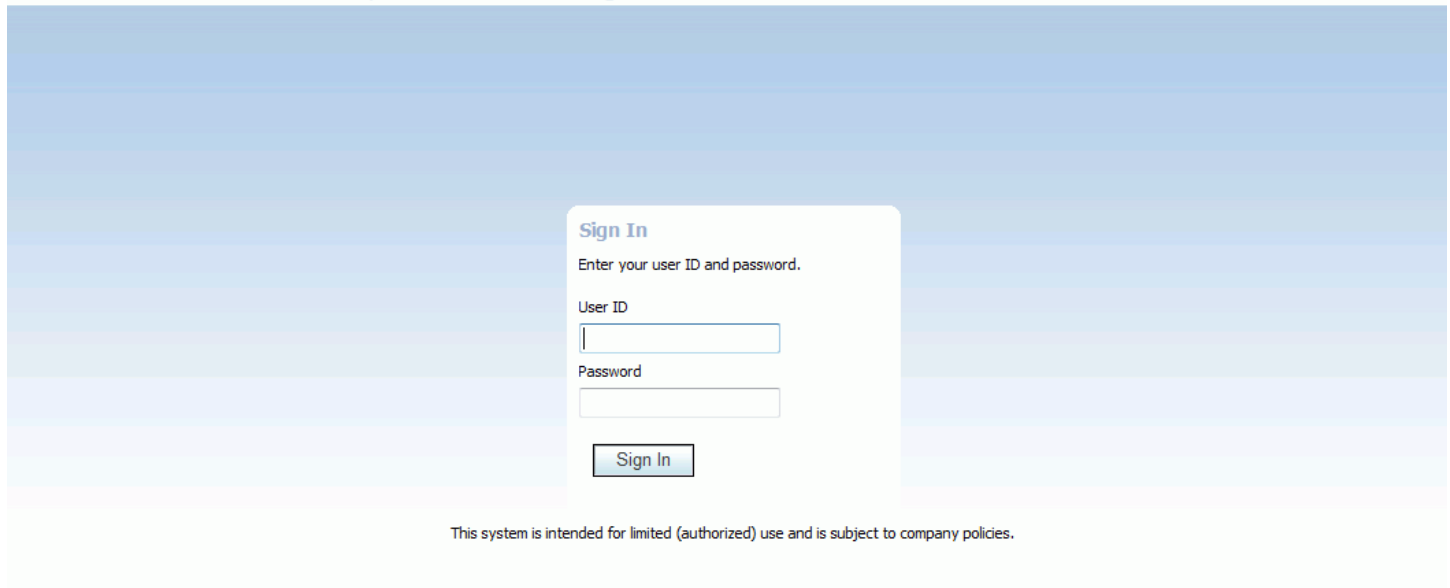
```
http://servername:port/manage
```

where `server_name` is the name of the *Server Manager* machine on which the *Management Console* is installed, and where `port` is the port that you specified for the *Management Console* when you ran the *Management Console* installer.

For example:

```
http://den1cmwn5.mlab.jdedwards.com:7000/manage/
```

ORACLE JD Edwards EnterpriseOne Server Manager



Run the Management Console Setup Wizard

The setup wizard guides you through the initial setup and configuration of the *Server Manager Management Console*. The wizard automatically starts the first time you access the *Management Console* after running the *Management Console* installer.

Tip:

You can stop and log out of the *Management Console* at any time. Upon signing back into the *Management Console*, you automatically return to the same wizard step.

Alternately, you can access the setup wizard at any time by entering this URL on the *Management Console* machine:

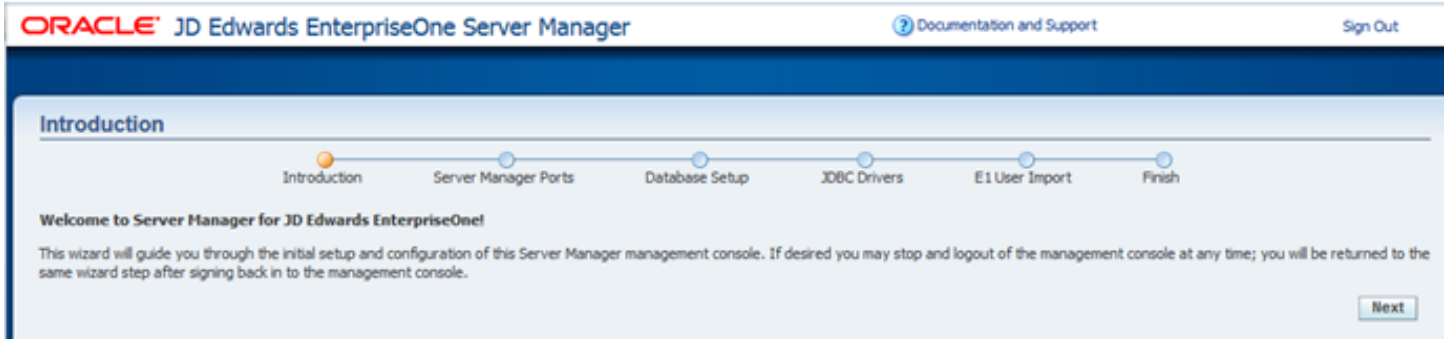
```
http://servername:port/manage
```

where `server_name` is the name of the *Server Manager* machine on which the *Management Console* is installed, and

where `port` is the port you specified for the *Management Console* when you ran the *Management Console* installer.

For example:

```
http://den1cmwn5.mlab.jdedwards.com:7000/manage/welcome
```



1. On Introduction, click Next to continue with the wizard.



Server Manager is comprised of a central *Management Console* and distributed *Management Agents* that reside on the physical machines that host the EnterpriseOne server components. The *Management Agents* communicate with the *Management Console* using a secure TCP/IP connection based on Java Management Extensions (JMX).

2. On Server Manager Ports, complete these fields:

- o *Management Server JMX Port*

This port is used by *Management Agents* to connect to the *Management Console*. This port must be unique and not in use on the *Management Console* machine. Once it is set, you cannot change this port without having to reinstall *Server Manager Management Agents*.

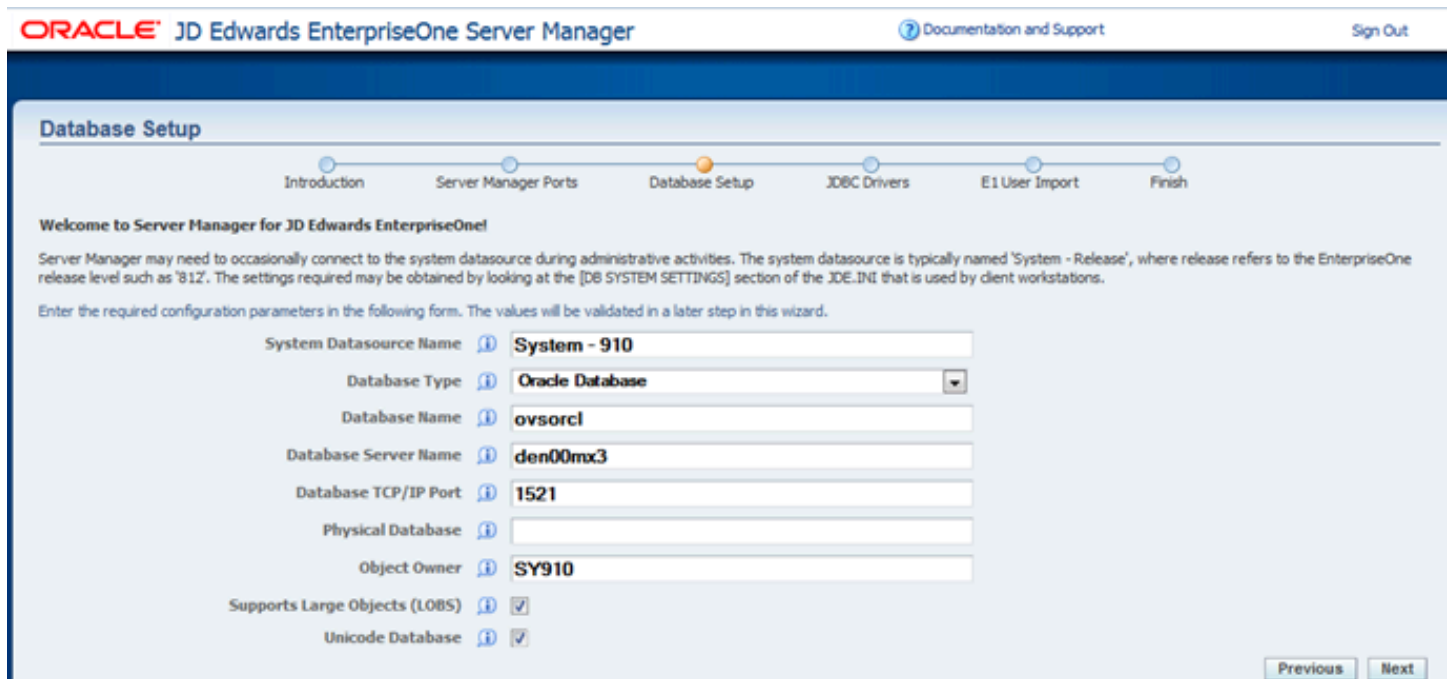
The default value is 14501.

- o *Management Agent Starting Point*

Once a *Management Agent* connects to the *Management Console* using the *Management Server JMX Port*, the *Management Console* dynamically assigns a port on which that *Management Agent* should listen. The *Management Console* assigns the next unused port for the physical machine beginning with the value specified for *Management Agent Starting Point*.

For example if you set this value to 14501 and three *Management Agents* are running on the same remote machine, the *Management Console* assigns each *Management Agent* a unique value from the range (14501, 14502, and 14503). If an additional *Management Agent* on the same machine connects to the *Management Console*, the *Management Console* assigns the value 14504. If a *Management Agent* on a different physical machine then connects with the *Management Console* it assigns the value 14501. This value can be changed at any time without the need to reinstall or restart any deployed *Management Agent* or EnterpriseOne software.

3. Click Next to continue the wizard.



Server Manager may need to occasionally connect to the system datasource during administrative activities. The system datasource is typically named *System Release*, where *Release* refers to the EnterpriseOne release level such as *900*. The settings required can be obtained from the [DB SYSTEM SETTINGS] section of the JDE.INI that is used by Development Client.

4. On Database Setup, complete the fields whose values will be validated in a later step in this wizard:

- o *System Datasource Name*

Enter the name of the data source where the OCM and other system tables reside.

This entry corresponds to the `Base Datasource` entry in `[DB SYSTEM SETTINGS]`.

Note: This setting is not critical for bootstrap connections, but if it is missing or incorrect, appropriate error messages will be logged.

- o *Database Type*

This value defines the type of database this datasource represents. Valid values are:

- AS/400
- Oracle Database
- SQL Server
- IBM DB2

This entry corresponds to the `Type` entry in the `[DB SYSTEM SETTINGS]` in the `JDE.INI` of a *JD Edwards EnterpriseOne Web Development Client*.

- o *Database Name*

Enter the name of the database that this datasource represents. This entry is applicable only to Oracle database and UDB database types.

The value for this entry corresponds to the `Database` entry in the `[DB SYSTEM SETTINGS]` in the `JDE.INI` of a *JD Edwards EnterpriseOne Web Development Client*.

For the Oracle database, the value of this entry is the name of the connect string (SID) identifying the database in the `tnsnames.ora` configuration file.

- o *Database Server Name*

Enter the name of physical machine that contains the database application. This entry corresponds to the 'Server' entry in the `[DB SYSTEM SETTINGS]` in the `JDE.INI` of a *JD Edwards EnterpriseOne Web Development Client*.

- o *Database TCP/IP Port*

Specify the TCP/IP port used to communicate with the database.

This entry corresponds to the `ServerPort` entry in the `[DB SYSTEM SETTINGS]` in the `JDE.INI` file of a *JD Edwards EnterpriseOne Web Development Client*.

If a database port is not applicable, such as DB2/400 datasources, enter a zero.

- o *Physical Database*

Enter the physical database name.

For AS/400 datasource types, this specifies the library name.

For MS SQL Server datasource types, this specifies the actual database name.

Otherwise, this setting is not used for the other datasource types.

This entry corresponds to the `DatabaseName2` entry in the `[DB SYSTEM SETTINGS]` in the JDE.INI file of a *JD Edwards EnterpriseOne* Web Development Client.

- *Object Owner*

Enter the object owner or schema of the tables within the database this datasource represents.

This setting is only used for Oracle, SQL Server, and UDB datasource types.

This entry corresponds to the `object owner` entry in the `[DB SYSTEM SETTINGS]` in a JDE.INI for of a *JD Edwards EnterpriseOne* Web Development Client.

- *Supports Large Objects (LOBs)*

Defines whether the datasource supports large objects (LOBs) as a column type.

This setting is used for Oracle and AS/400 datasource types only.

This entry corresponds to the `LOBFlag` entry in the `[DB SYSTEM SETTINGS]` in a JDE.INI for of a *JD Edwards EnterpriseOne* Web Development Client.

- *Unicode Database*

Defines whether the datasource contains UNICODE encoded data.

This setting is only used for SQL Server.

This entry corresponds to the `unicodeFlag` entry in the `[DB SYSTEM SETTINGS]` in a JDE.INI for of a *JD Edwards EnterpriseOne* Web Development Client.

5. Click Next to continue the wizard.

Note: In this context at this stage in the Welcome Wizard, the JDBC drivers are only required to complete the next step in the Wizard, which is to import users from an existing *JD Edwards EnterpriseOne* installation.

For information on managing JDBC drivers, refer to the chapter of the *Server Manager Guide* entitled: *Manage JDBC Drivers*.

When your *Management Console* already has the appropriate JDBC driver, the *Management Console* displays the message **The appropriate JDBC driver has been successfully detected and initialized** and then prompts you to restart the *Management Console* in order to use the drivers.

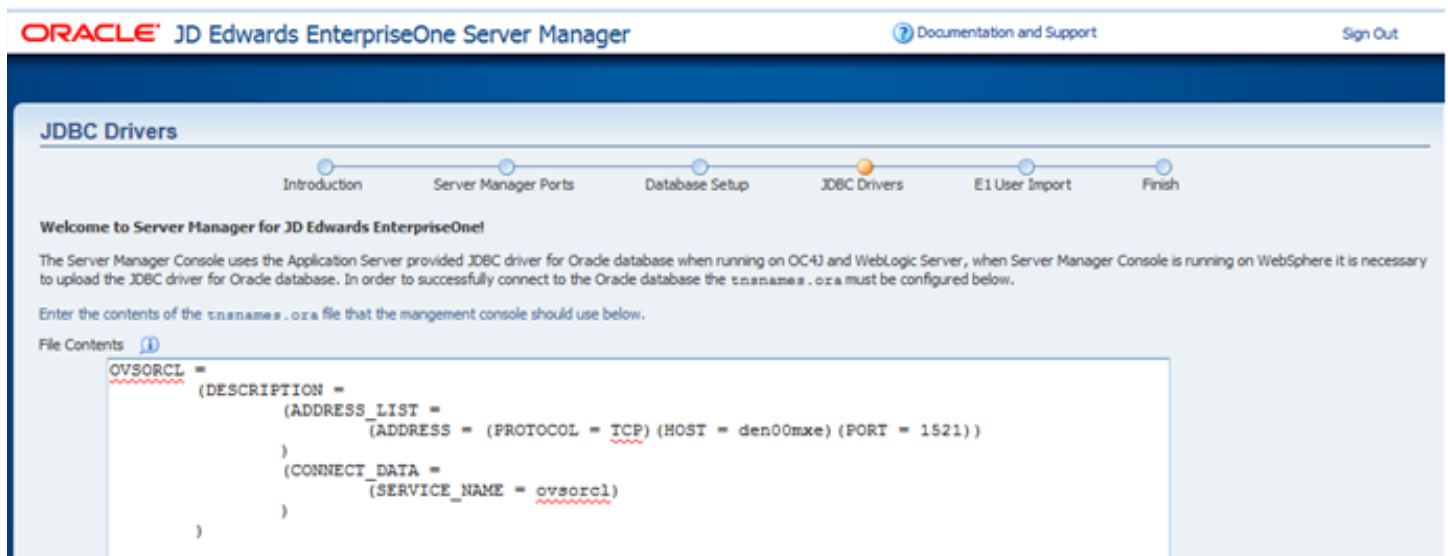
6. On JDBC Drivers, click the **Restart Management Console** button.

Note: It might take a few minutes for the *Management Console* to restart. Upon restart, you are prompted to enter your *Management Console* login credentials. *Server Manager* returns you to the same *Management Console* Setup Wizard step that you were using before to the restart.

7. Click Next.

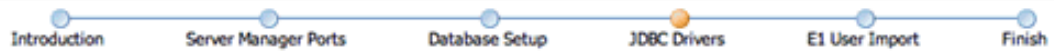
The *Management Console* verifies that your JDBC Driver is properly setup and if so it proceeds to the next screen. If not, then you are prompted to remedy errors as appropriate.

8. On Database Setup, the *Management Console* displays the appropriate page depending on the database that you selected from the Database Type dropdown, as described in these substeps:
 - AS400, see Substep a.
 - Oracle database, see Substep b.
 - MS SQL Server, see Substep c.
 - IBM DB2, see Substep d.
 - a. For AS400, once the Database Setup and JDBC Drivers forms are properly completed, the last page on the JDBC Drivers portion of the wizard is displayed indicating that the appropriate JDBC driver has been successfully detected and initialized:



- b. For the Oracle database, you are prompted to complete this form to configure your `tnsnames.ora` file:

JDBC Drivers



Welcome to Server Manager for JD Edwards EnterpriseOne!

The management console includes a JDBC driver for Oracle databases; uploading a suitable driver is not necessary. In order to successfully connect to the Oracle database the `tnsnames.ora` must be configured below.

Enter the contents of the `tnsnames.ora` file that the management console should use below.

File Contents ⓘ

```
# tnsnames.ora Network Configuration File: D:\oracle\product\10.2.0\client_1\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.
LISTENER_ORCL =
  (ADDRESS = (PROTOCOL = TCP)(HOST = ROYA.mlab.jdedwards.com)(PORT = 1521))

ORCL =
  (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = ROYA.mlab.jdedwards.com)(PORT = 1521))
    (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl) ) )

EXTPROC_CONNECTION_DATA =
  (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0)) )
    (CONNECT_DATA = (SID = PLSExtProc) (PRESENTATION = RO) ) )

ORCL10G =
  (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = denlcmix1.mlab.jdedward:
    (CONNECT_DATA = (SERVICE_NAME = ORCL10G) ) ) )

orcl812 =
  (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = denlcmix2.mlab.jdedward:
    (CONNECT_DATA = (SERVICE_NAME = orcl812) ) ) )
```

✔ The appropriate JDBC driver has been successfully detected and initialized.

Previous Next

Tip: You can cut and paste the contents of the `tnsnames.ora` file from the *JD Edwards EnterpriseOne* Web Development Client into this form.

- c. For Microsoft SQL Server, you are initially prompted to upload the `mssql-jdbc-7.4.1.jre8.jar` file.

Note: Depending on the value that you enter for *Database Type*, the wizard chooses the appropriate next screen for JDBC Drivers. If the *Management Console* displays this message, you have already uploaded the appropriate driver and proceed to Step 8.

✔ The appropriate JDBC driver has been successfully detected and initialized.

If you have not yet uploaded the JDBC driver for the database that you selected, the *Management Console* displays the appropriate form that you can use to Upload the driver.

JDBC Drivers



Welcome to Server Manager for JD Edwards EnterpriseOne!

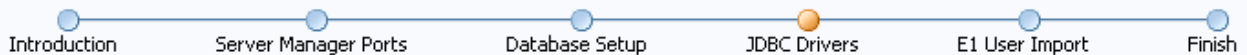
The management console requires an appropriate JDBC driver in order to connect to the configured SQL Server datasource.

✔ The appropriate JDBC driver has been successfully detected and initialized.

[Previous](#) [Next](#)

- d. For IBM UDB, once the Database Setup and JDBC Drivers forms are properly completed, the last page on the JDBC Drivers portion of the wizard is displayed indicating that the appropriate JDBC driver has been successfully detected and initialized:

JDBC Drivers



Welcome to Server Manager for JD Edwards EnterpriseOne!

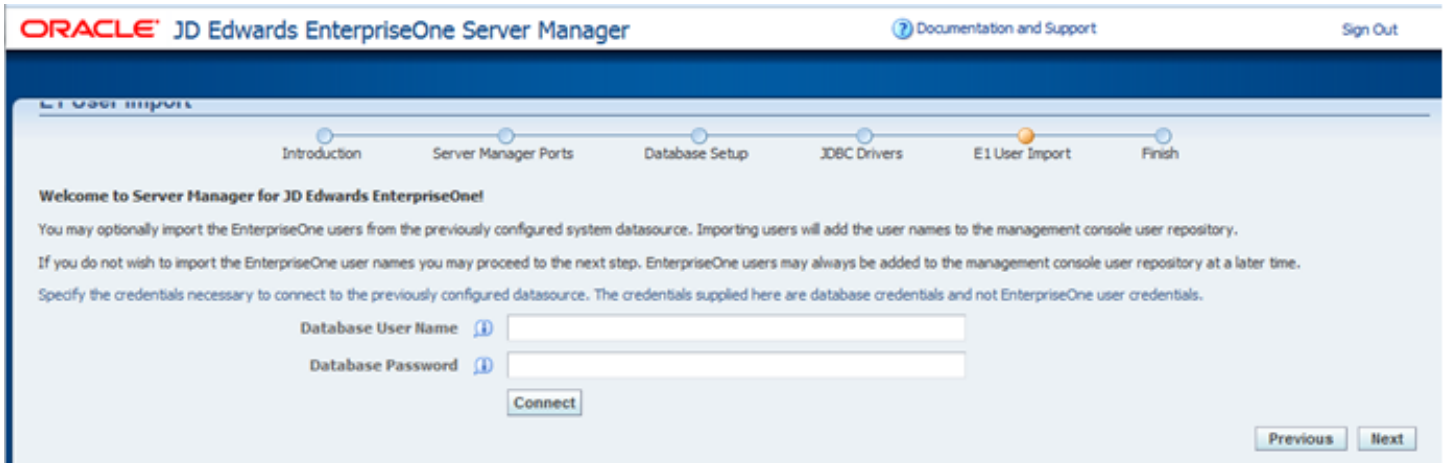
The management console requires an appropriate JDBC driver in order to connect to the configured UDB/DB2 datasource. The binary directory of the DB2 client software must be within the system path (environment variable PATH), and the DB2 catalog must be correct.

✔ The appropriate JDBC driver has been successfully detected and initialized.

[Previous](#) [Next](#)

9. When you have completed setting up your JDBC drivers, click Next.

The *Management Console* saves the current configuration data before continuing to the next screen. This enables you to exit and re-enter the wizard and not lose any entered configuration data up to this point in the wizard.



10. On E1 User Import, you can optionally import the *JD Edwards EnterpriseOne* users from the previously configured System Datasource. Importing users adds the user names to the *Management Console* user repository.

If you do not wish to import the EnterpriseOne user names, you can proceed to Step 11. *JD Edwards EnterpriseOne* users can always be added to the *Management Console* user repository later. Refer to the chapter of the *Server Manager Guide* entitled: *Configure Management Console Users*.

If you want to import *JD Edwards EnterpriseOne* users, you must specify the credentials necessary to connect to the previously configured datasource. The credentials supplied here are database credentials and not EnterpriseOne user credentials.

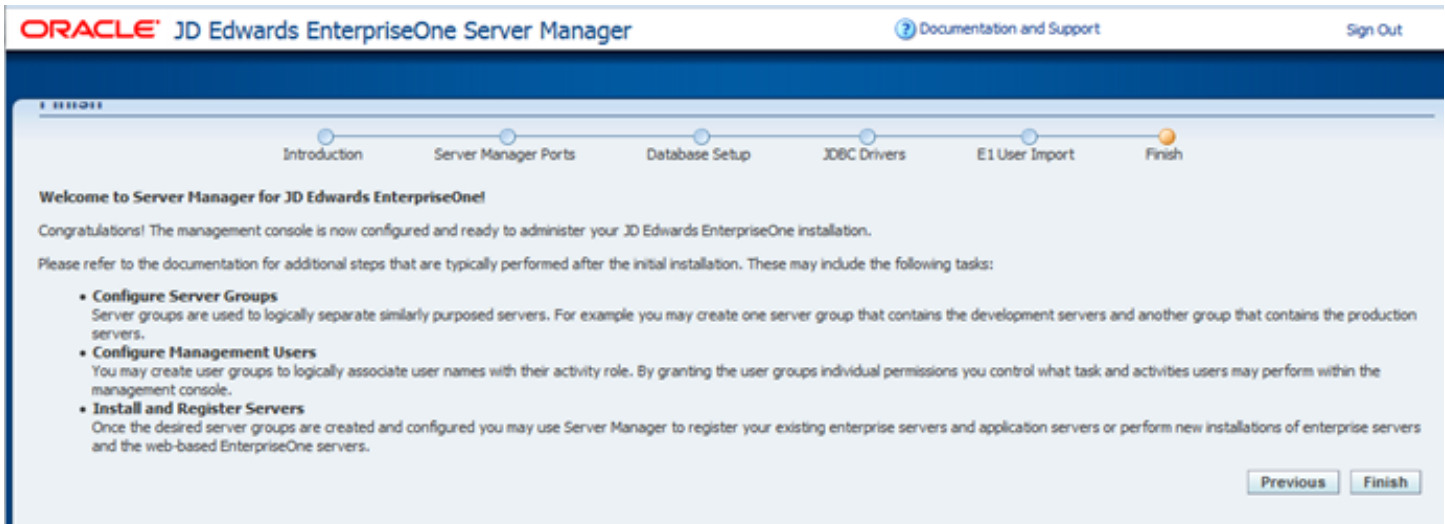
- o *Database User Name*

Enter a valid user name for the database to use when connecting directly to the configured database.

- o *Database Password*

Enter a valid password for the user name specified in the *Database User Name* field.

11. Click Next to continue with the setup wizard.



Congratulations! The *Management Console* is now configured and ready to administer your *JD Edwards EnterpriseOne* installation.

12. On Finish, you are advised to review the *Management Console* documentation for additional steps that are typically performed after the initial installation. These steps include:
 - o Configure Server Groups

Server groups are used to logically separate servers with a similar purpose. For example, you might create one server group that contains the development servers and another group that contains the production servers.

Refer to the sections in the *Server Manager Guide* entitled: *Administer Server Groups* .
 - o Configure Management Users

You can create user groups to logically associate user names with their activity role. By granting the user groups individual permissions, you control what task and activities users may perform within the *Management Console* .

Refer to the section in the *Server Manager Guide* entitled: *Administer Management Console Users and User Groups* .
 - o Install and Register Servers

Once the desired server groups are created and configured you can use *Server Manager* to register your existing Enterprise Servers and application servers or perform new installations of Enterprise Servers and the web based EnterpriseOne servers.

Refer to the sections in the *Server Manager Guide* entitled:

 - *Register an Application Server*
 - *Register or Create a JD Edwards Enterprise Server as a New Managed Instance*

- *Create a JD Edwards EnterpriseOne Web-Based Server as a New Managed Instance*

This chapter includes the steps to create these *JD Edwards EnterpriseOne* web-based servers:

- HTML Web Server
- Transaction Server
- Collaborative Portal
- Business Services Server

13. Click Finish to complete the *Management Console* setup wizard.

Upgrade the Server Manager Management Console with Oracle WebLogic Server 12.1.2

This section discusses these topics:

- *Overview*
- *Uninstalling Server Manager Console Installed on Oracle WebLogic Server 10.3.6*
- *Installing Oracle WebLogic Server 12.1.2*
- *Installing Server Manager Console on WebLogic Server 12.1.2*
- *Restoring the Previous Server Manager Console Configurations*

Overview

The purpose of this document is to provide information about upgrading the Server Manager Console to be used with WebLogic Server 12.1.2.

There is no direct upgrade path available for upgrading Server Manager Console installed on WebLogic Server 10.3.6 to WebLogic Server 12.1.2.

WebLogic Server 12.1.2 has to be a new install and Server Manager Console needs to be installed on it.

Most of the Server Manager configuration from the previous installation can be preserved with some manual configuration.

The steps below can be followed to upgrade Server Manager Console install to WebLogic Server 12.1.2

1. Uninstall the Server Manager console installed on WebLogic Server 10.3.6.
2. Install Oracle WebLogic Server 12.1.2.
3. Install Server Manager Console on WebLogic Server 12.1.2.
4. Restore the previous Server Manager Console Configurations.

Uninstalling Server Manager Console Installed on Oracle WebLogic Server 10.3.6

To uninstall the Server Manager Console, you must use the Oracle Universal Installer.

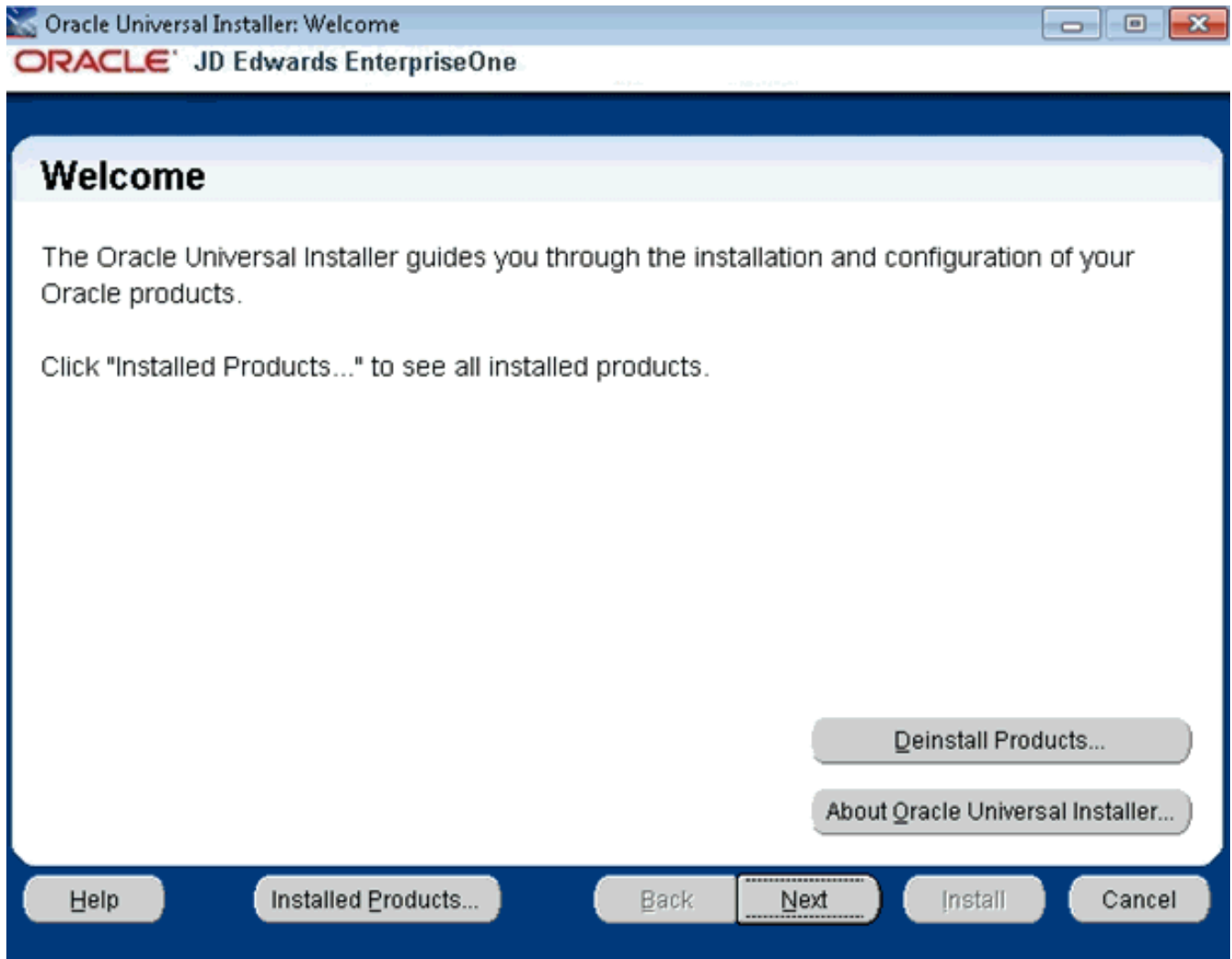
Prior to uninstalling the existing Server Manager Console, keep a backup these folders and files:

1. The folder "<SM_CONSOLE_HOME>\targets\home\config"
2. management-console.xml under "<SM_CONSOLE_HOME>\targets\home"
3. monitors.xml under "<SM_CONSOLE_HOME>\targets\home"
4. scf-history.xml under "<SM_CONSOLE_HOME>\targets\home"
5. security-realm.xml under "<SM_CONSOLE_HOME>\targets\home"

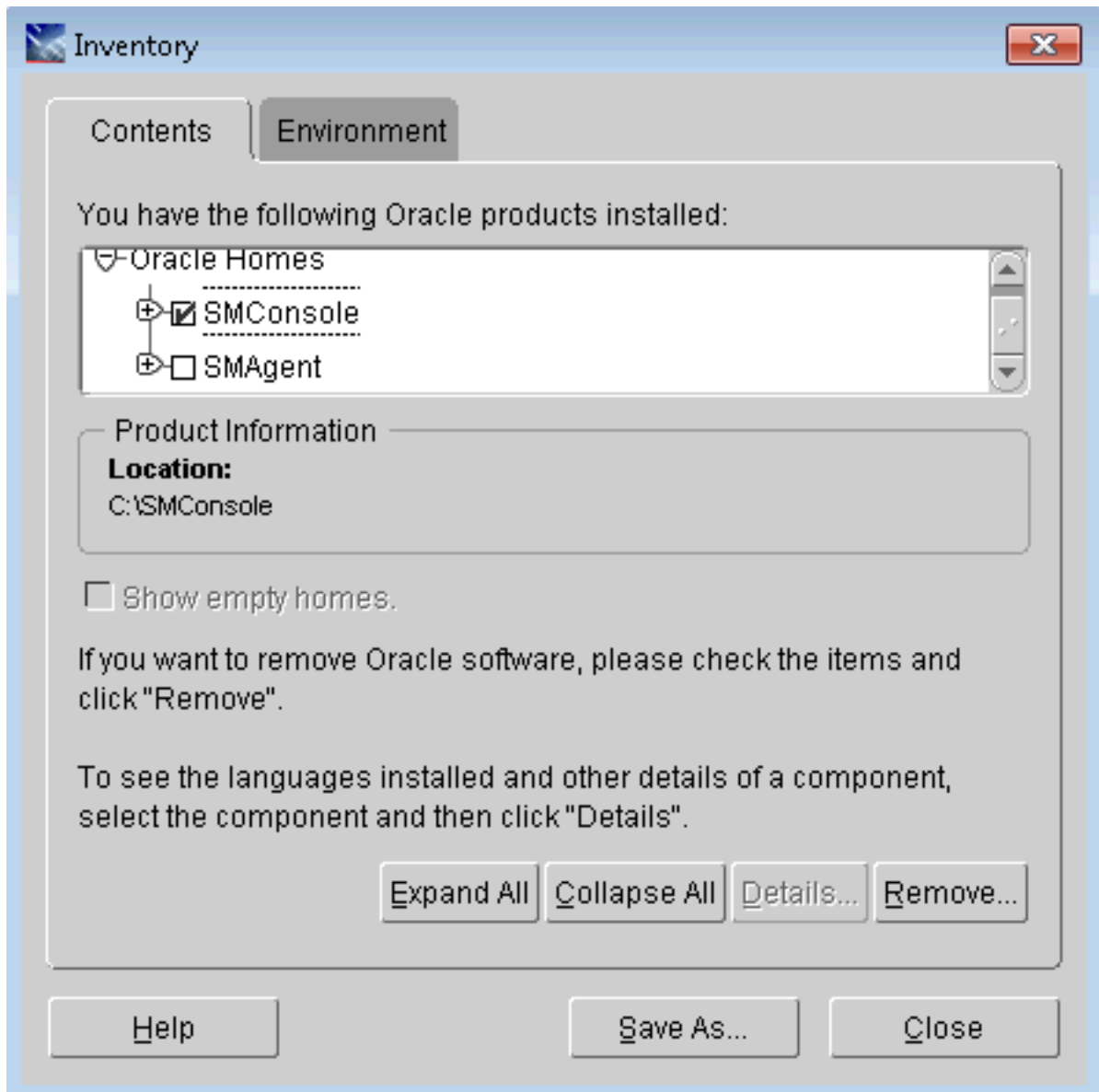
To uninstall the Server Manager Console using the Oracle Universal Installer:

Note: The JRE or JDK that was specified during installation was copied to the Oracle Home (for example, installation directory); the deinstaller uses that JRE or JDK when it is run so no `-jreLoc` argument is needed.

1. Invoke the Oracle Universal Installer on the Server Manager Console installed machine.



2. The welcome screen appears. Click on **Deinstall Products**.



3. The Inventory screen appears. Select the Server Manager Console component. Click **Remove**. This will guide you further and remove the Server Manager Console component.

Installing Oracle WebLogic Server 12.1.2

The examples in this document assume you are using a Windows based platform. If you are installing the Oracle WebLogic Server on a UNIX machine, some of the files names and directories may be slightly different. When installing on UNIX, the Oracle web tier components should be installed using a non-root user.

Note:

- **Microsoft Windows:** *HTML Server on Oracle WebLogic Server Reference Guide Release 9.2 for Microsoft Windows*
- **UNIX:** *HTML Server on Oracle WebLogic Server Reference Guide Release 9.2 for UNIX*

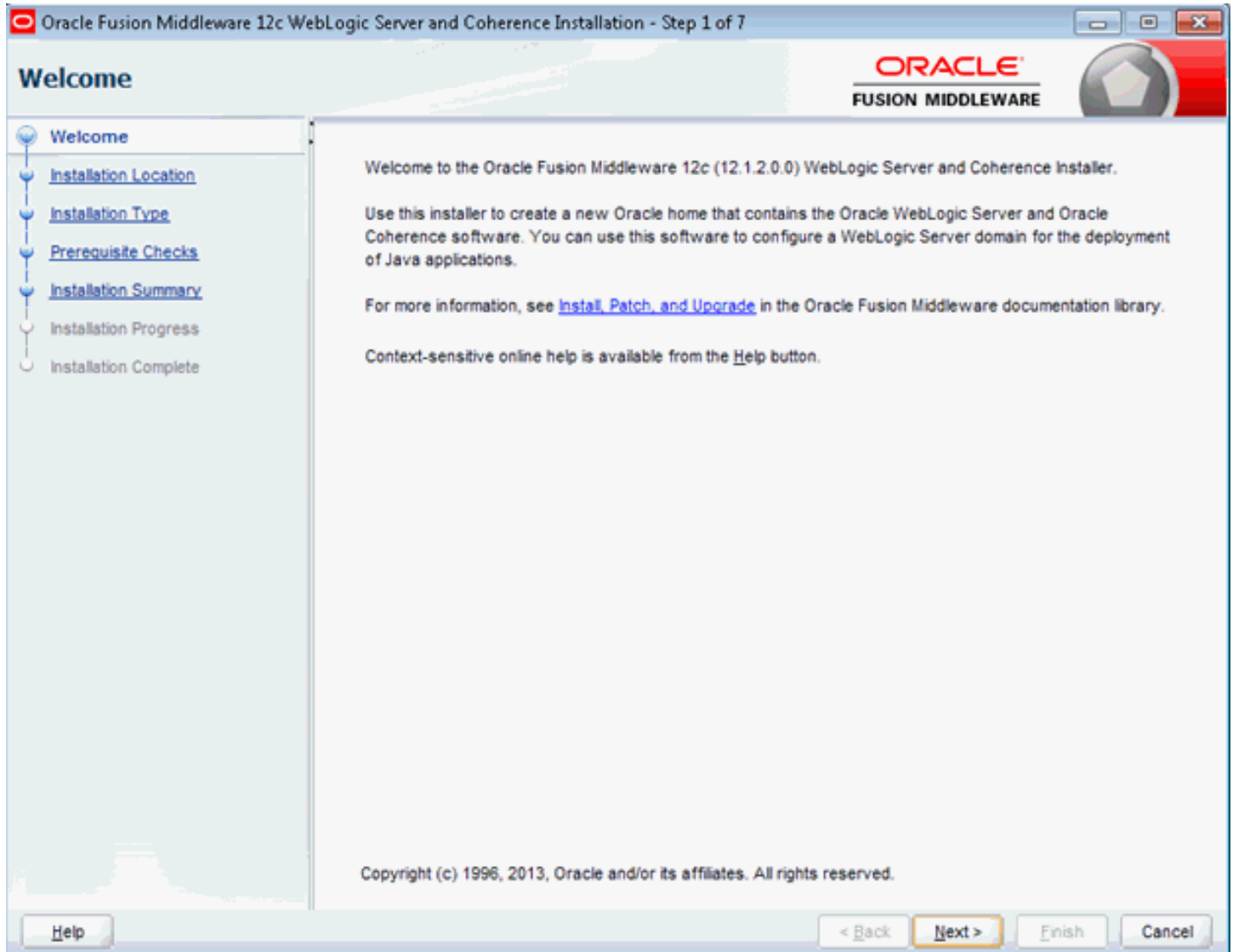
1. Download the "Oracle Fusion Middleware 12c WebLogic Server and Coherence (12.1.2.0.0)" package that is appropriate for your platform from the Oracle Software Delivery Cloud site (<https://edelivery.oracle.com>). The file name of the installer is `wls_121200.jar`. Refer to the JD Edwards EnterpriseOne Certifications for more information.
2. Unzip the downloaded file into a temporary directory on the machine you are targeting for installation.
3. Open a Command window with Run as Administrator option and run this command from the prompt:

```
>java -jar wls_121200.jar
```

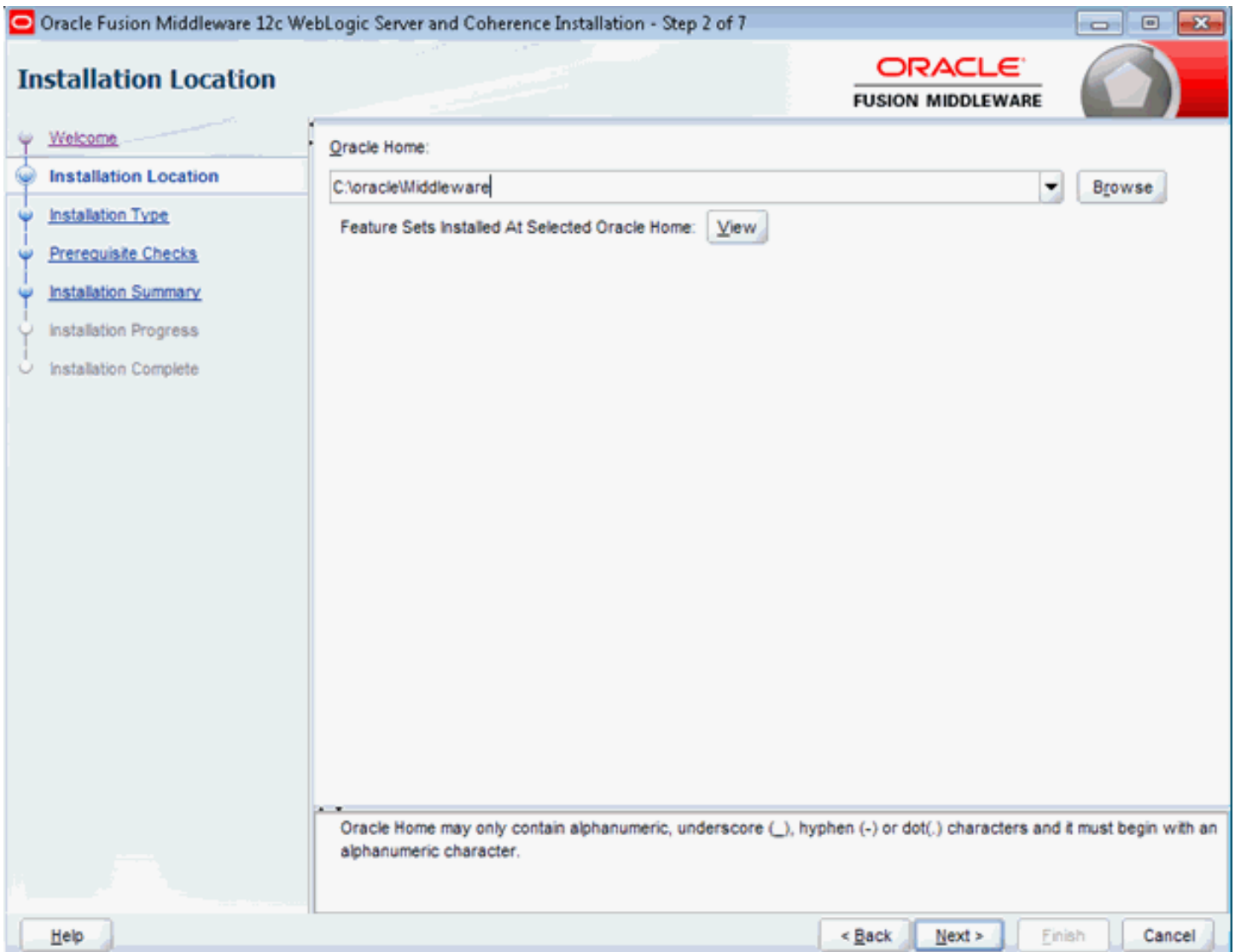
For HP-UX and Solaris use the '-d64' option:

```
>java -jar -d64 wls_121200.jar
```

The first screen you will see is the Welcome screen.



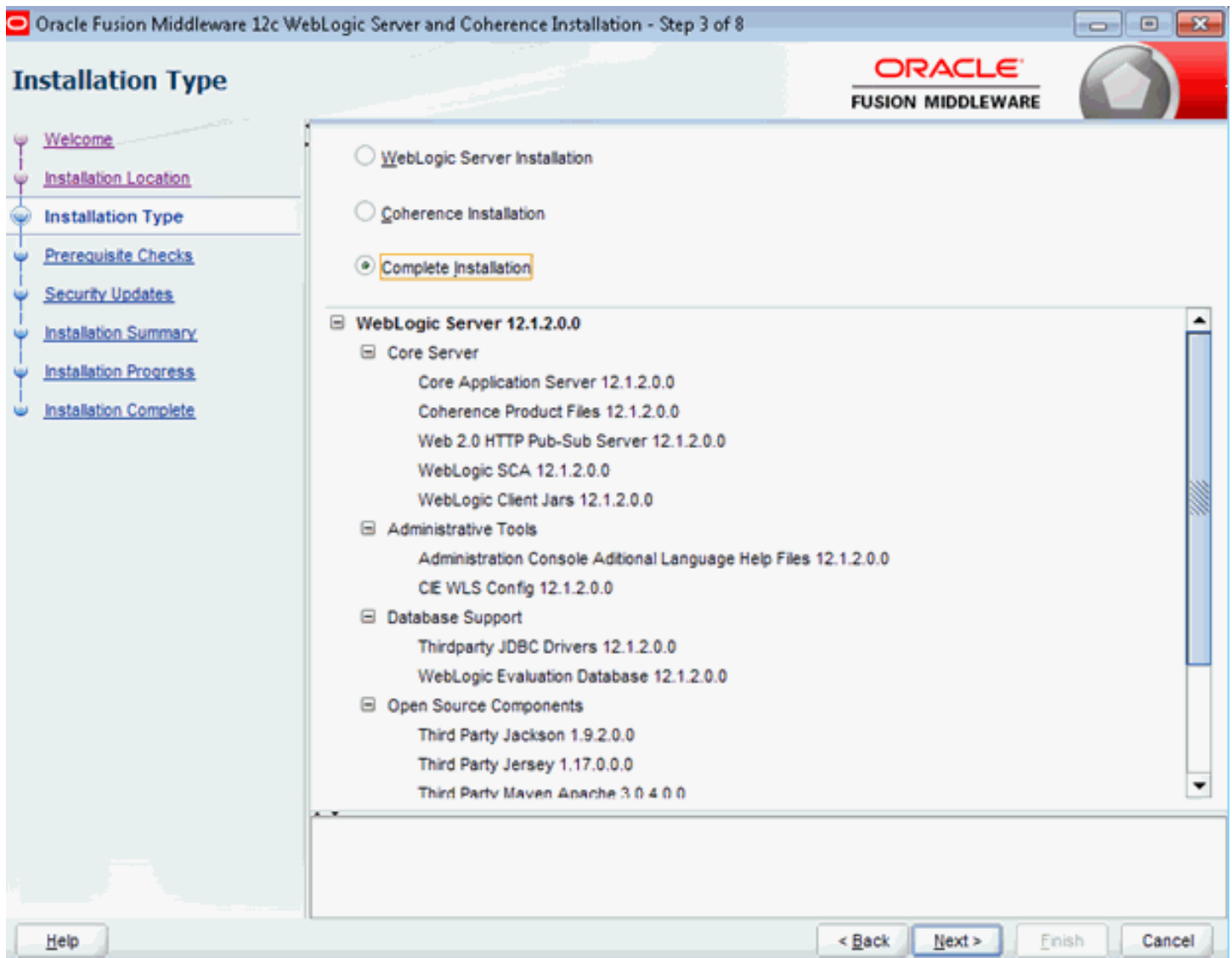
4. Click the **Next** button to begin the installation.



If you have an existing directory into which one or more Oracle products have already been installed, that directory can be viewed in the drop-down list. You can see which products are installed in that particular directory by clicking View next to “Features Sets Installed at Selected Oracle Home.”

If you want your product to be installed in a new directory, type the full path of your new directory in the Oracle Home field; the installer will create the specified directory for you.

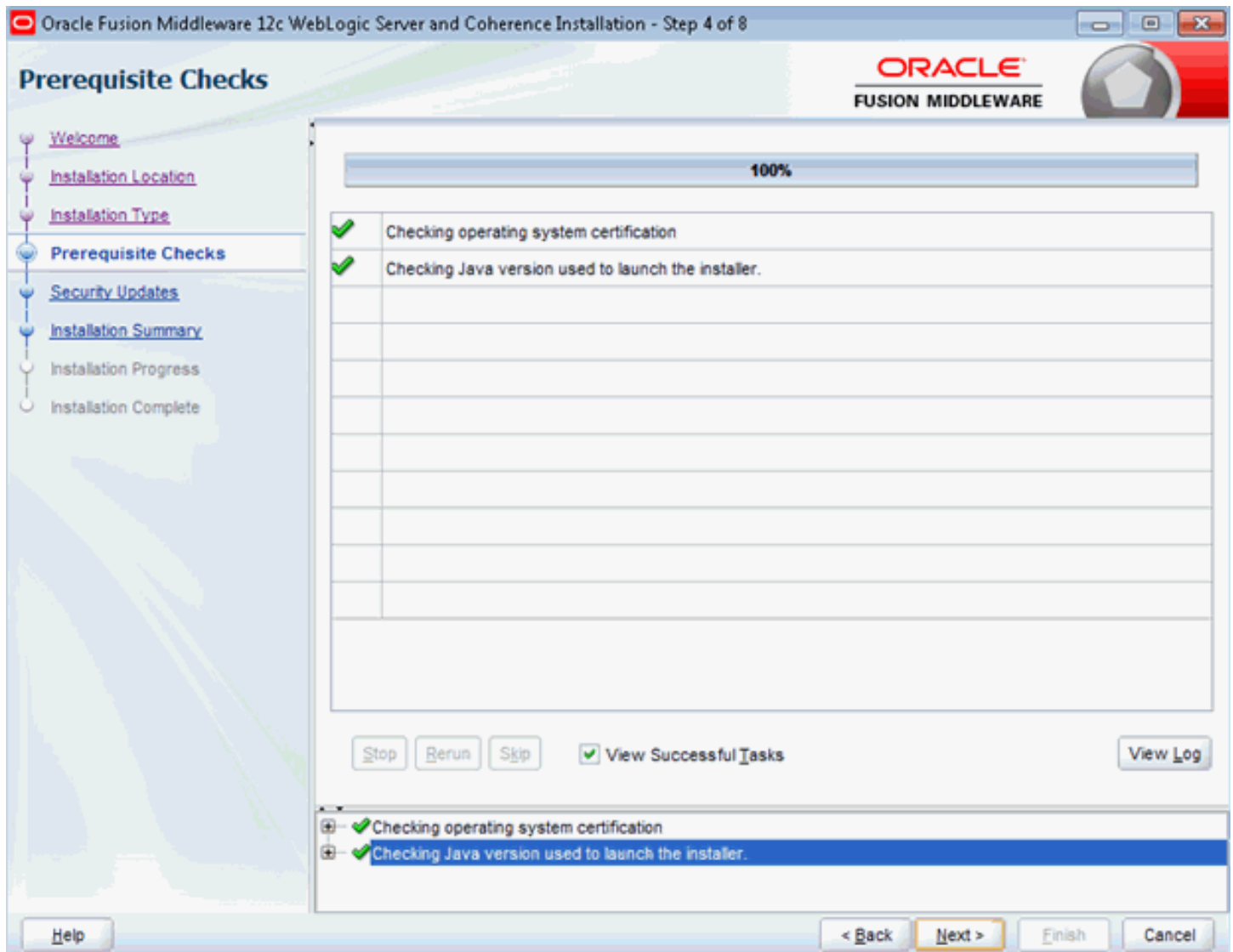
5. Click **Next**.



Use this screen to determine the type of installation you want to perform and consequently, which products and features are installed.

The options you see on this screen will differ depending on the product you are installing. Refer to your product installation guide for specific details.

6. Click **Next**.



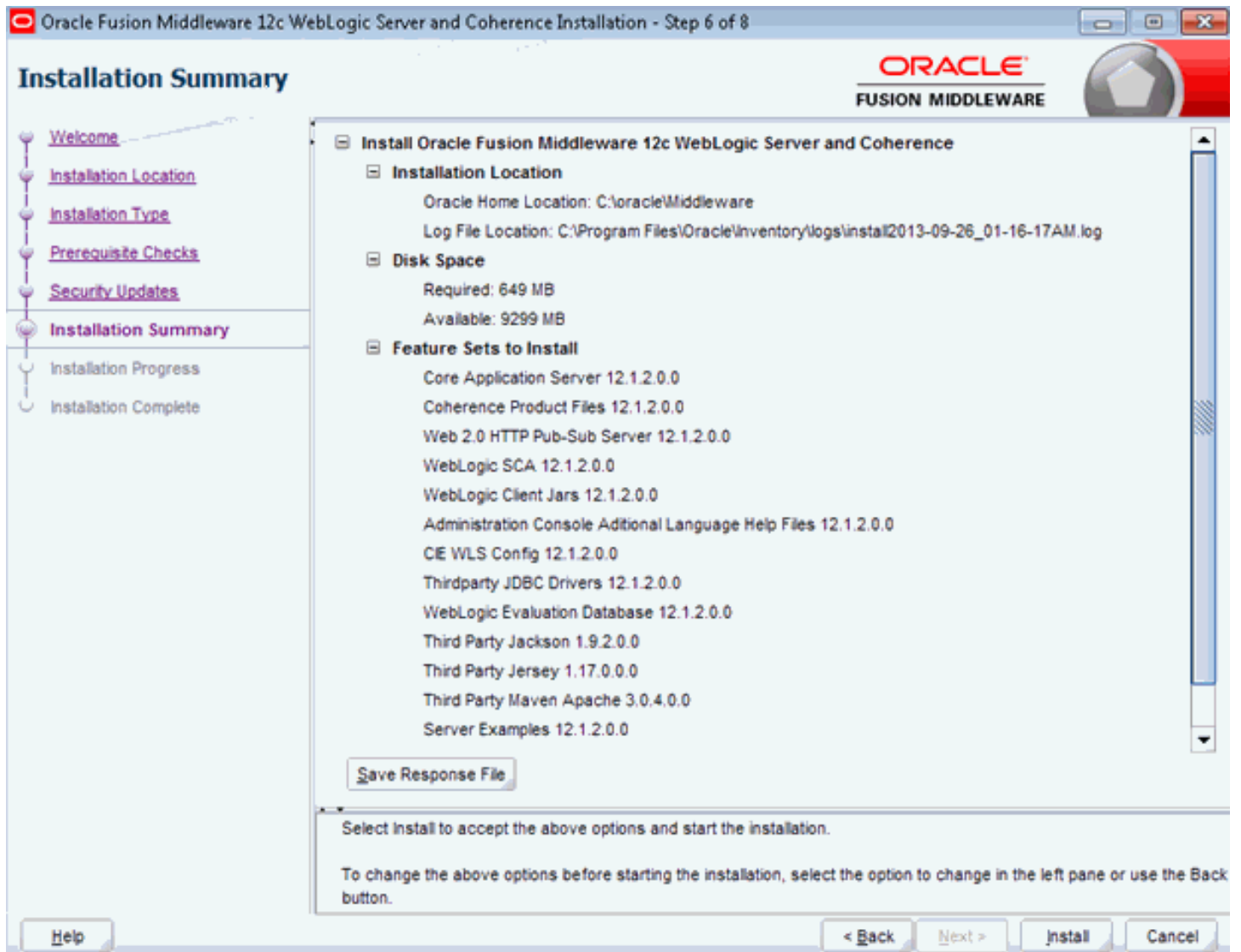
This screen analyzes the host computer to ensure that specific operating system prerequisites have been met.

7. On completion of the Prerequisites Checks, click **Next**.



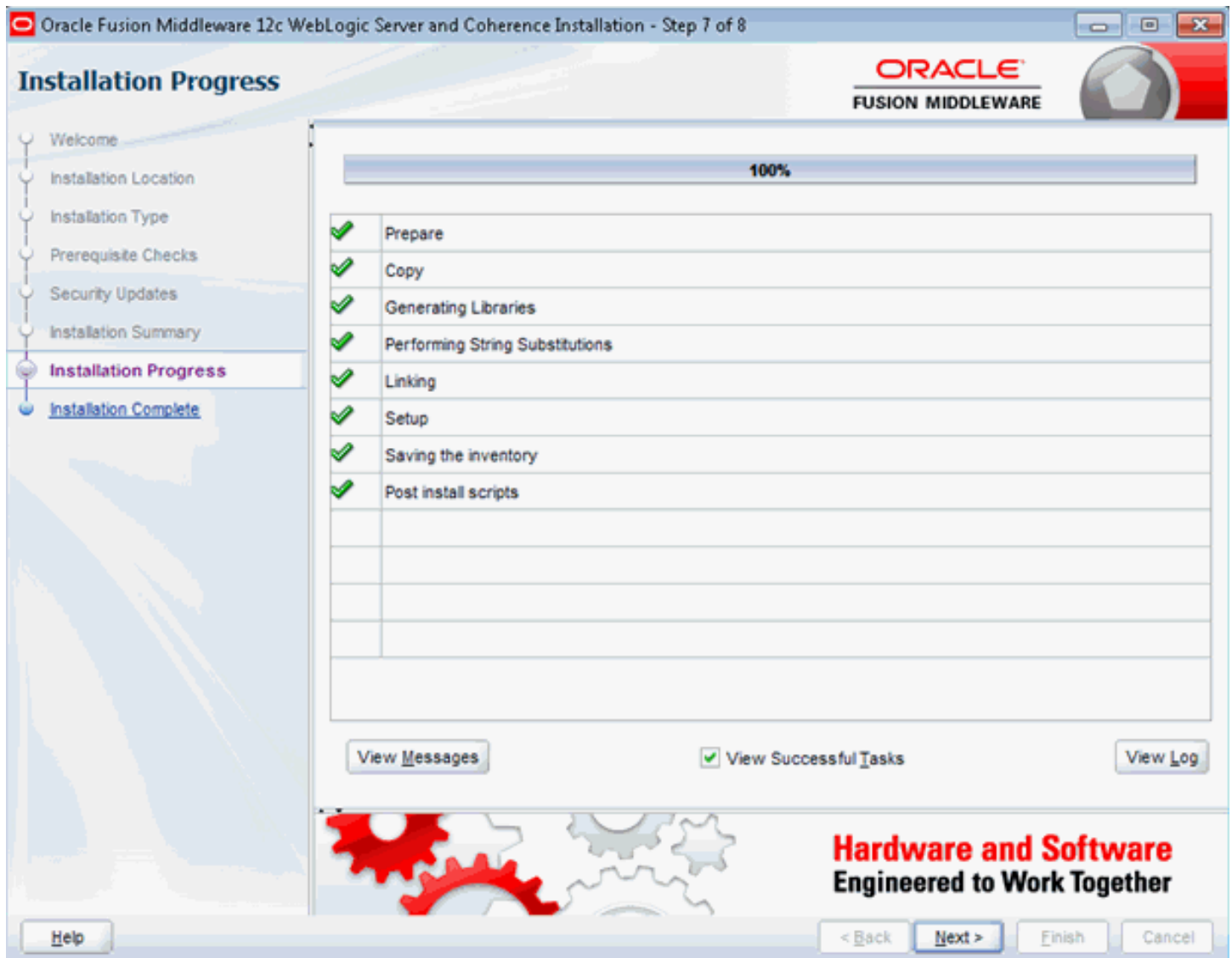
If you wish to register your installation, enter your Email address and your My Oracle Support password. If you wish to decline registration, deselect **I wish to receive security updates via My Oracle Support** and confirm your choice.

8. Click **Next**.



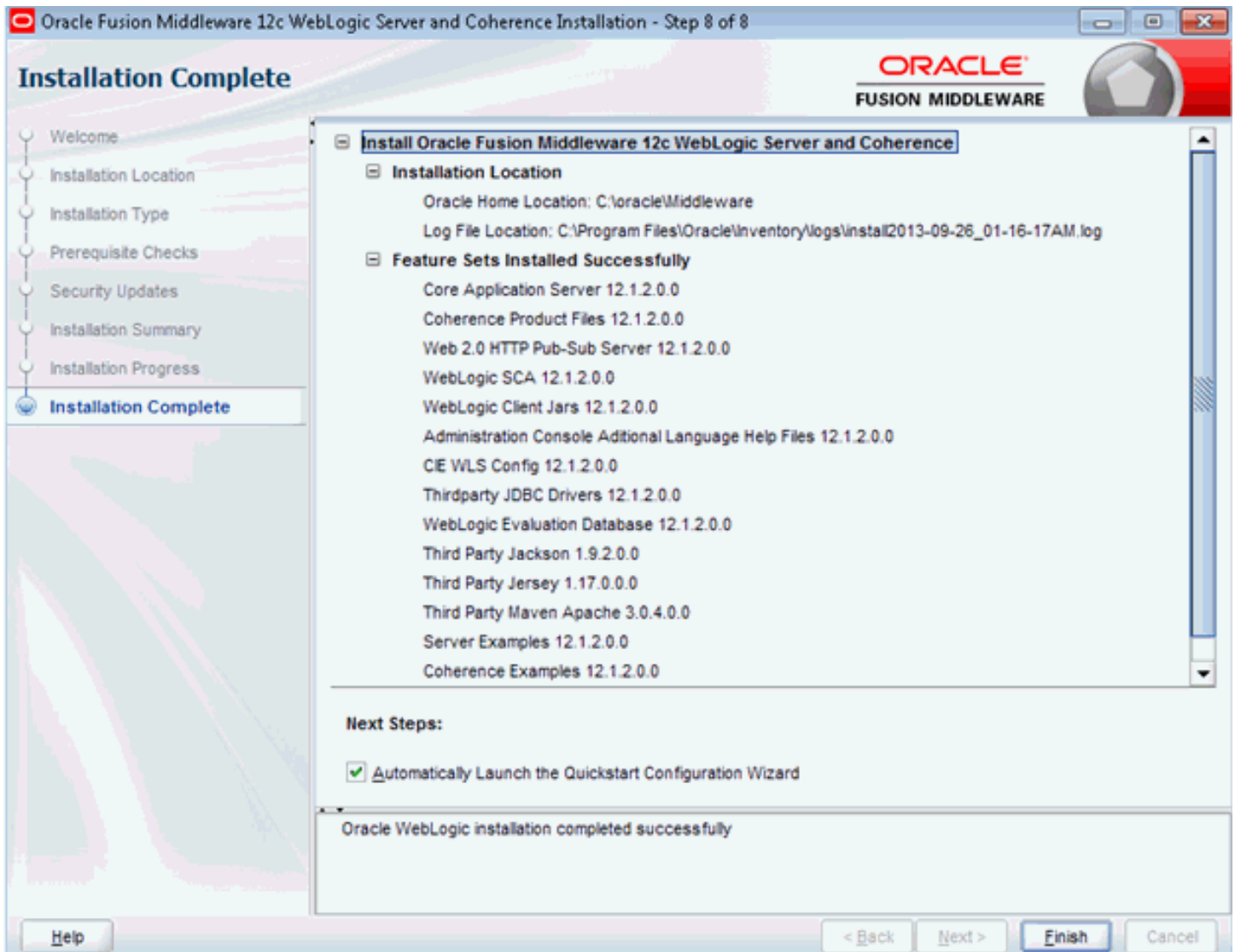
The Installation Summary screen contains a list of the feature sets you selected for installation.

9. Click **Install**.



This screen shows the progress of the installation. When the progress bar reaches 100%, the installation is complete.

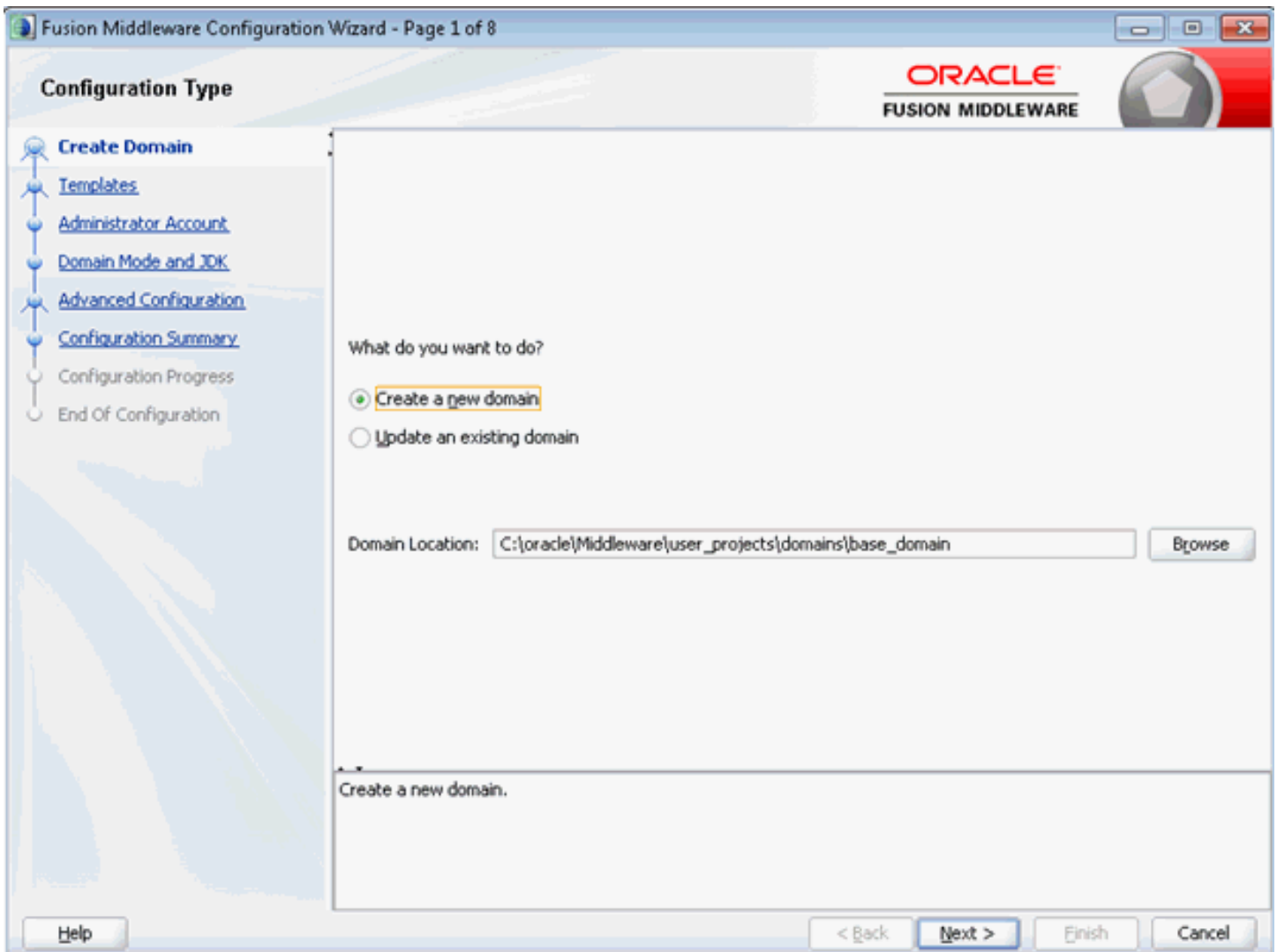
10. Click **Next**.



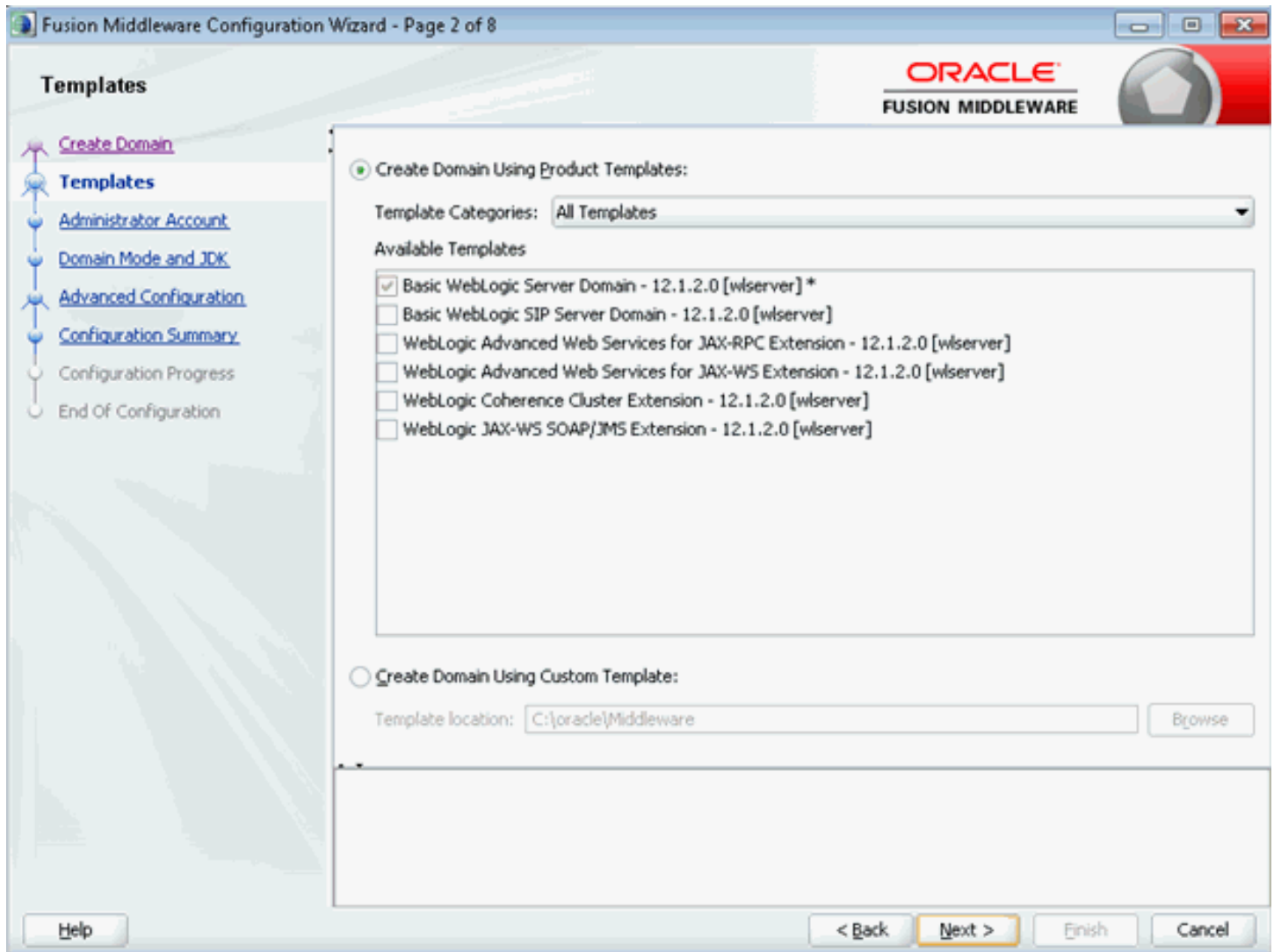
This screen appears at the conclusion of the installation and provides a summary of the products and features that were installed. Click **Finish**.

11. Create a domain using the Configuration Wizard.

Run the Configuration Wizard to create a domain. Configuration Wizard can also be invoked by running the command `< ORACLE_HOME>\oracle_common\common\bin\config.cmd`.



12. Provide the domain location. The domain location is `c:\oracle\Middleware\user_projects\domains\base_domain` and the `base_domain` is the domain name. Click **Next**.



13. Select the template **Basic WebLogic Server Domain** and Click **Next**.

Fusion Middleware Configuration Wizard - Page 3 of 8

Administrator Account

ORACLE
FUSION MIDDLEWARE

Create Domain
Templates
Administrator Account
Domain Mode and JDK
Advanced Configuration
Configuration Summary
Configuration Progress
End Of Configuration

Name:

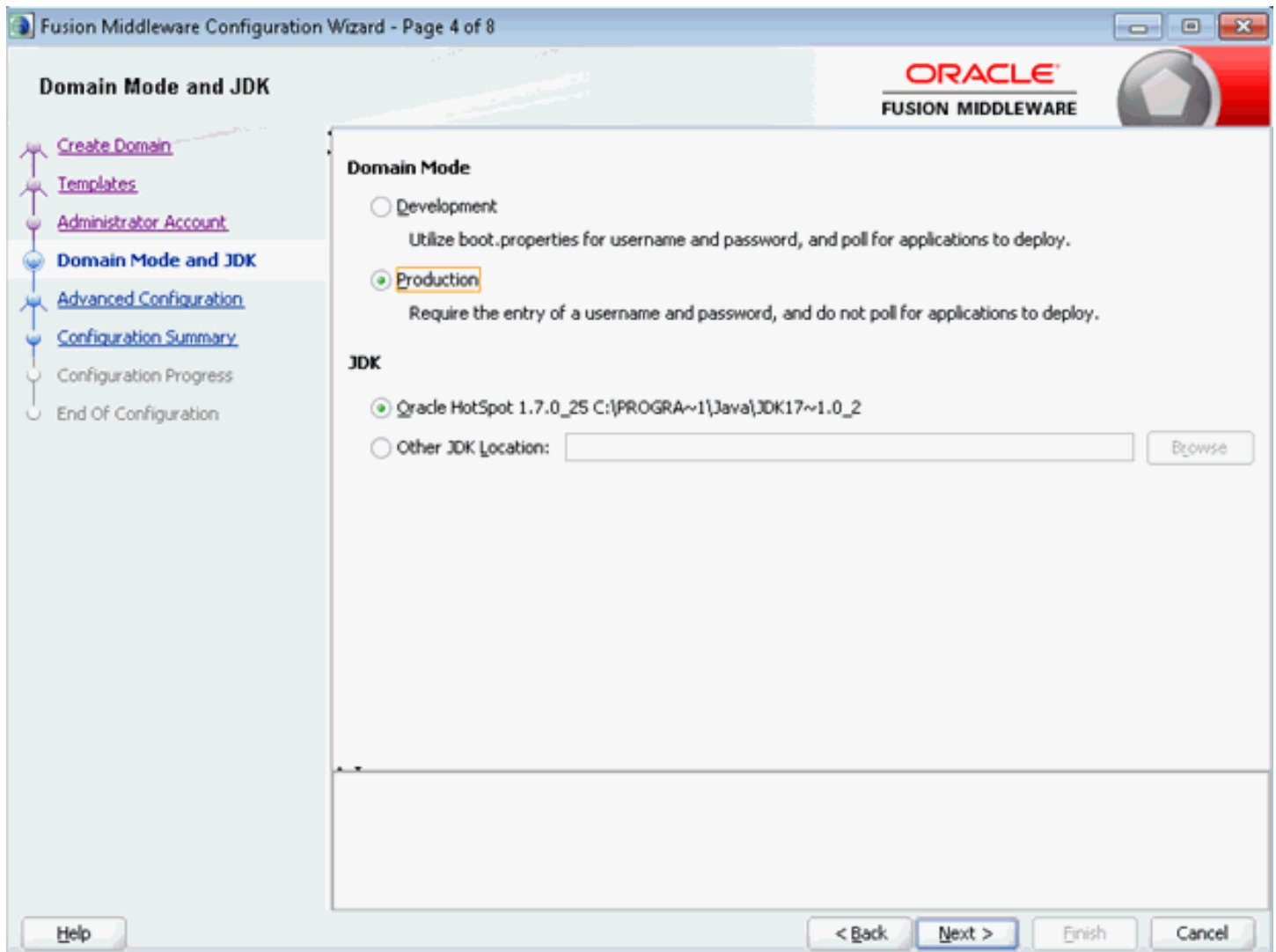
Password:

Confirm Password:

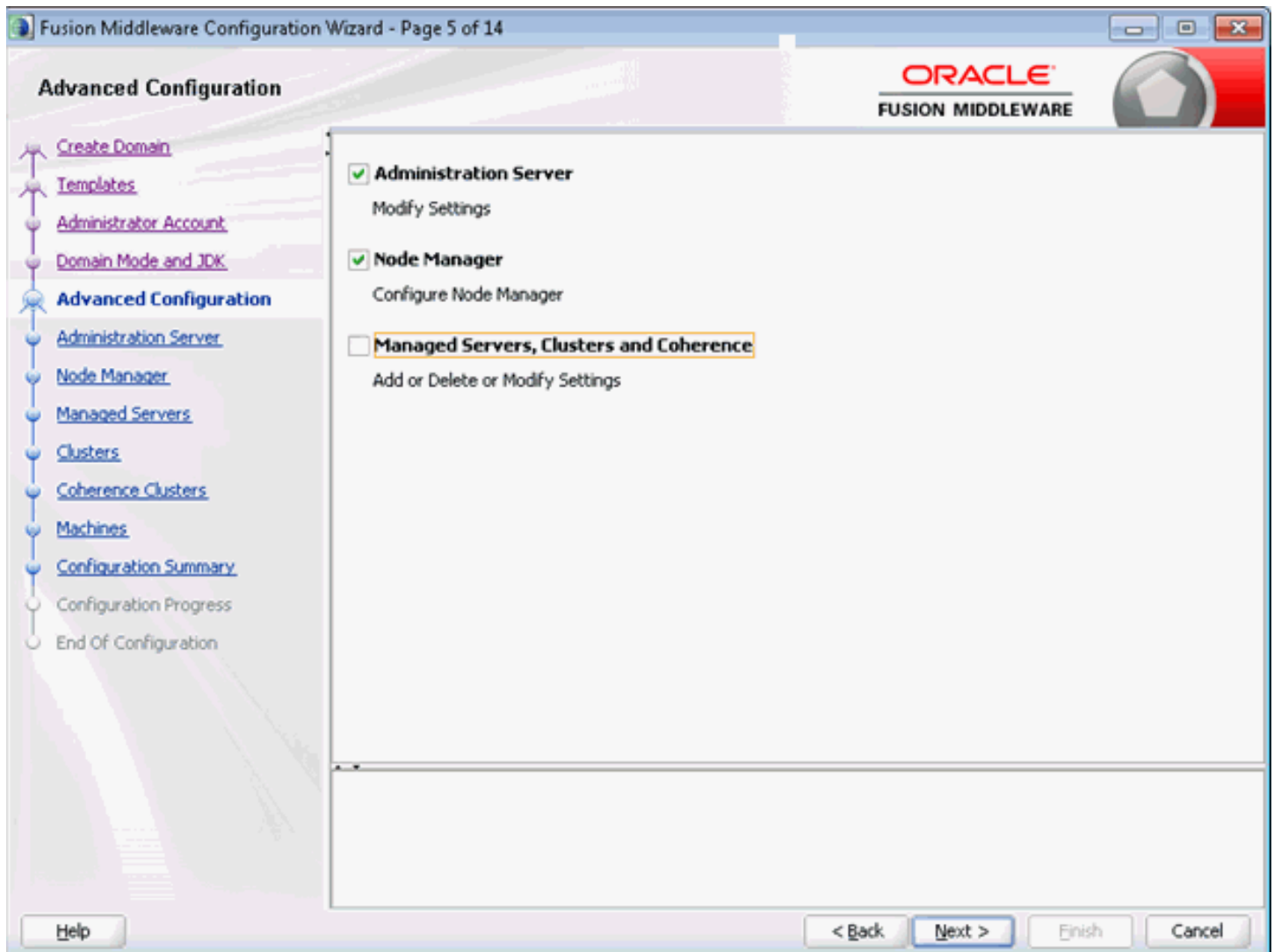
Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.

Help < Back Next > Finish Cancel

14. Provide the Administrative Username/Password for the domain and Click **Next**.



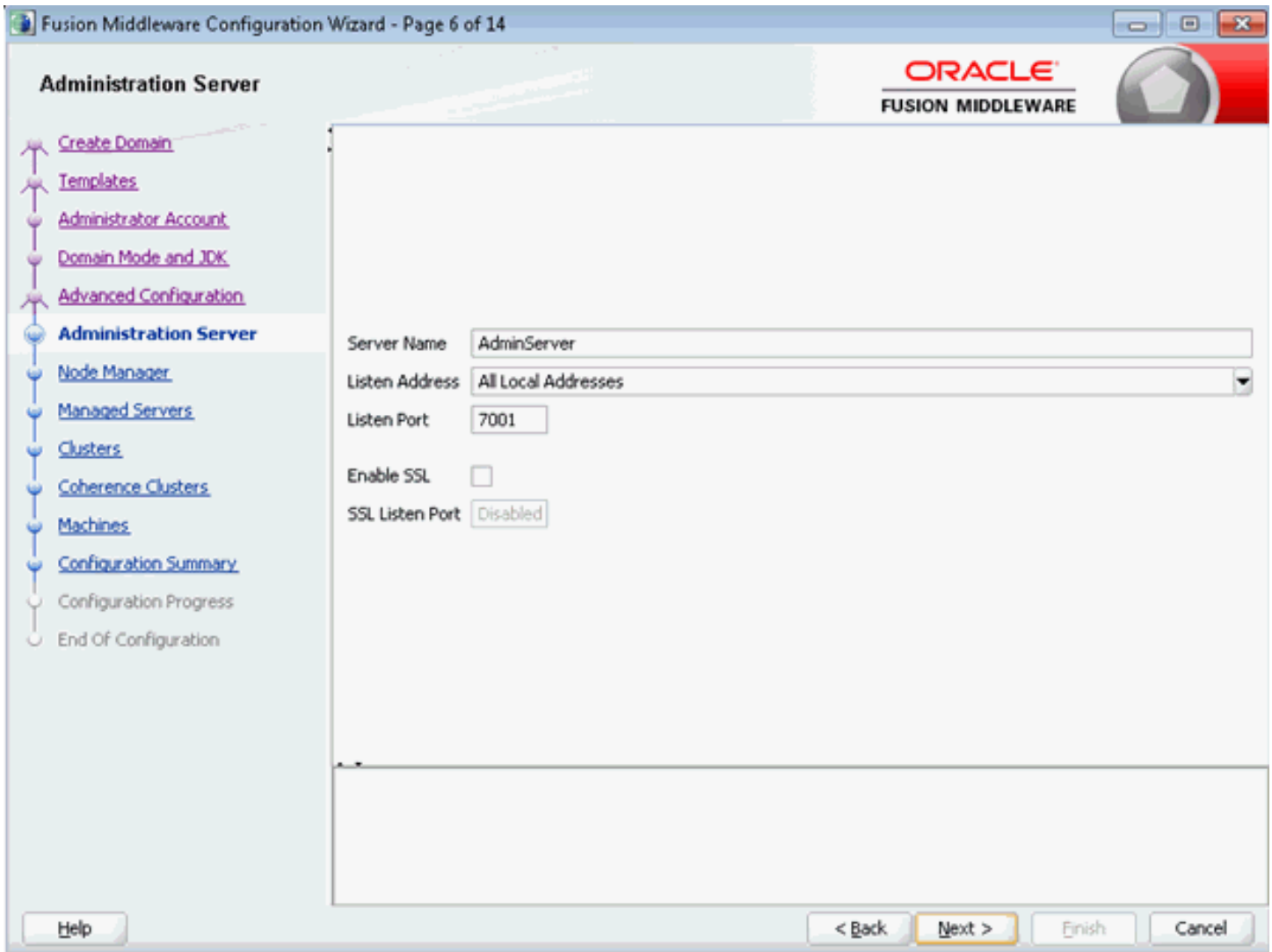
15. On Domain Mode for use with JD Edwards EnterpriseOne, you must select **Production**. JDK Location is selected by default. You can provide any external JDK Location also. Click **Next**.



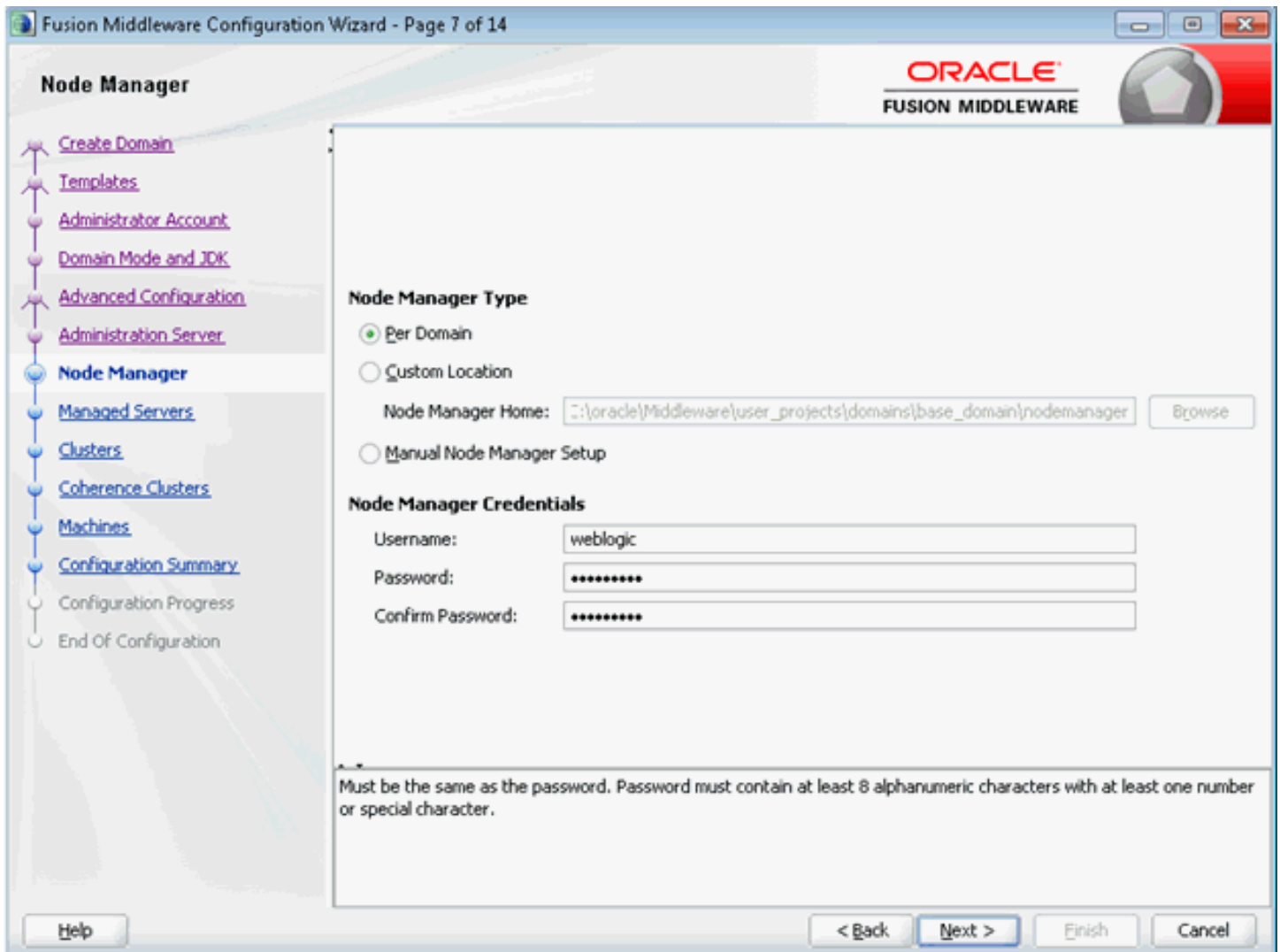
16. On Advanced Configuration, select these check boxes to modify the server settings:

- o Administration Server
- o Node Manager

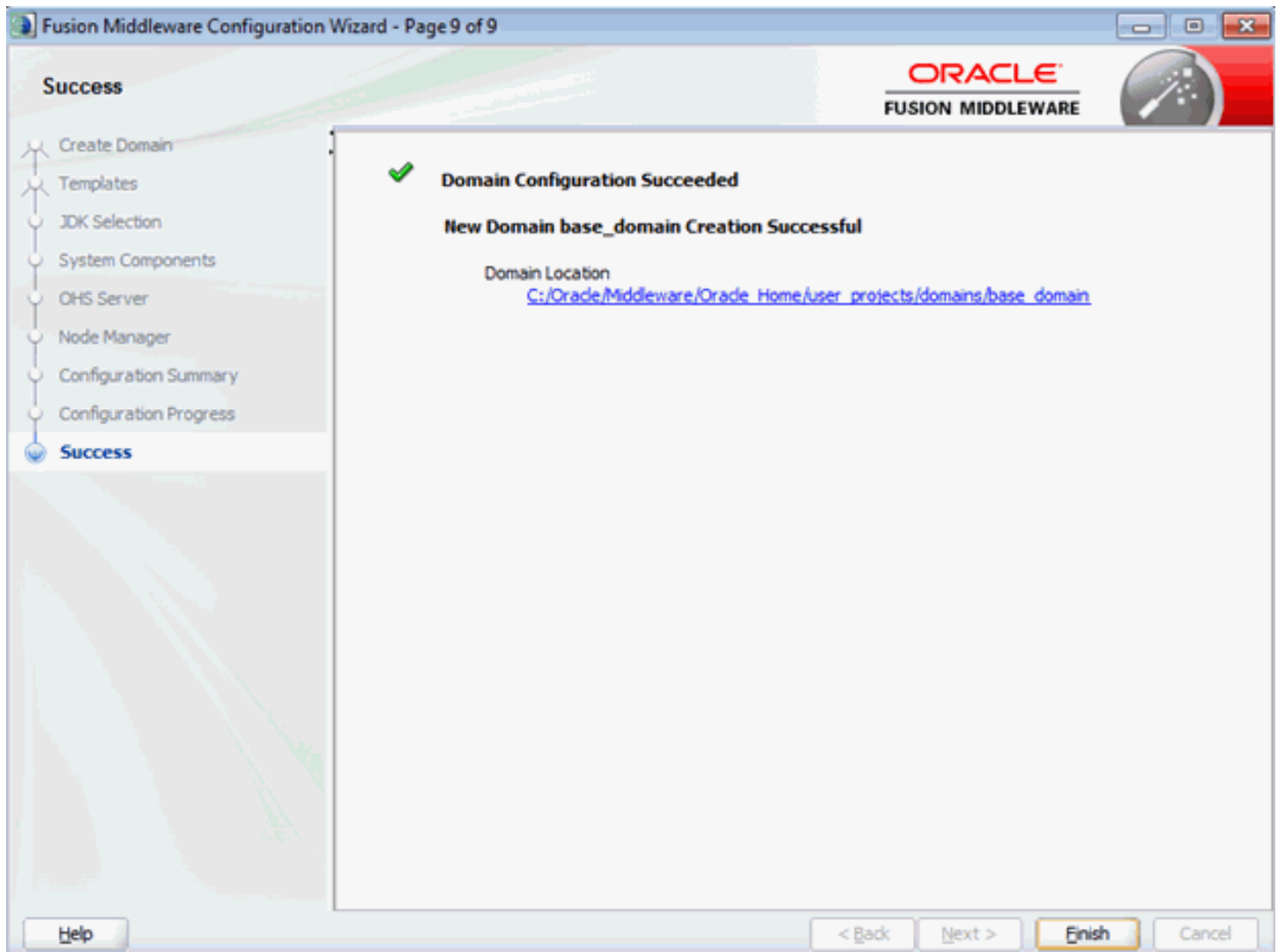
Click **Next**.



17. You may change the Listen Port on this screen. Click **Next**.



18. Select the Node Manager Type as **Per Domain**. Provide Node Manager Username and Password. Configuration Summary is displayed. Click **Create**.



19. Domain creation is successful. Click **Finish**.
20. Start the WebLogic Server. from:

```
<ORACLE_HOME>\user_projects\domains\base_domain\bin\startWebLogic.bat
```
21. Login into the admin console of the domain created in the previous step (i.e. `http://<host>:<domain_port>/console`).
22. Configure the machines. For information on configuring a machine, see:

http://docs.oracle.com/middleware/1213/wls/NODEM/starting_nodemgr.htm#BABJJAGA

23. Start the Node Manager from:

```
<ORACLE_HOME>\user_projects\domains\base_domain\bin\startNodeManager.bat
```

24. Verify whether the nodemanager is reachable or not.

Installing Server Manager Console on WebLogic Server 12.1.2

To install the Server Manager Console, follow the instructions in *Installing the Management Console on WebLogic Server*.

Restoring the Previous Server Manager Console Configurations

If you had server groups setup in the previous Server Manager Console, you can preserve them by copying all the files and folders you had backed up from the previous installation under `<SM_CONSOLE_HOME>\targets\home\config` to the same location after Server Manager is re-installed.

To restore the user's setup in the previous Server Manager Console, you can preserve them copying all the files and folders you had backed up from the previous installation under `<SM_CONSOLE_HOME>\targets\home\security-realm.xml` to the same location after SM is re-installed.

To restore monitors setup in the previous Server Manager Console, you can preserve them copying all the files and folders you had backed up from the previous installation under `<SM_CONSOLE_HOME>\targets\home\monitors.xml` to the same location after SM is re-installed.

To restore history in the previous Server Manager Console, you can preserve them copying all the files and folders you had backed up from the previous installation under `<SM_CONSOLE_HOME>\targets\home\scf-history.xml` to the same location after SM is re-installed.

To restore registered instances in the previous Server Manager Console, you can preserve them copying all the files and folders you had backed up from the previous installation under `<SM_CONSOLE_HOME>\targets\home\management-console.xml` to the same location after SM is re-installed.

After restoring these configurations, you need to restart the Server Manager console to take effect.

2 Install a Server Manager Management Agent

Obtain the Management Agent Installer Application

To obtain the *Management Agent* Installer application:

1. On the Management Dashboard, in the INSTALL section on the left pane titled **What do you want to do?**, click the *Management Agents* link.

The screenshot shows the 'Managed Homes and Managed Instances' page in the Server Manager interface. On the left, a navigation pane titled 'What do you want to do?' contains three sections: 'INSTALL' with links for 'Management Agents', 'Manage Software', and 'Database Drivers'; 'CONFIGURE' with links for 'Server Manager Users' and 'Server Groups'; and 'TRACK' with links for 'User Activity', 'Server Activity', and 'Table Cache'. The main content area has a title 'Managed Homes and Managed Instances' and a dropdown menu set to 'Managed Homes and Managed Instances'. Below this is a table with one entry for a managed home. The table has columns for 'Managed Home Location' and 'Managed Instances'. The entry shows a location 'den00byy.us.oracle.com' with a path 'C:\jde_home_1\SCFMC' and a 'home' instance that is 'Running'.

Managed Home Location	Managed Instances
<input type="checkbox"/> den00byy.us.oracle.com C:\jde_home_1\SCFMC	home Management Console <input type="checkbox"/> Running

2. On the **Server Manager Agent Downloads** page, navigate to the **Management Agent Installers** section.

Management Agent Installers [Return To Top](#)

Download and install the appropriate Server Manager agent installer from the list below. When prompted to enter the server name and port to use for the management console enter the following values:

Management Console Machine Name
dencuxsvr6.us.oracle.com

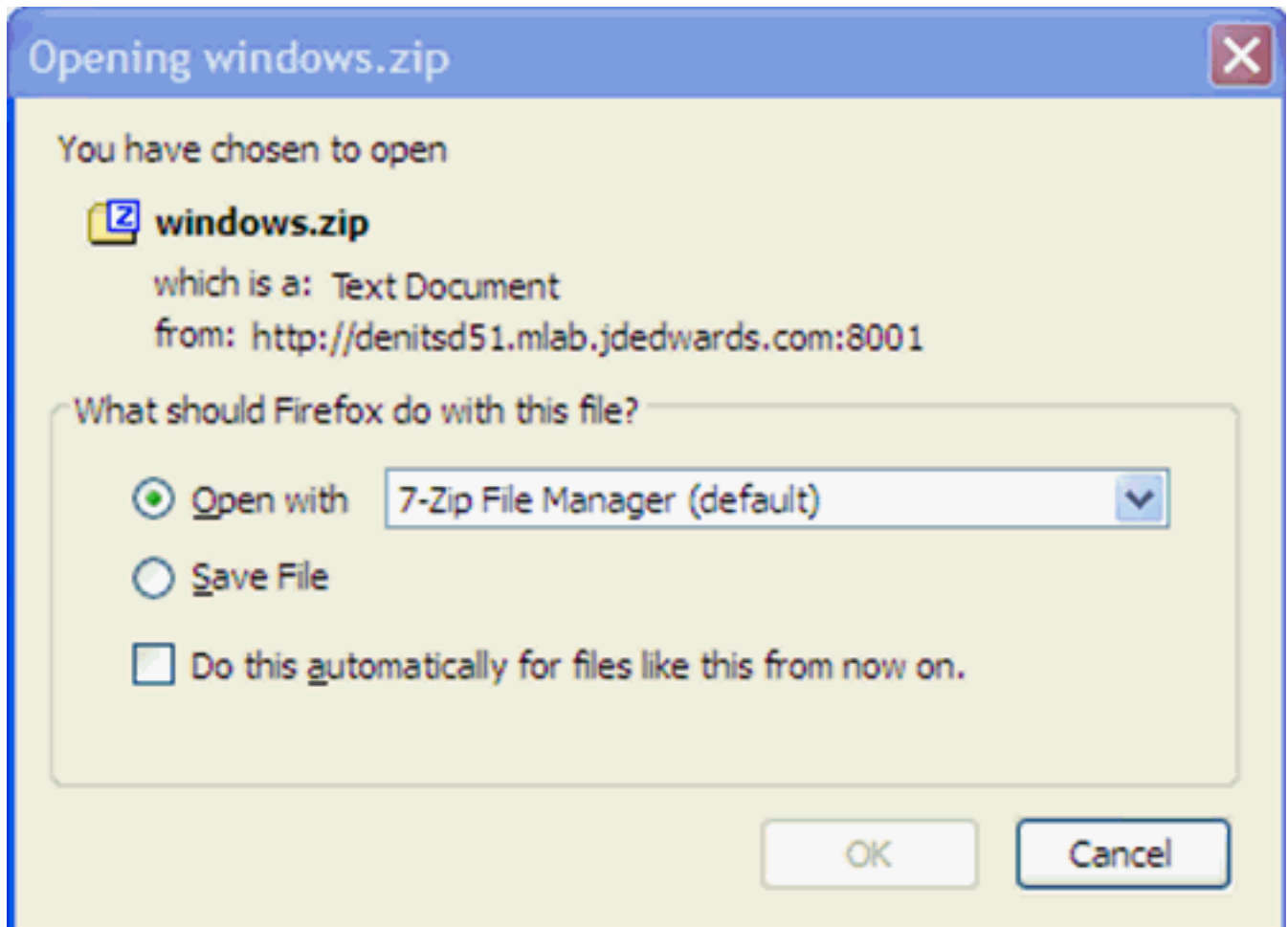
Management Console HTTP Port
8999

Operating System
windows
linux
solaris
aix
hpia64
os400

3. From the **Management Agent Installers** section, you can select from the available Management Agents, which are listed by operating system:
 - o windows
 - o linux
 - o solaris
 - o HP-UX on Itanium (HPIA64)
 - o aix
 - o os400

4. When you click a link to choose an operating system, depending on your browser, you are prompted to **Save** the `.zip` file.

For example, if you select the **windows** Management Agent Installer, you will receive a prompt similar to this:



5. Depending which Management Agent Installer you choose, proceed to the following sections of this chapter entitled: *Distribute and Unzip the Management Agent Installer Application*.

Distribute and Unzip the Management Agent Installer Application

After you have saved the downloaded `.zip` file for the *Management Agent* installer appropriate to your platform, you must move it to the target on which you will run the downloaded installer and unzip it. The move process and the file names are platform-dependent as described in these sections:

- *Microsoft Windows*
- *UNIX*
- *(OS400)*

Note: Some of the functionality described in this topic is to accommodate legacy platforms. Refer to the Oracle Certify System on My Oracle Support for information about currently supported platforms.

Microsoft Windows

Use this procedure to move and unzip the Management Agent Installer.

Note: Depending on the EnterpriseOne Tools Release, Microsoft VC++ 2017, 2013, or 2010 Runtime Libraries x86 and x64 on Windows platforms must be installed on the system before the Server Manager Agent Installer can be executed. The proper Runtime Libraries to install for JD Edwards EnterpriseOne are specified by Oracle Certifications at this link: <https://www.oracle.com/support/index.html>

1. Move this `.zip` file (which you downloaded in the section of this guide entitled: Obtain the Management Agent Installer Application) using Microsoft Windows Explorer with mapped drives:

```
windows.zip
```

2. Extract the `.zip` file to a folder (for example, `c:\SM_Agent`). If you extracted into the example folder, the structure would look like this:

```
C:\SM_Agent\Disk1\install
```

```
C:\SM_Agent\Translations
```

UNIX

These are the available versions of UNIX:

- Linux
- Solaris
- AIX
- HP-UX on Itanium (HPIA64)

CAUTION: Oracle User ID. You must login to the UNIX machine with an Oracle user ID; otherwise you cannot run the installer.

Use this procedure to move and unzip the Management Agent Installer.

1. Move this `.zip` file (which you downloaded in the section of this guide entitled: Obtain the Management Agent Installer Application) using FTP services:

Linux

```
linux.zip
```

Solaris

```
solaris.zip
```

AIX

```
aix.zip
```

HP-UX on Itanium

`hpia64.zip`

2. Extract the `.zip` file to a folder, resulting in the following subfolders:

```
\Disk1\install  
\Translations
```

IBM i(OS400)

CAUTION: You cannot run the OS400 Management Agent installer directly on the *IBM i* machine. Therefore you must download and extract the Management Agent Installer file on a Microsoft Windows machine as described in this procedure. Likewise, you must run the Management Agent installer on a Windows machine, as described later in this section in the topic entitled: *Run the Management Agent Installer*.

1. Move this `.zip` file (which you downloaded in the section of this guide entitled: *Obtain the Management Agent Installer Application*) using Microsoft Windows Explorer to a machine that can access your IBM i OS400 machine with mapped drives:

`os400.zip`

2. Extract the `.zip` file to a folder (for example, `c:\SM_Agent`). If you extracted into the example folder, the structure would look like this:

```
C:\SM_Agent\Disk1\install  
C:\SM_Agent\Translations
```

Run the Management Agent Installer

Running the *Management Agent* installer is platform-dependent:

- *Microsoft Windows*
- *UNIX*
- *(OS400)*

Microsoft Windows

To install the Server Manager Agent on Microsoft Windows target machines:

1. Log on to the machine onto which you are installing the Server Manager Management Agent.
2. Change to the directory in which you extracted the Server Manager Agent installer as described in the subsection of this chapter entitled: *Distribute and Unzip the Management Agent Installer Application*.
3. Depending on your Tools release, launch the OUI installer according to these notes:

Note:

- **For Tools Release 9.2.3.3 and Greater:** Microsoft Visual Studio 2017 and 2013 64-bit Redistributables must be installed prior to running the Server Manager Console installer.
- **For Tools Releases prior to 9.2.3.3:** Microsoft Visual Studio 2010 32-bit Redistributables must be installed prior to running the Server Manager Console installer.
- **For Tools Release 9.2.2.0 and Greater:** A 64-bit JDK or JRE, version 1.8 or later must be installed before starting the Server Manager Agent installer.
- **For Tools Releases prior to 9.2.2.0:** A JDK is included in the installer. Therefore, a separate JDK is not required.

Note: One of the following requirements must be met:

- **For Tools Release 9.2.3.3 and Greater:** You must specify the location of the JDK or JRE on the command line. If the location is not specified, the installer will fail immediately.
- **For Tools Release 9.2.2.0 up to but not including 9.2.3.3:** You can specify the location of the JDK or JRE on the command line. If the location is not specified, you will be prompted for it.
- **For Tools Releases prior to 9.2.2.0:** Because a JDK is included in the installer, you will not be prompted for one.

To specify the location of a JDK or JRE on the command line:

1. Open a Windows Command window with **Run as administrator**.
2. Change directory (cd) to the directory in which you unzipped the installer. For example, if you followed the recommendation in *Distribute and Unzip the Management Agent Installer Application* the command would be:

```
cd C:\SM_Agent\Disk1\install
```

3. Use this command to run `setup.exe` followed by the argument `-jreLoc` and the directory to the JDK or JRE:

```
setup.exe -jreLoc C:\PROGRA~1\Java\JRE18~1.0_1
```

Note: Regarding the above command:

- Include a space after the `-jreLoc` argument.
- The path to the JDK or JRE must be of the Windows short form, which is 8 + 3 format.
- The specified JDK or JRE directory must contain this directory and executable:

```
bin\java.exe
```

To skip specifying the location of a JDK or JRE on the command line:

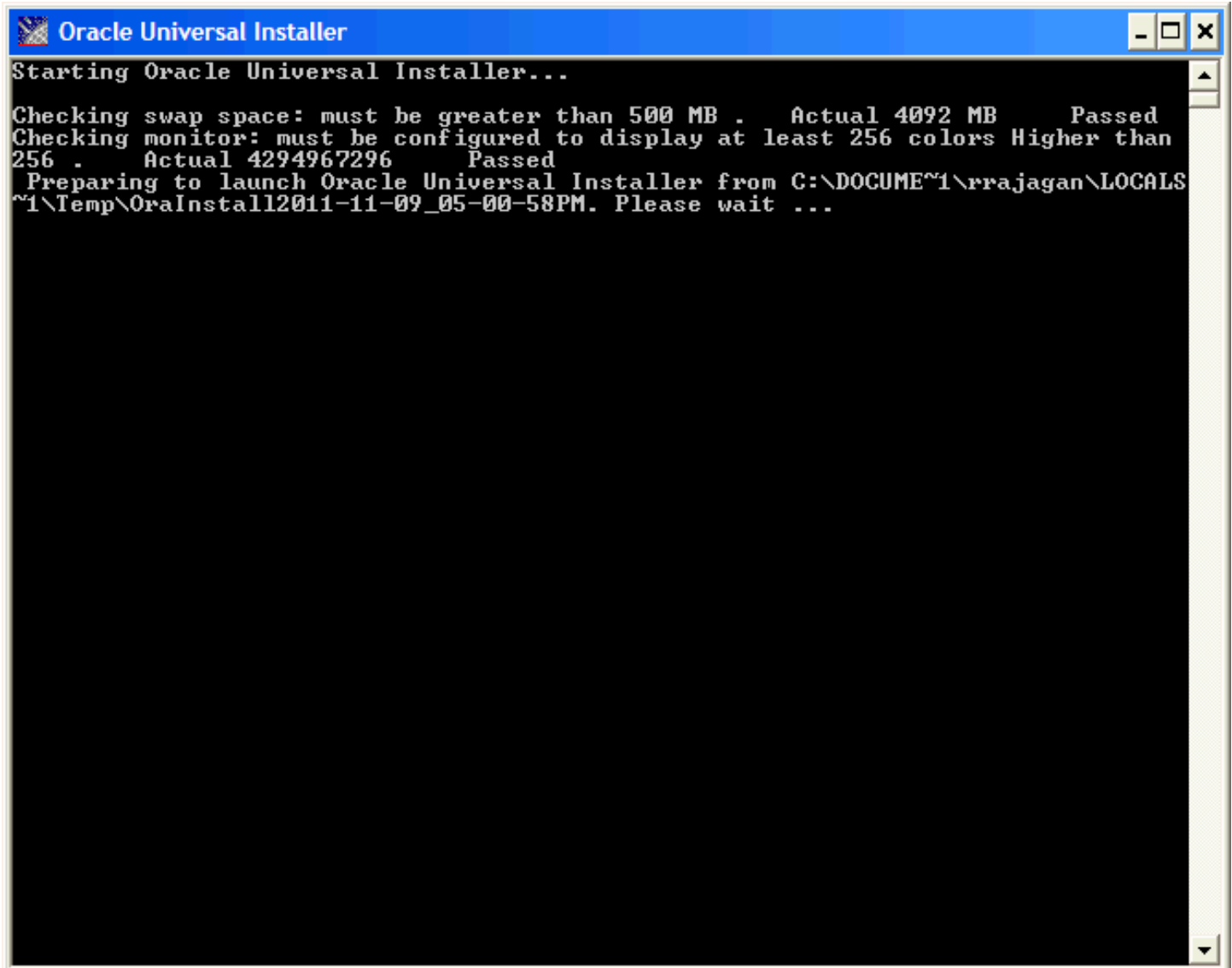
Do one of the following:

1. Follow the instructions above to run from a Windows Command window but without the `-jreLoc` argument.

2. In Windows Explorer, right-click on `setup.exe` in the directory in which you unzipped the installer and select **Run As Administrator**. For example, if you followed the recommendation in *Distribute and Unzip the Management Agent Installer Application* the file will be located in this directory:

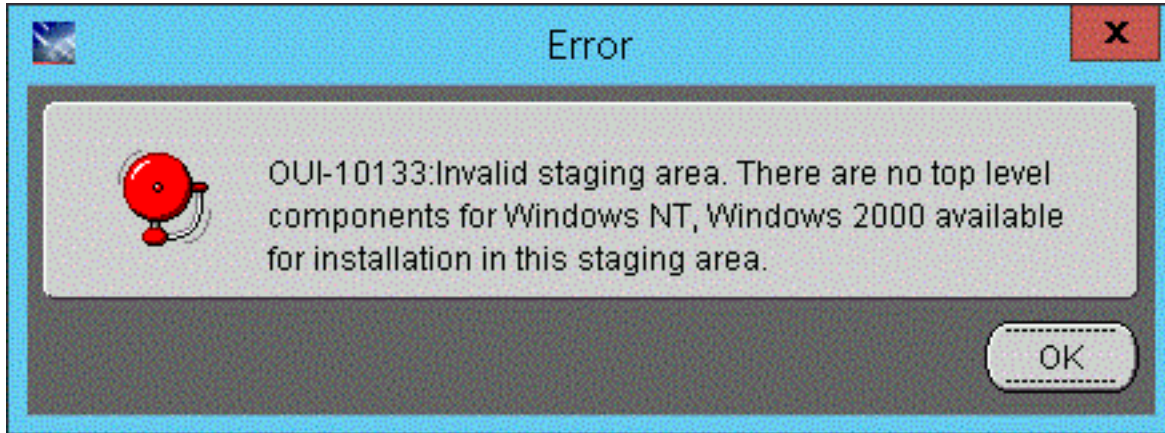
`C:\SM_Agent\Disk1\install\setup.exe`

This process opens a Microsoft Windows command window as shown in the below example.

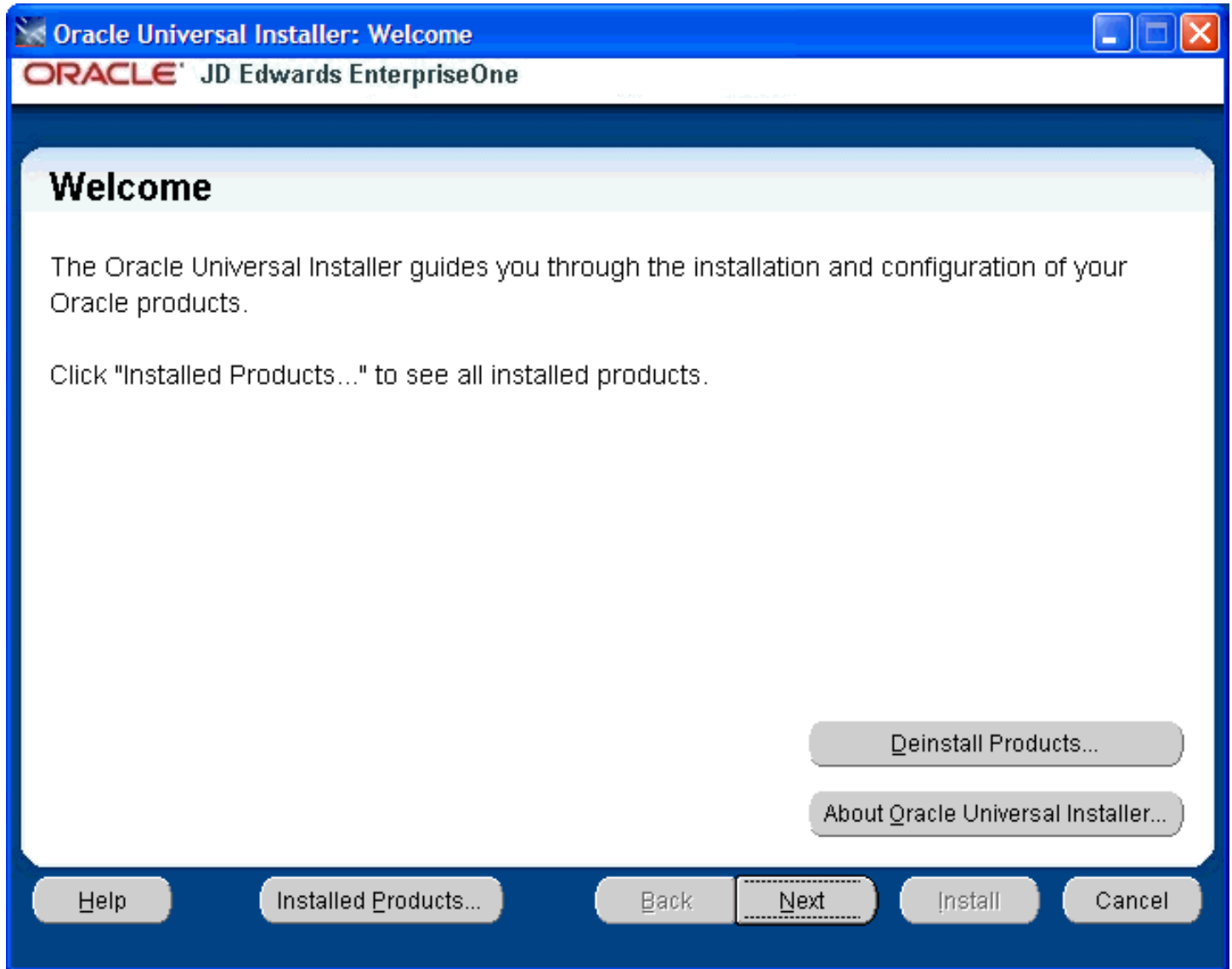


Tools Release 9.2.2.0 up to but not including 9.2.3.3. If you did not specify the location of a JDK or JRE using the `-jreLoc` argument, the installer prompts you to specify the location of that at a command prompt.

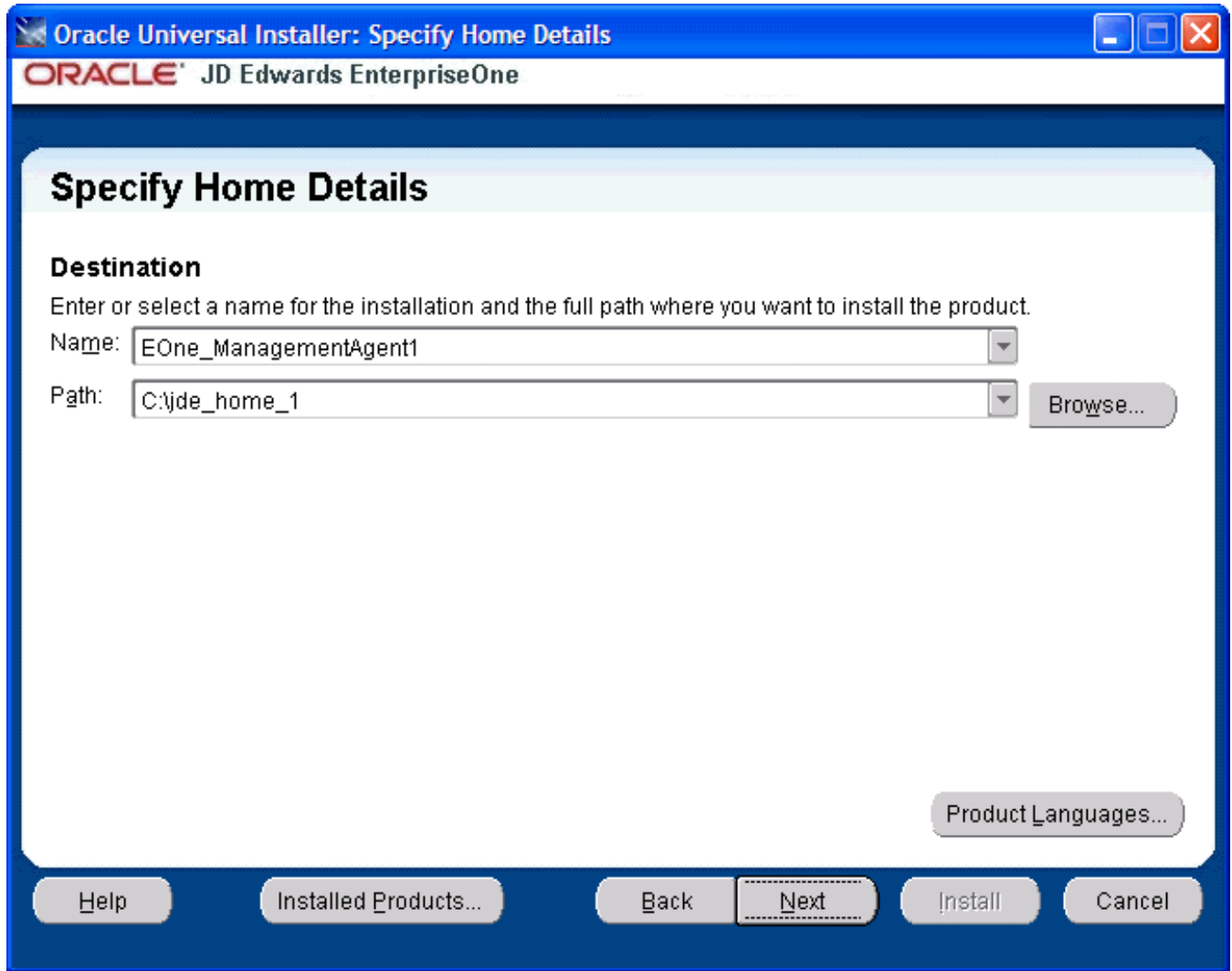
Note: For the 9.2.2.0 and greater, the installer will fail if the JDK/JRE is not at least Version 1.8. Upon failure it displays the following error:



After the installer validates existence of the JDK in the specified location, the OUI installer user interface appears. All further installer behavior remains the same as previous Tools Releases.



1. On Welcome, click the **Next** button.



2. On Specify Home Details, complete these fields:

- o *Name:*

Enter a name for the Management Agent. The default name is:

EOne_Management_Agent

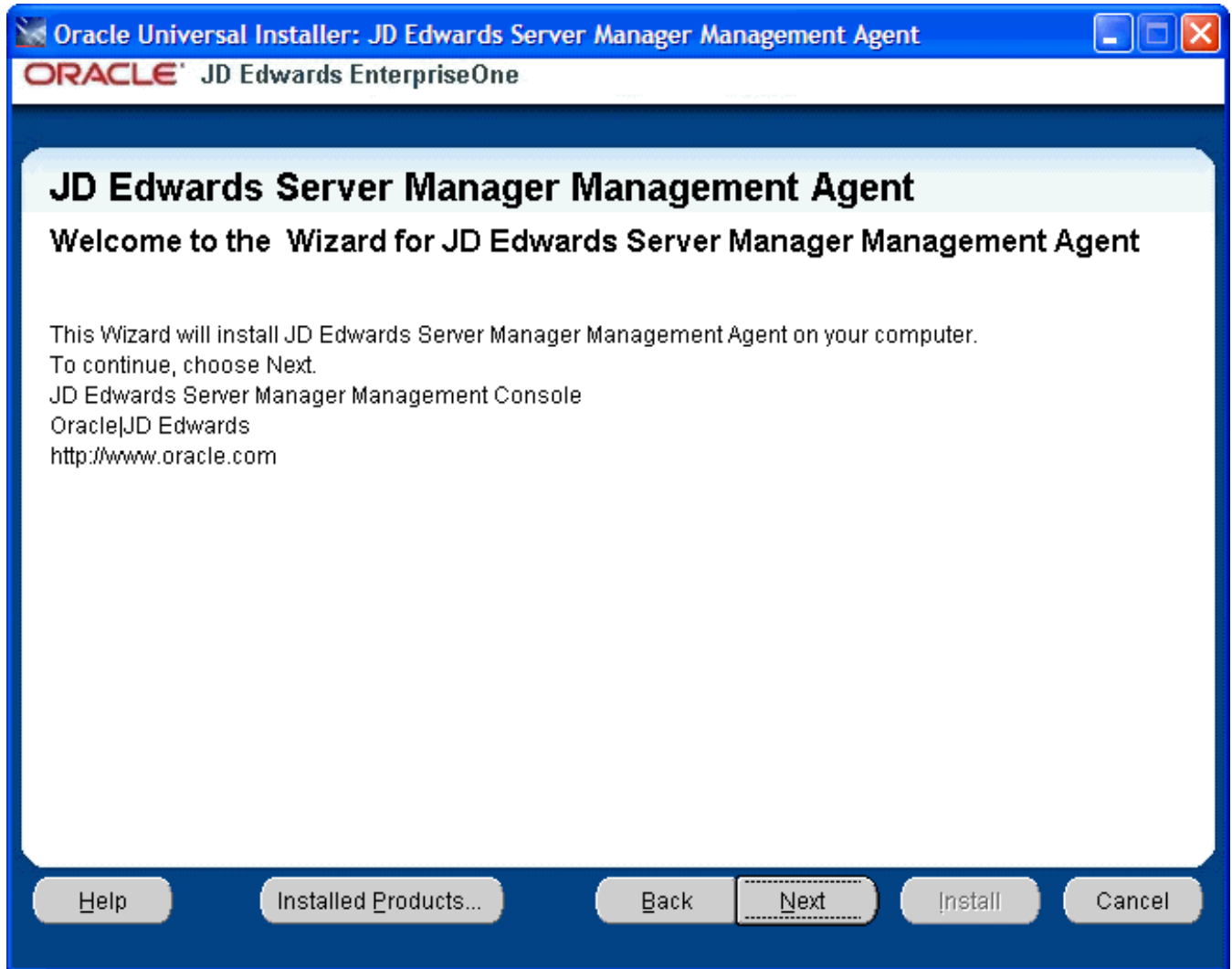
- o *Path:*

The installer automatically detects the root drive location on the Microsoft Windows machine and by default appends this value:

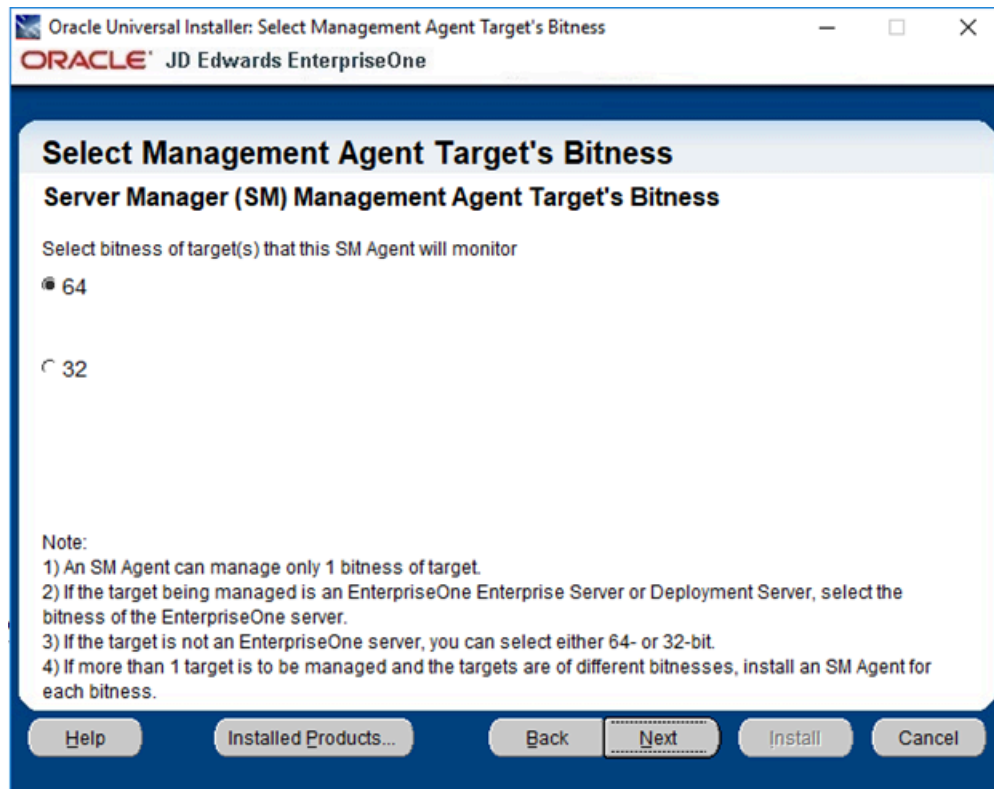
`jde_home`

Note: Although **jde_home** is the default and recommended setting, you can specify any value to replace the default value.

The directory that you specify cannot already exist.



3. On Welcome to the Wizard for JD Edwards Server Manager Management Agent, click the **Next** button.

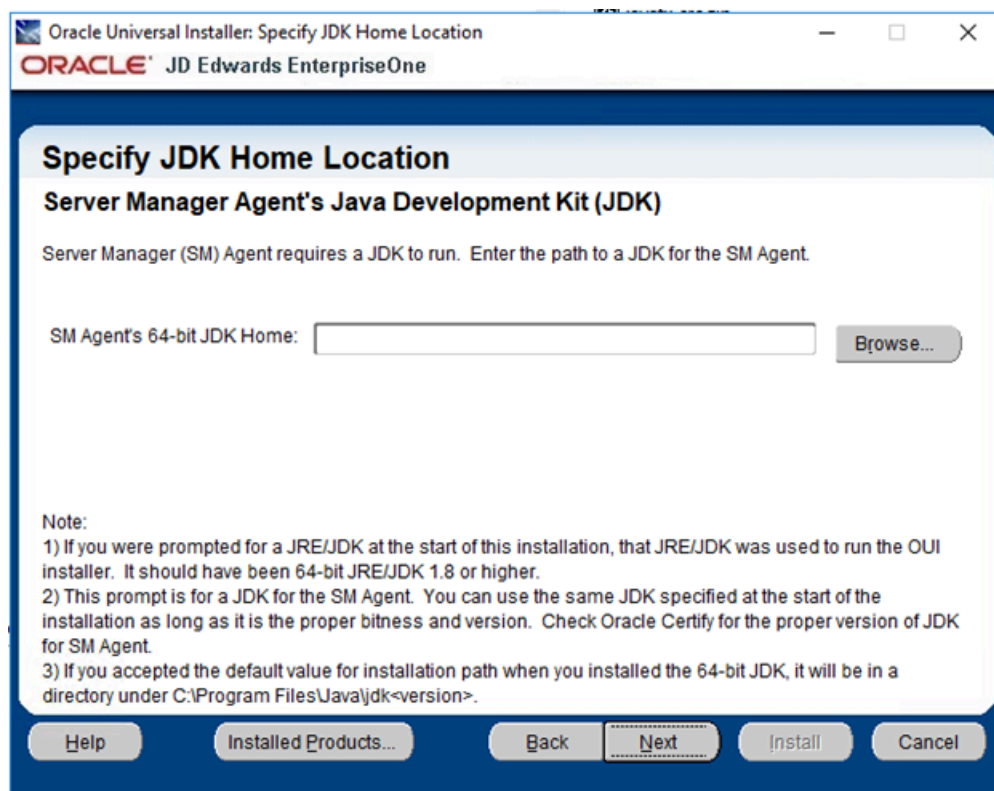


4. On Select Agent Target's Bitness, select the bitness of the targets that the Server Manager Agent will monitor and click the **Next** button.

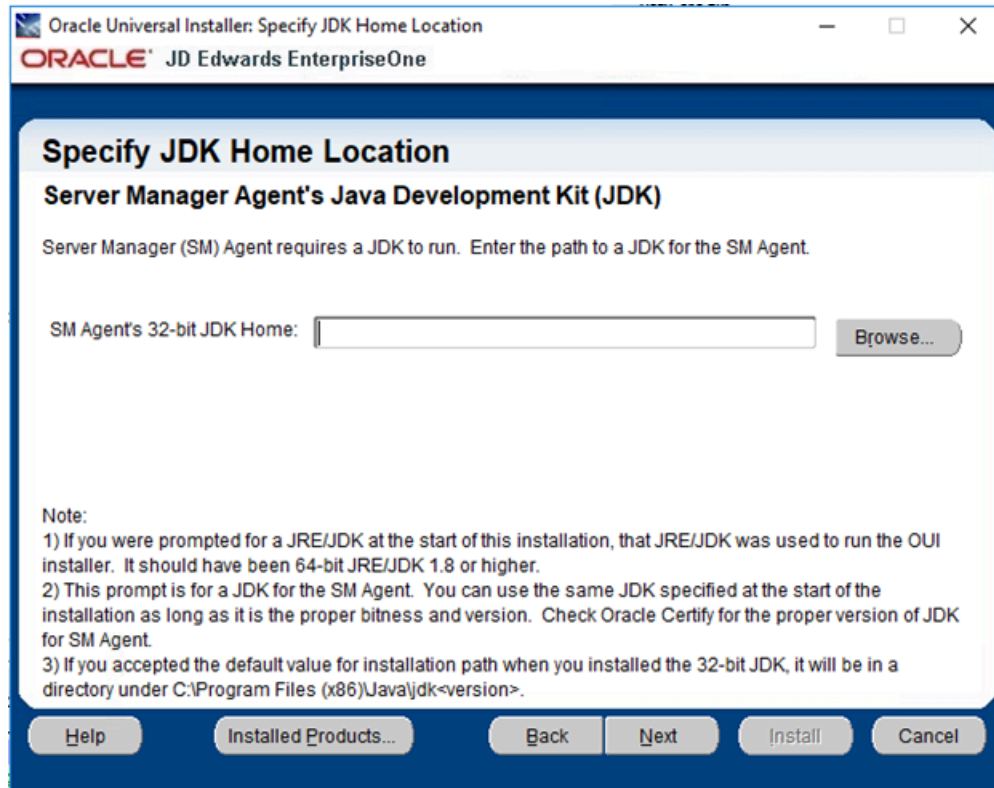
Note: These considerations apply to bitness:

- o Each Server Manager Agent can manage only a single bitness of target objects. That is, it cannot manage multiple objects if the objects are a mixture of 32-bit and 64-bit bitness.
- o If the target being managed is a JD Edwards EnterpriseOne Enterprise Server or Deployment Server, select the bitness of the EnterpriseOne server.
- o If the target is not an EnterpriseOne server, you can select either 64-bit or 32-bit.
- o If more than one target is to be managed and the targets are of different bitnesses, you must install a Server Manager Agent for each bitness.

If **64** is selected, then this 64-bit JDK Home screen will appear:



If **32** is selected, then this 32-bit JDK Home screen will appear:



5. On Specify JDK Home Location and in the **JDK Home** field, enter or browse to the location of your Java Development Kit (JDK). In order to proceed, you cannot leave this value blank and you must specify an existing valid location. If you accepted the default path when you installed the JDK, it will be in a directory under this path:

`c:\Program Files\Java\jdk<version>` (64-bit JDK)

`c:\Program Files (x86)\jdk<version>` (32-bit JDK)

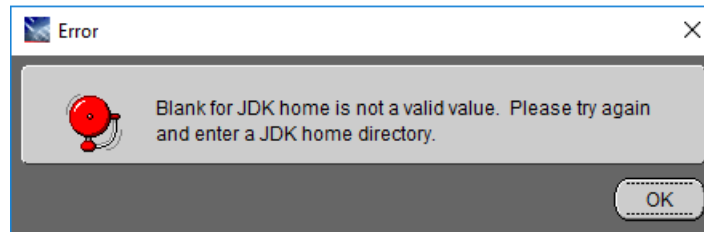
Note: These considerations apply to the JDK:

- The JRE/JDK that you specified at the start of this installation was used to run the OUI installer. For Tools Release 9.2.2.0 and greater, it should have been a 64-bit JRE/JDK 1.8 or higher.
- This prompt is for a JDK that the Server Manager Agent will use. You can use the same JDK specified at the start of the installation as long as it is the proper bitness and version.

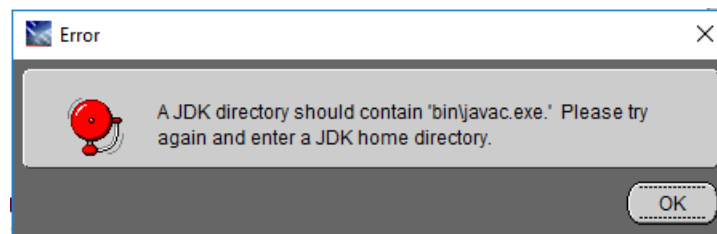
The installer validates the specified location and copies the JDK to a location where it can be used by the runtime processes of JD Edwards EnterpriseOne.

6. Enter the appropriate JDK path and click the **Next** button. This JDK is a prerequisite to installing JD Edwards Enterprise and must meet the supported version as specified by the Oracle certifications.

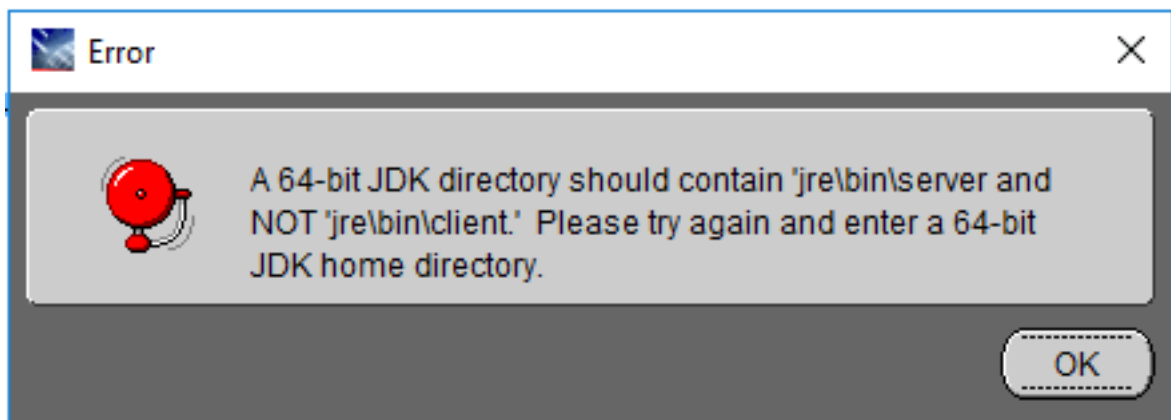
CAUTION: If the **JDK Home** field is left blank and the **Next** button is selected, the following error will occur.



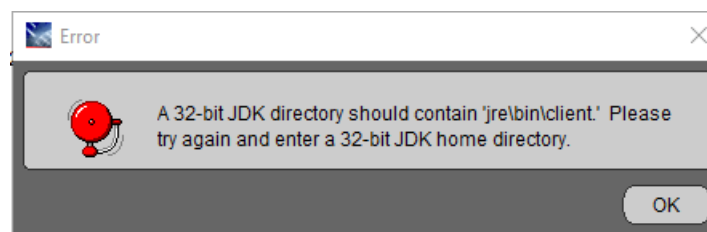
If a path to a non-existent JDK is entered in the **JDK Home** field and the **Next** button is selected, the following error will occur.



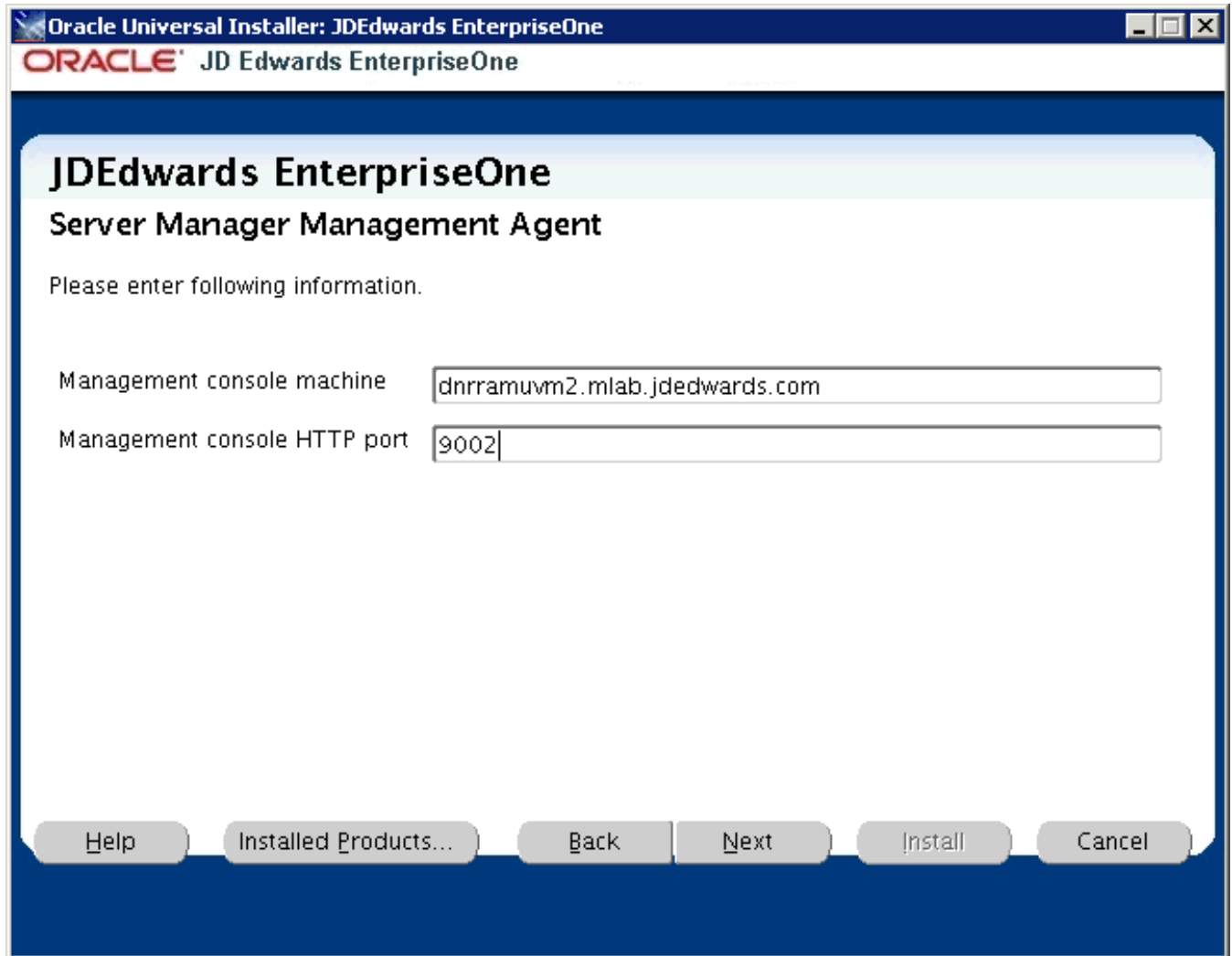
If a 64-bit target was selected and a 32-bit JDK directory was entered, the following error will occur.



If a 32-bit target was selected and a 32-bit JDK directory was entered, the following error will occur.



After the JDK location is validated, the Server Manager Management Agent screen is displayed.



7. On Server Manager Management Agent, complete these fields:

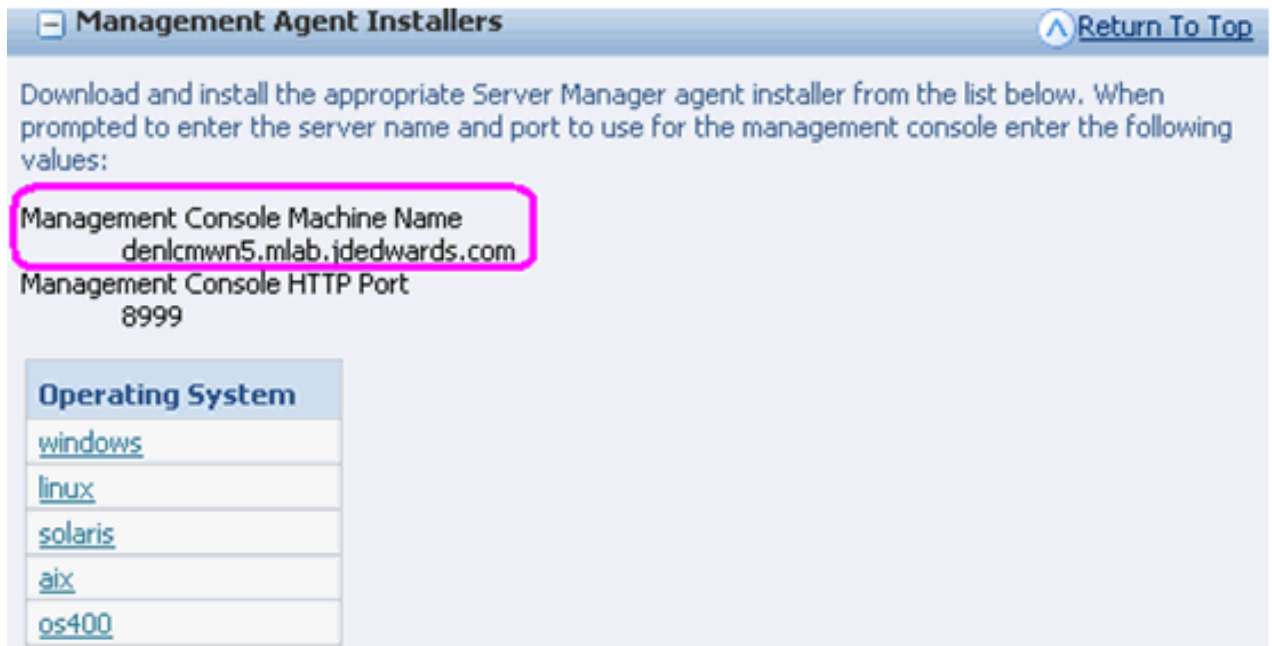
- o *Management console machine*

You must specify the host name of an existing *Management Console* machine.

The installer verifies the connection to the *Management Console* during the install. The *Management Console* machine must be started and the *Management Console* must be running in order to run the installer. In some cases, depending on your machine, operating systems, or network, you might need to

fully qualify your machine name. For example, instead of specifying only `dnrramuv2` you might need to specify `dnrramuv2.mlab.jdedwards.com`.

Tip: You can determine the name of your *Management Console* from the information supplied on the **Management Agent Installers** screen. For navigation, refer to Step 2 in the section entitled: *Obtain the Management Agent Installer Application*. You can also view the `readme.txt` file in the root directory of the *Management Console*.



- o *Management console HTTP port*

You must specify a valid port of an existing *Management Console* machine.

The installer verifies the port connection to the *Management Console*. The machine must be started and the *Management Console* must be running in order to run the installer.

Tip: You can determine the port of your *Management Console* from the information supplied on the **Management Agent Installers** screen. For navigation, refer to Step 2 in the section entitled: *Obtain the Management Agent Installer Application*.

Management Agent Installers [Return To Top](#)

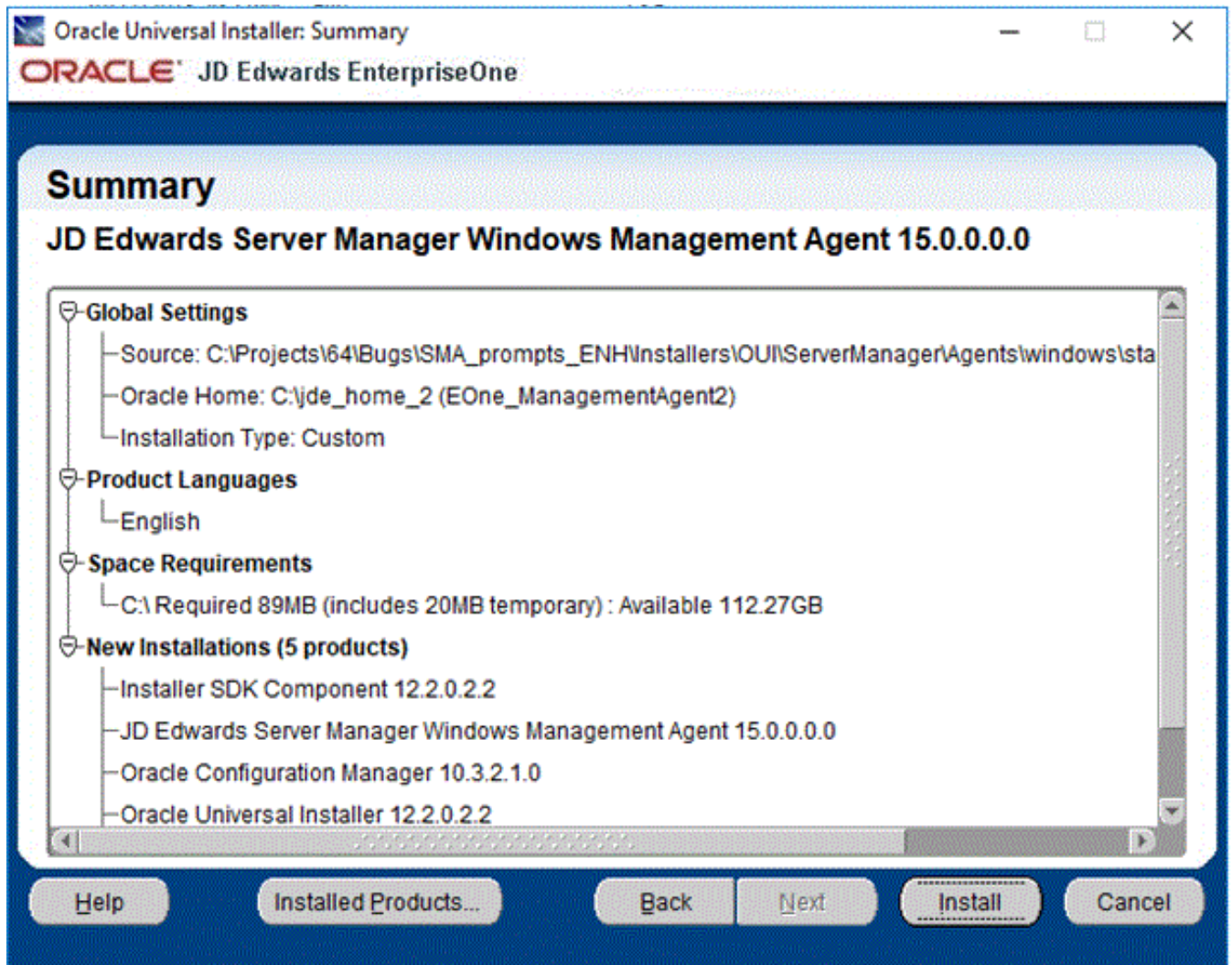
Download and install the appropriate Server Manager agent installer from the list below. When prompted to enter the server name and port to use for the management console enter the following values:

Management Console Machine Name
donlcmwne.mlab.jdedwards.com

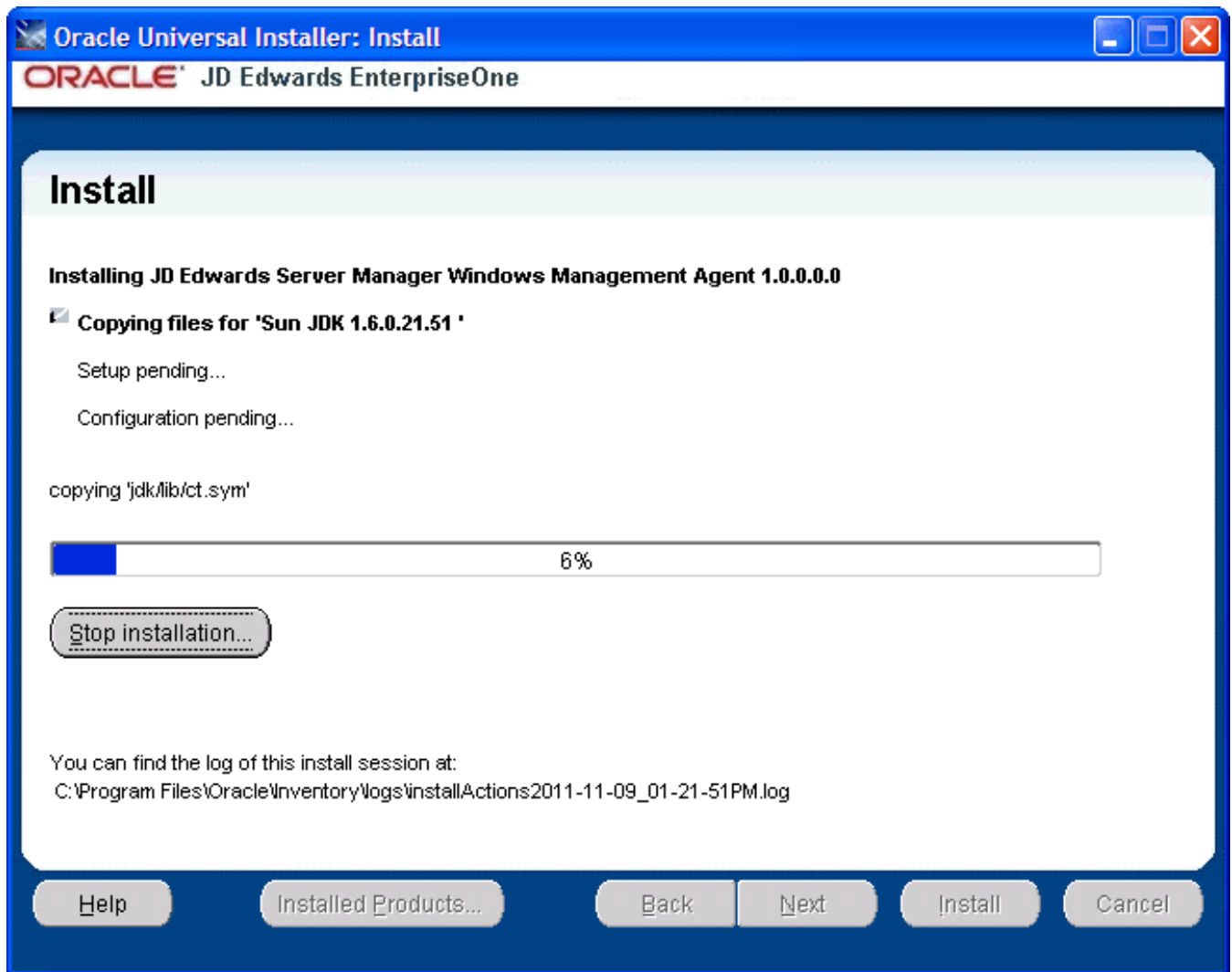
Management Console HTTP Port
8999

Operating System
windows
linux
solaris
aix
os400

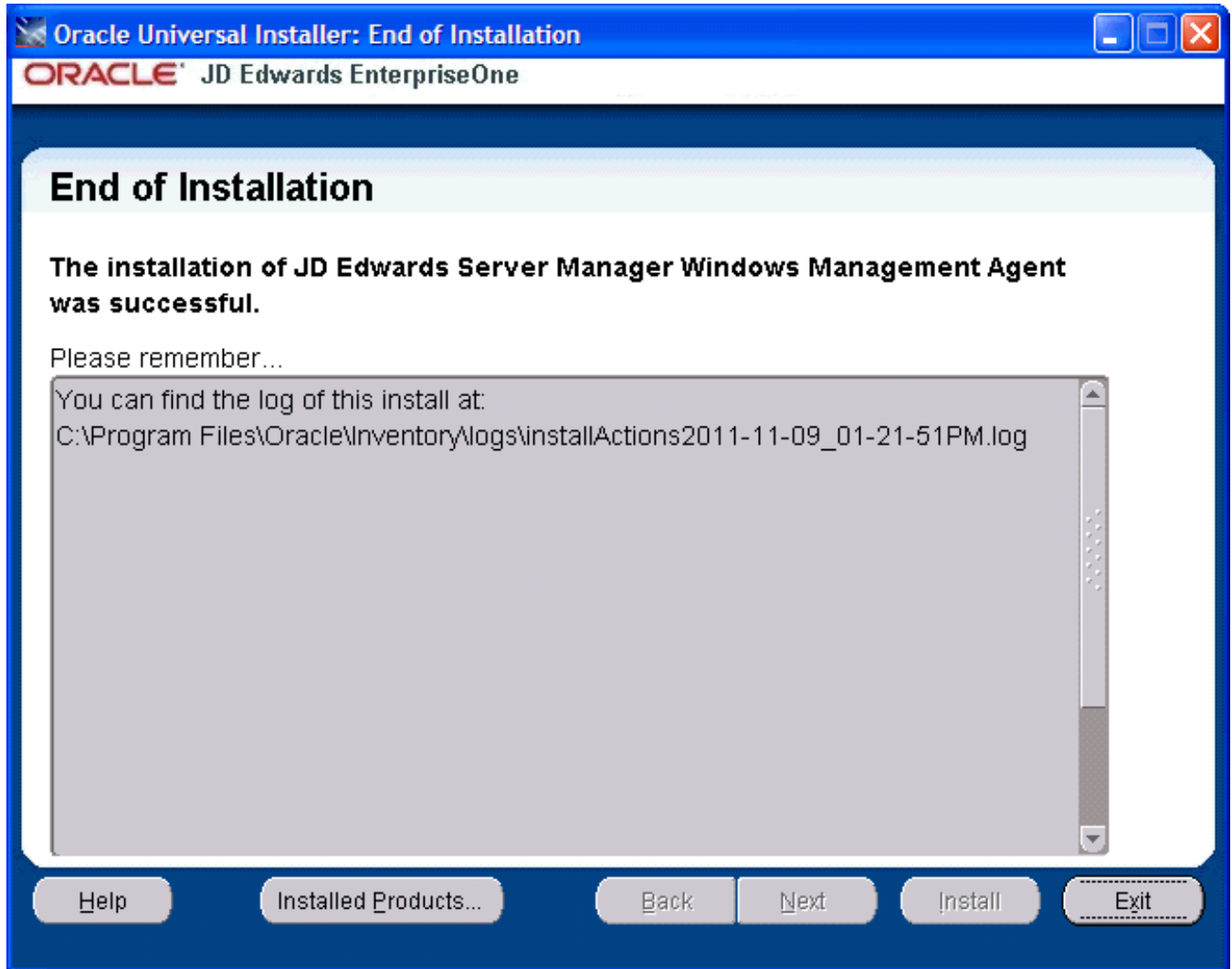
8. Click the **Next** button to verify the machine and port values.



9. On Summary, review the information and click the **Install** button to begin the installation.



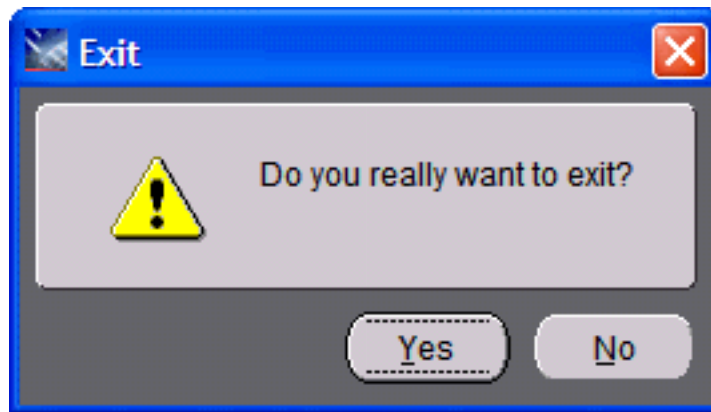
The Management Agent installer displays a panel showing the ongoing status of the installation.



10. When the installation finishes, the End of Installation screen is displayed.

CAUTION: Examine the Installer Logs. This screen also displays the location of the install log. Even though the screen indicates that the installation was successful, you should always check the logs before you attempt to run the Agent. The file name starts with "installActions" and includes a time stamp; it is located in c:\oraInventory\logs directory. For example: cc:\Program Files\Oracle\Inventory\logs\installActions2018-11-09_01-21-51PM.log

11. Click the **Exit** button.



12. On the Exit dialog, click the **Yes** button to confirm you want to exit the Management Agent installer.

Note: After a successful installation, the *Management Agent* automatically starts and connects to the *Server Manager Management Console*. The resulting newly installed *Managed Home* can be viewed in the *Management Dashboard* of the *Management Console*.

UNIX

These are the available versions of the *Management Agent* installers for UNIX:

- Linux
- Solaris
- AIX
- HP-UX on Itanium (HPIA64)

Before launching the *Management Agent* installer on UNIX platform, you should review these important notes as applicable to your installation and *Server Manager* environments:

- [Permissions](#)
- [/tmp location](#)
- [Oracle User ID](#)
- [Management Agent on the Application Server](#)
- [Enterprise Server](#)
- [Graphic Mode](#)
- [Running the Management Agent Installer](#)

To run the Management Agent installer for UNIX, refer to this section: [Running the Management Agent Installer](#), which follows the Notes below.

Permissions

All files that you extracted from the `.zip` file must have execute permissions. You can use the `chmod` command to set these permissions.

/tmp location

The *Management Agent* installer uses the `/tmp` location to temporarily store files used during the installation. Before installing ensure that at least 400 MB is available in the `/tmp` location.

Oracle User ID

You must login to the UNIX machine with an Oracle user ID; otherwise you cannot run the installer.

Management Agent on the Application Server

If you will be using the *Management Agent* to manage an Application Server, you must install the *Management Agent* as the oracle user. After installing the agent, change the ownership of the agent installation directory to the appropriate user and then start the agent with same user which owns the application server services.

Enterprise Server

If you will be using the *Management Agent* to manage a UNIX-based Enterprise Server, you must install the *Management Agent* as an Oracle user. Once the agent is installed, change the agent installation directory ownership to *JD Edwards EnterpriseOne* user (which owns running the enterprise server services) and then run agent services. For example, valid *JD Edwards EnterpriseOne* users might be `jde809`, `jde811`, `jde812`, or `jde900`.

You can use the **chown** command to change the ownership directory:

```
$chown -R jde920:jde920 <agent_install_dir>
```

Graphic Mode

For all UNIX environments, you should run the installer in graphic mode.

Running the Management Agent Installer

To install the Server Manager Agent on UNIX-based target machines.

1. Log on to the machine onto which you are installing the Server Manager Management Agent.
2. Change to the directory in which you extracted the Server Manager Agent installer as described in the appropriate subsection of this chapter entitled: *Distribute and Unzip the Management Agent Installer Application*.

3. Launch the OUI installer as follows:

Note:

- **For Tools Release 9.2.2.0 and Greater:** A 64-bit JDK or JRE, version 1.8 or later must be installed before starting the Server Manager Agent installer.
- **For Tools Releases prior to 9.2.2.0:** A JDK is included in the installer. Therefore, a separate JDK is not required.

Note: One of the following requirements must be met:

- **For Tools Release 9.2.3.3 and Greater:** You must specify the location of the JDK or JRE on the command line. If the location is not specified, the installer will fail immediately.
- **For Tools Release 9.2.2.0 up to but not including 9.2.3.3:** You can specify the location of the JDK or JRE on the command line. If the location is not specified, you will be prompted for it.
- **For Tools Releases prior to 9.2.2.0:** Because a JDK is included in the installer, you will not be prompted for one.

To specify the location of a JDK or JRE on the command line:

1. Run this script to launch the installer:

Launch this installer with the necessary GUI settings to run in graphic mode:

```
/Disk1/install/runInstaller.sh -jreLoc /u01/jre1.8.191
```

Note: The unzipped installer files will be in the location specified in the section of this guide entitled: *Distribute and Unzip the Management Agent Installer Application* in the subsection entitled: *UNIX*.

- Include a space after the `-jreLoc` argument.
- The specified JDK or JRE directory must contain this path and executable:

```
bin\java.exe
```

To skip specifying the location of a JDK or JRE on the command line:

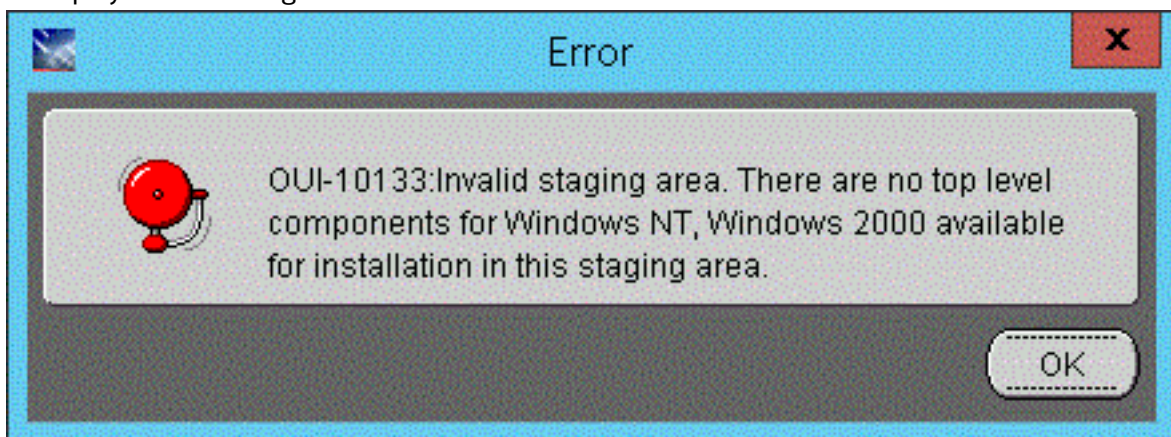
1. Run this script to launch the installer:

Launch this installer with the necessary GUI settings to run in graphic mode:

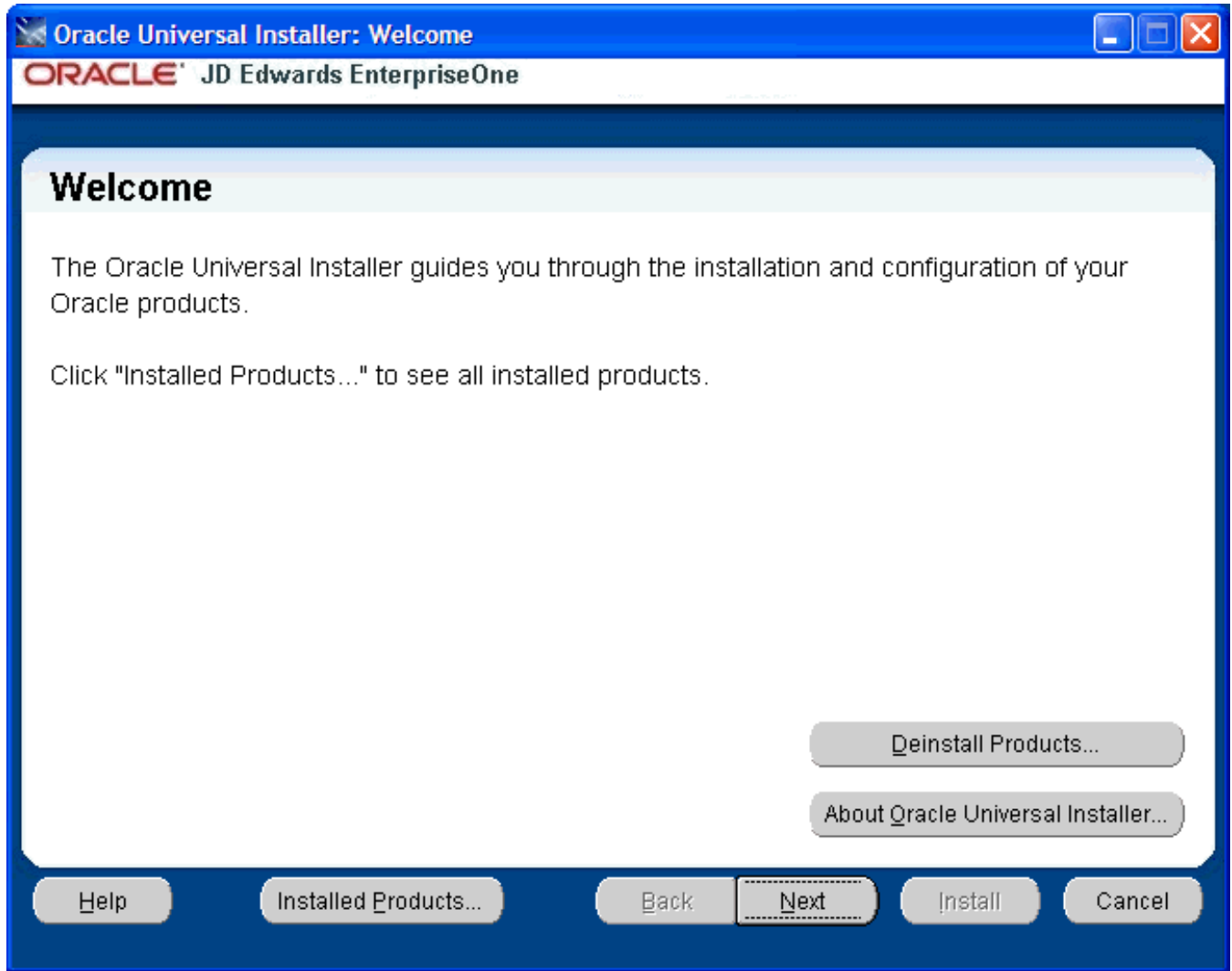
```
/Disk1/install/runInstaller.sh
```

Note: The unzipped installer files will be in the location specified in the section of this guide entitled: *Distribute and Unzip the Management Agent Installer Application* in the subsection entitled: **UNIX. Tools Release 9.2.2.0 up to but not including 9.2.3.3.** If you did not specify the location of a JDK or JRE via the `-jreLoc` argument, the installer prompts you to specify the location of that at a command prompt.

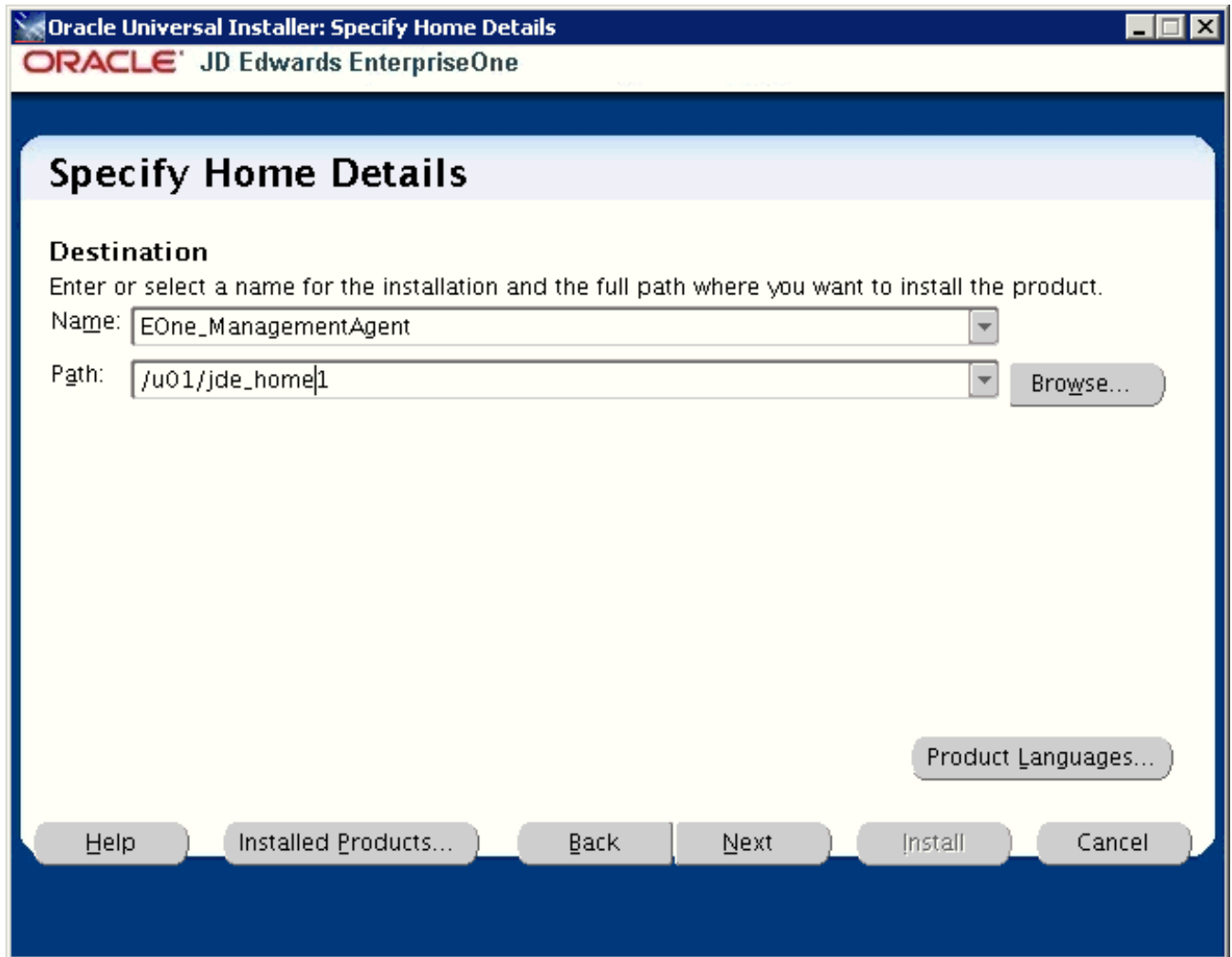
Note: For the 9.2.2.0 installer, as the installer runs, it will fail if the JDK/JRE is not at least Version 1.8. Upon failure it displays the following error:



After the installer validates existence of the JDK in the specified location, the OUI installer user interface appears. All further installer behavior remains the same as previous Tools Releases.



2. On Welcome, click the **Next** button.



3. On Specify Home Details, complete these fields:

- o *Name:*

Enter a name for the Management Agent. The default name is:

EOne_Management_Agent

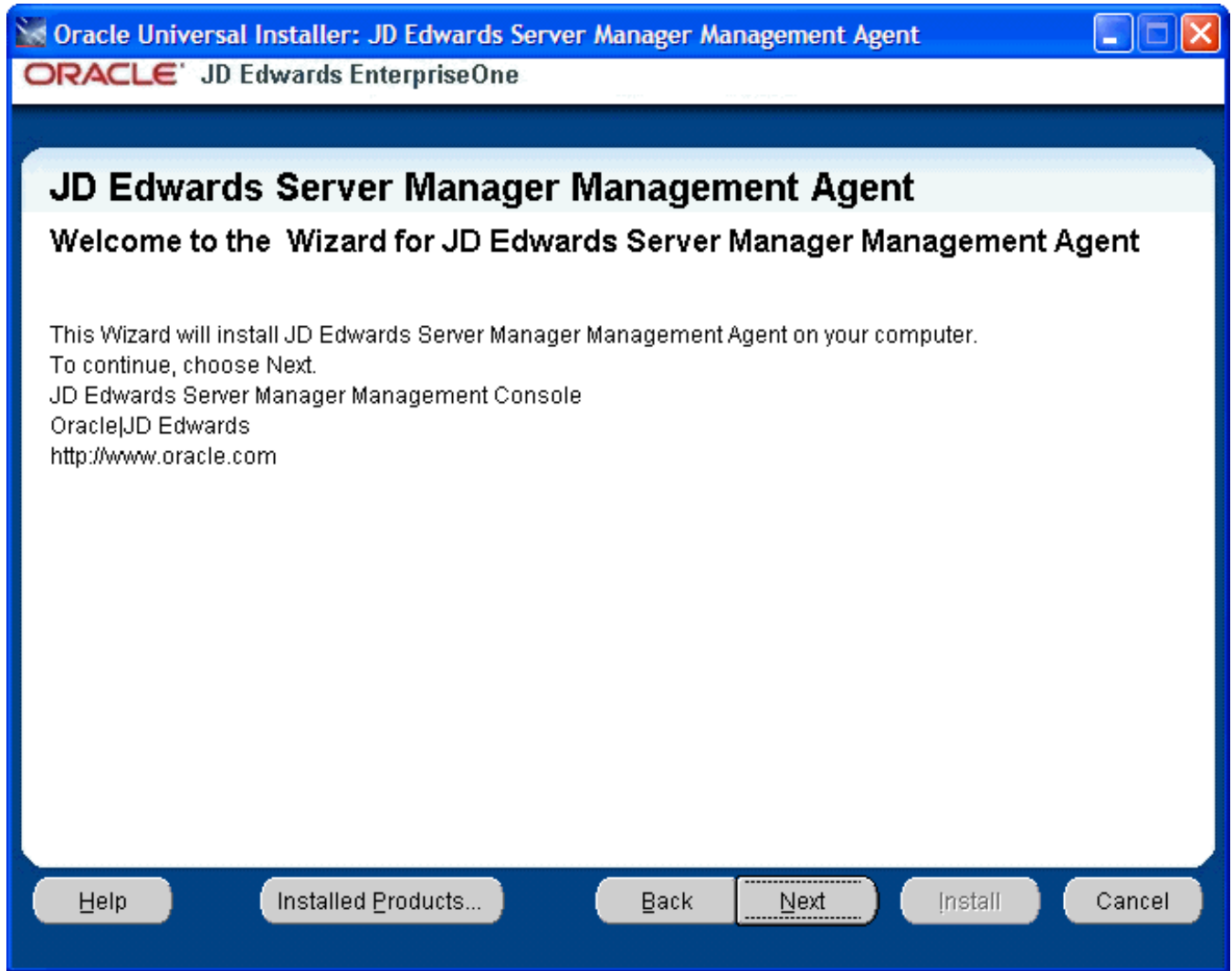
- o *Path:*

The installer automatically detects the root mount point location on the machine and by default appends this value:

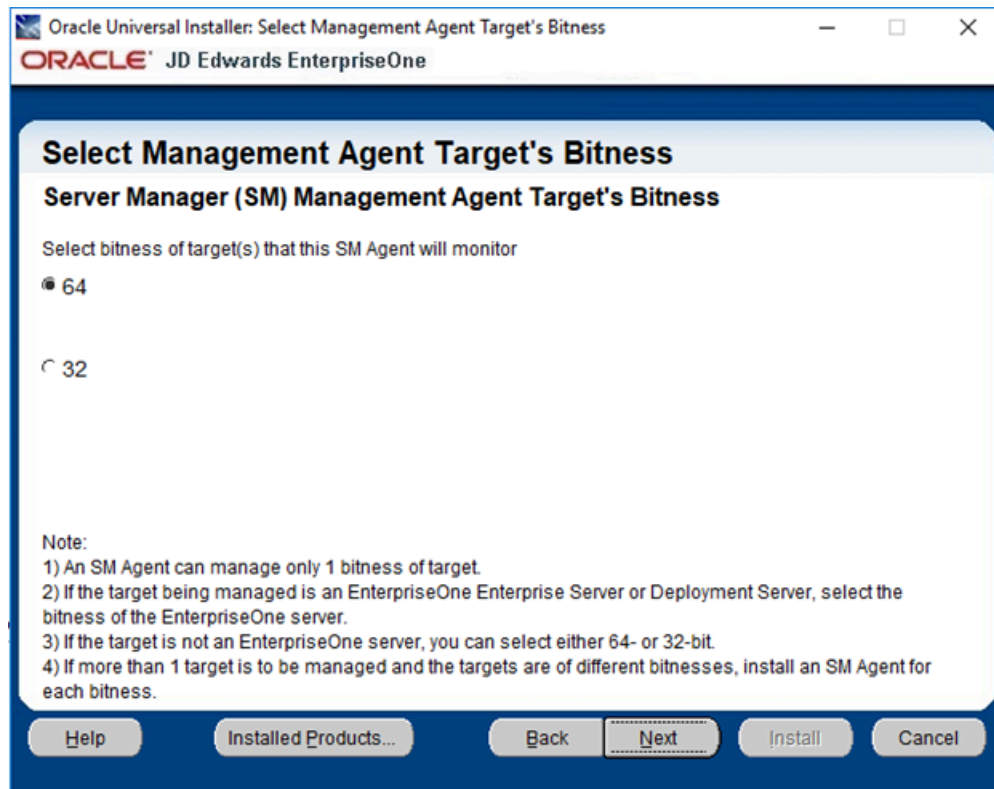
`jde_home`

Note: Although **jde_home** is the default and recommended setting, you can specify any value to replace the default value.

The directory that you specify cannot already exist.



4. On Welcome to the Wizard for JD Edwards Server Manager Management Agent, click the **Next** button.

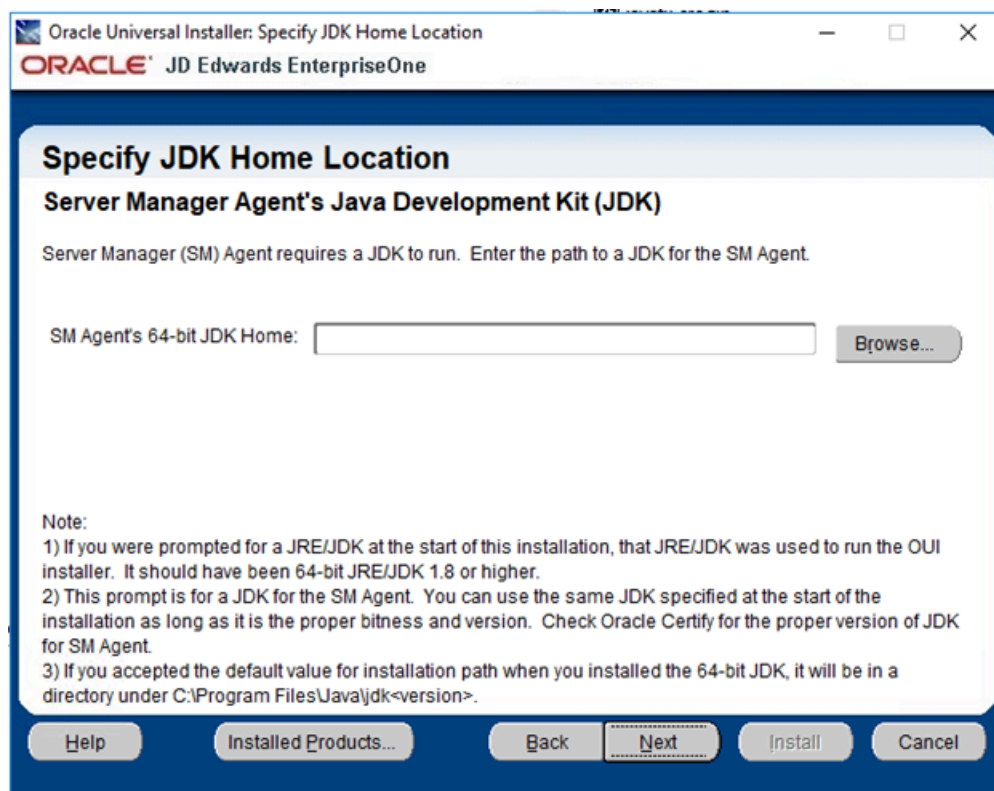


5. On Select Agent Target's Bitness, select the bitness of the targets that the Server Manager Agent will monitor and click the **Next** button.

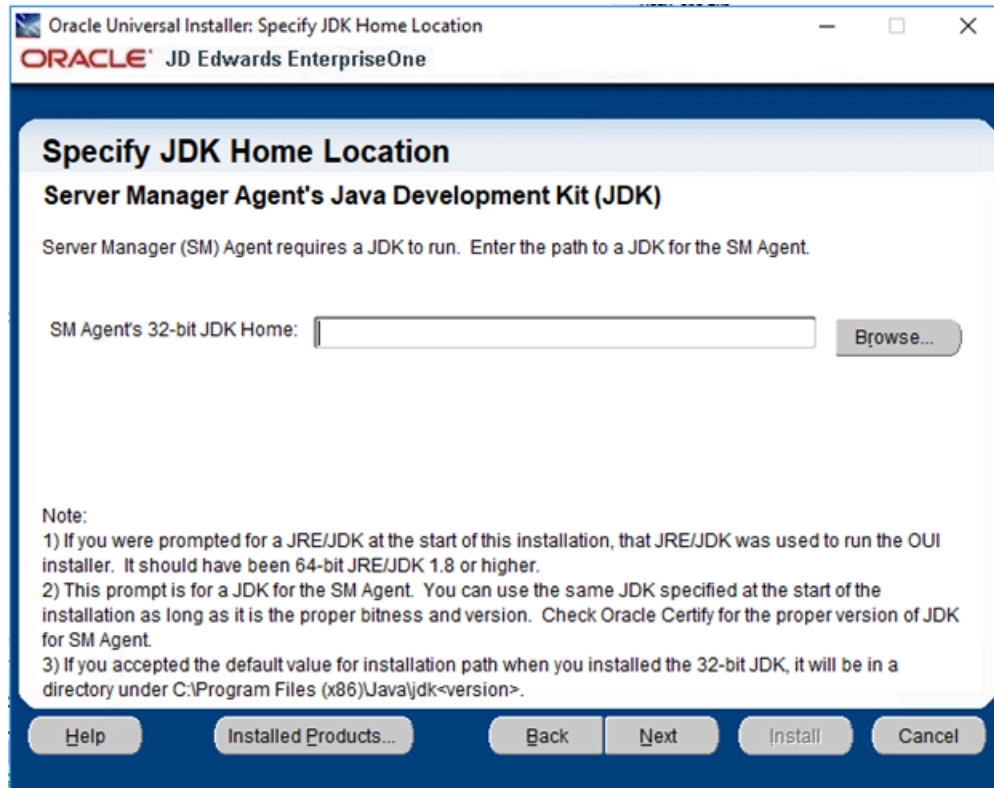
Note: These considerations apply to bitness:

- o Each Server Manager Agent can manage only a single bitness of target objects. That is, it cannot manage multiple objects if the objects are a mixture of 32-bit and 64-bit bitness.
- o If the target being managed is a JD Edwards EnterpriseOne Enterprise Server or Deployment Server, select the bitness of the EnterpriseOne server.
- o If the target is not an EnterpriseOne server, you can select either 64-bit or 32-bit.
- o If more than one target is to be managed and the targets are of different bitnesses, you must install a Server Manager Agent for each bitness.

If **64** is selected, then this 64-bit JDK Home screen will appear:



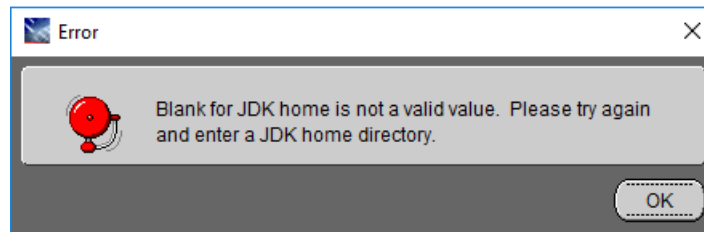
If **32** is selected, then this 32-bit JDK Home screen will appear:



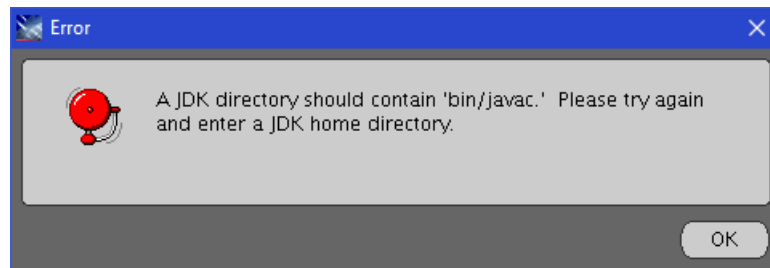
6. In the **JDK Home** field, enter or browse to the location of your Java Development Kit (JDK). In order to proceed, you cannot leave this value blank and you must specify an existing valid location.

Note: These considerations apply to the JDK:

- o The JRE/JDK that you specified at the start of this installation was used to run the OUI installer. For Tools Release 9.2.2.0 and greater, it should have been a 64-bit JRE/JDK 1.8 or higher.
- o This prompt is for a JDK that the Server Manager Agent will use. You can use the same JDK specified at the start of the installation as long as it is the proper bitness and version.



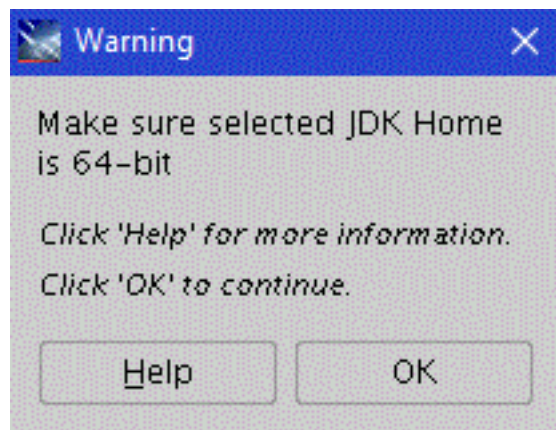
If you enter a blank JDK Home directory, you will get the above error.

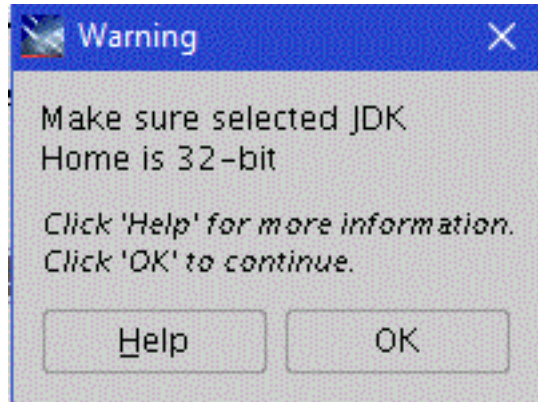


If you enter a directory that does not contain `bin/javac`, you will get the above error.

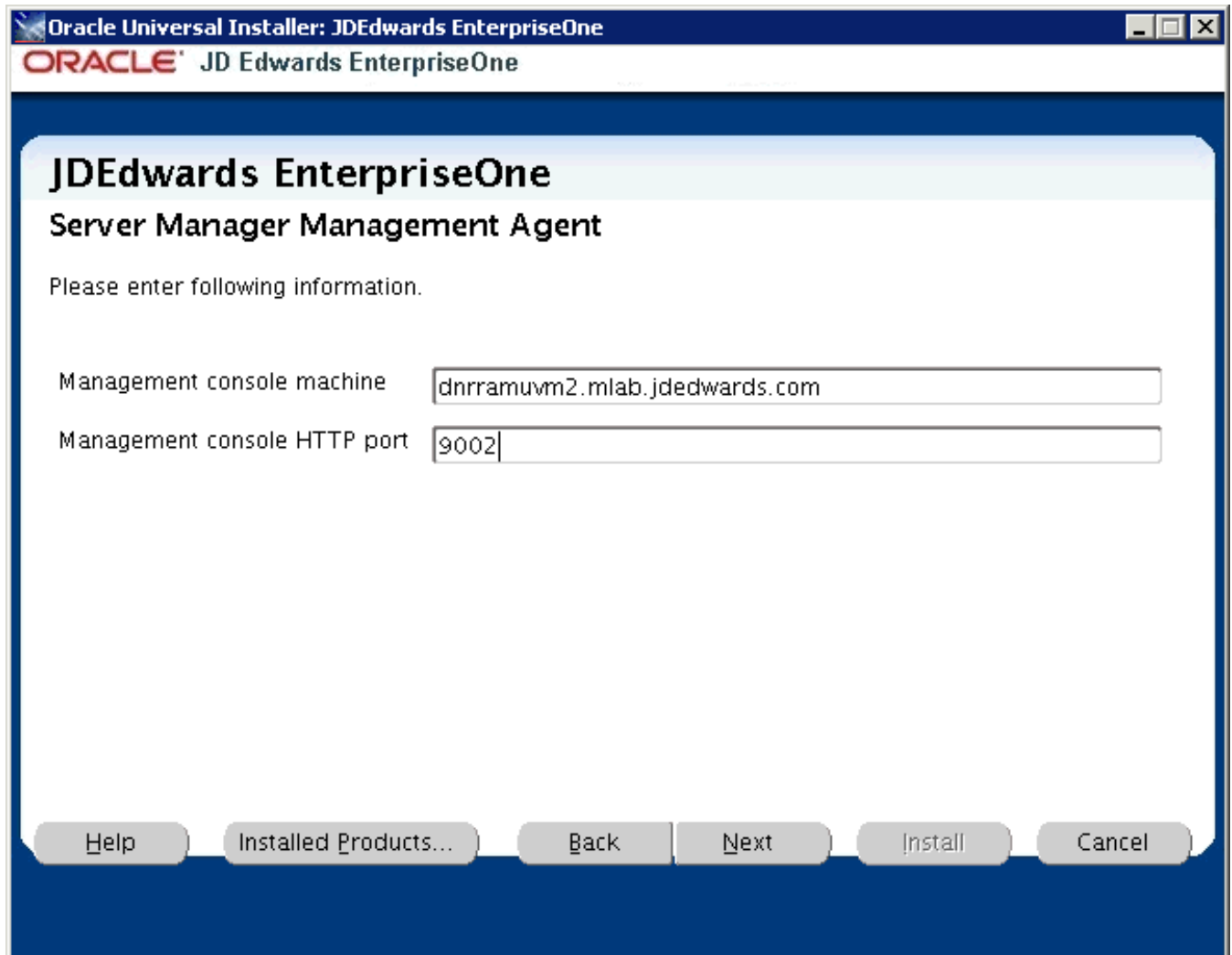
7. Enter the appropriate JDK path and click the **Next** button.
8. After you click the **Next** button, a popup **Warning** displays and prompts you to confirm that you have entered the path to the correct JDK. The warning is dependent on whether you previously selected 64 or 32 bit, as respectively shown below.

Note: The installer does **NOT** programmatically verify that the proper bitness of JDK was selected. The user is responsible for confirming the bitness.





9. When you have confirmed the correct path, click the **OK** button to proceed.



10. On Server Manager Management Agent, complete these fields:

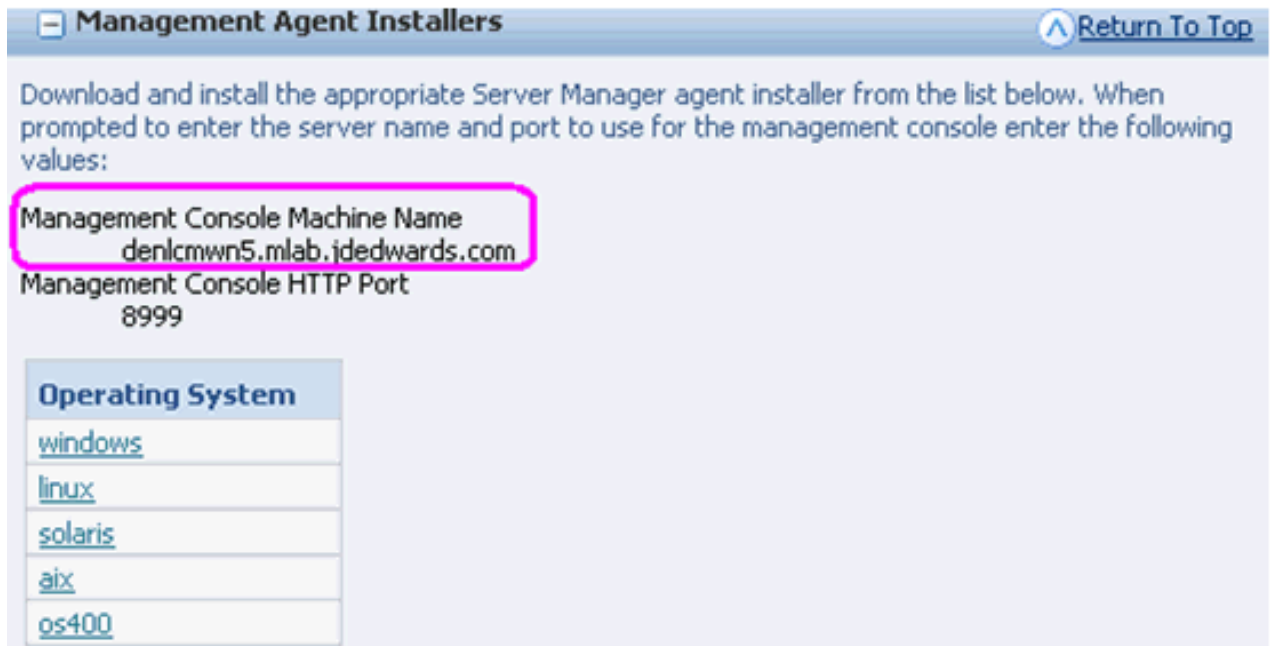
- o *Management console machine*

You must specify the host name of an existing *Management Console* machine.

The installer verifies the connection to the *Management Console* during the install. The *Management Console* machine must be started and the *Management Console* must be running in order to run the installer. In some cases, depending on your machine, operating systems, or network, you might need to

fully qualify your machine name. For example, instead of specifying only `dnrramuv2` you might need to specify `dnrramuv2.mlab.jdedwards.com`.

Tip: You can determine the name of your *Management Console* from the information supplied on the **Management Agent Installers** screen. For navigation, refer to Step 2 in the section entitled: *Obtain the Management Agent Installer Application*. You can also view the `readme.txt` file in the root directory of the *Management Console*.



- o *Management console HTTP port*

You must specify a valid port of an existing *Management Console* machine.

The installer verifies the port connection to the *Management Console*. The machine must be started and the *Management Console* must be running in order to run the installer.

Tip: You can determine the port of your *Management Console* from the information supplied on the **Management Agent Installers** screen. For navigation, refer to Step 2 in the section entitled: *Obtain the Management Agent Installer Application*.

Management Agent Installers [Return To Top](#)

Download and install the appropriate Server Manager agent installer from the list below. When prompted to enter the server name and port to use for the management console enter the following values:

Management Console Machine Name
donlcmwne.mlab.jdedwards.com

Management Console HTTP Port
8999

Operating System
windows
linux
solaris
aix
os400

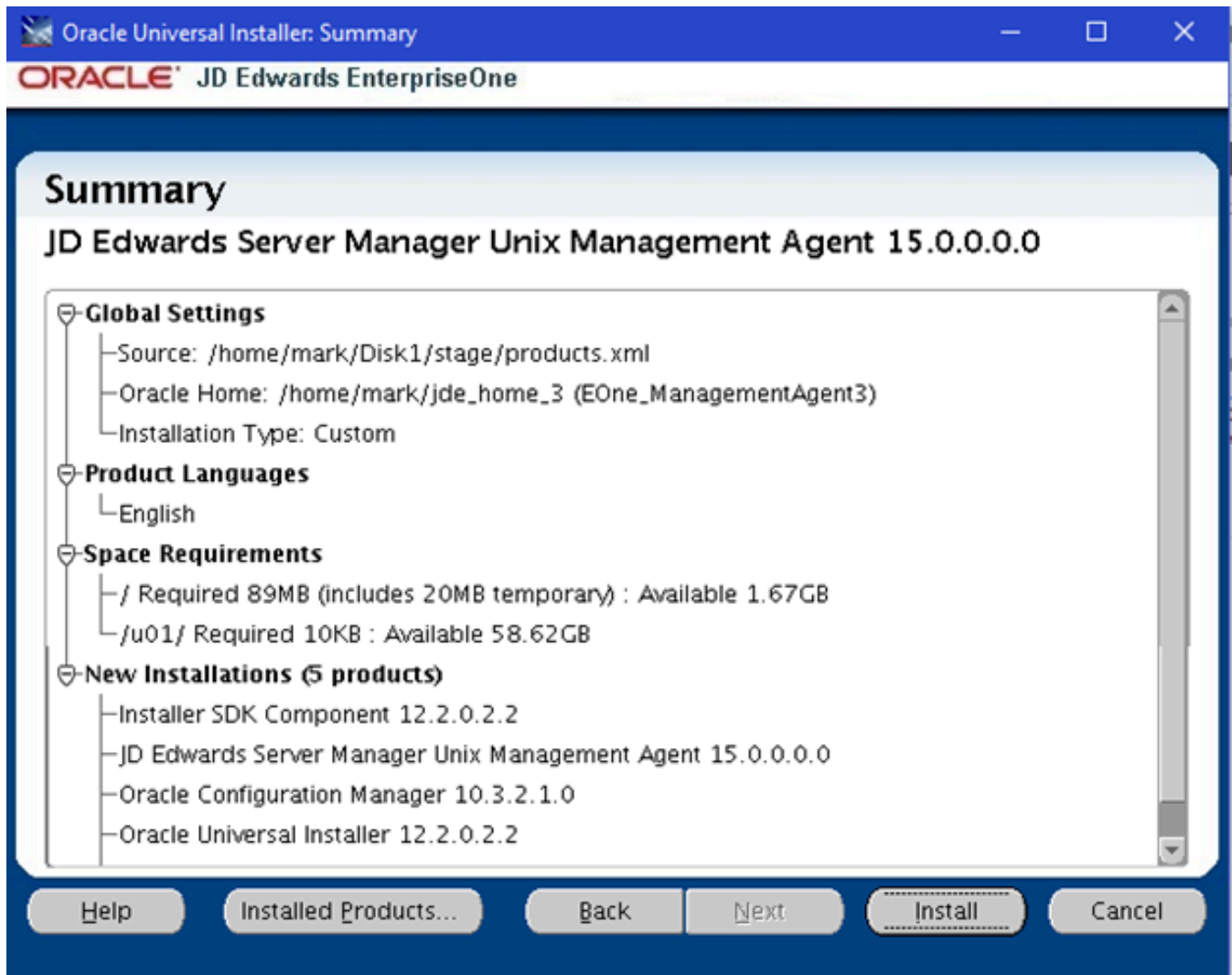
- o *Management console Using SSL*

Select:

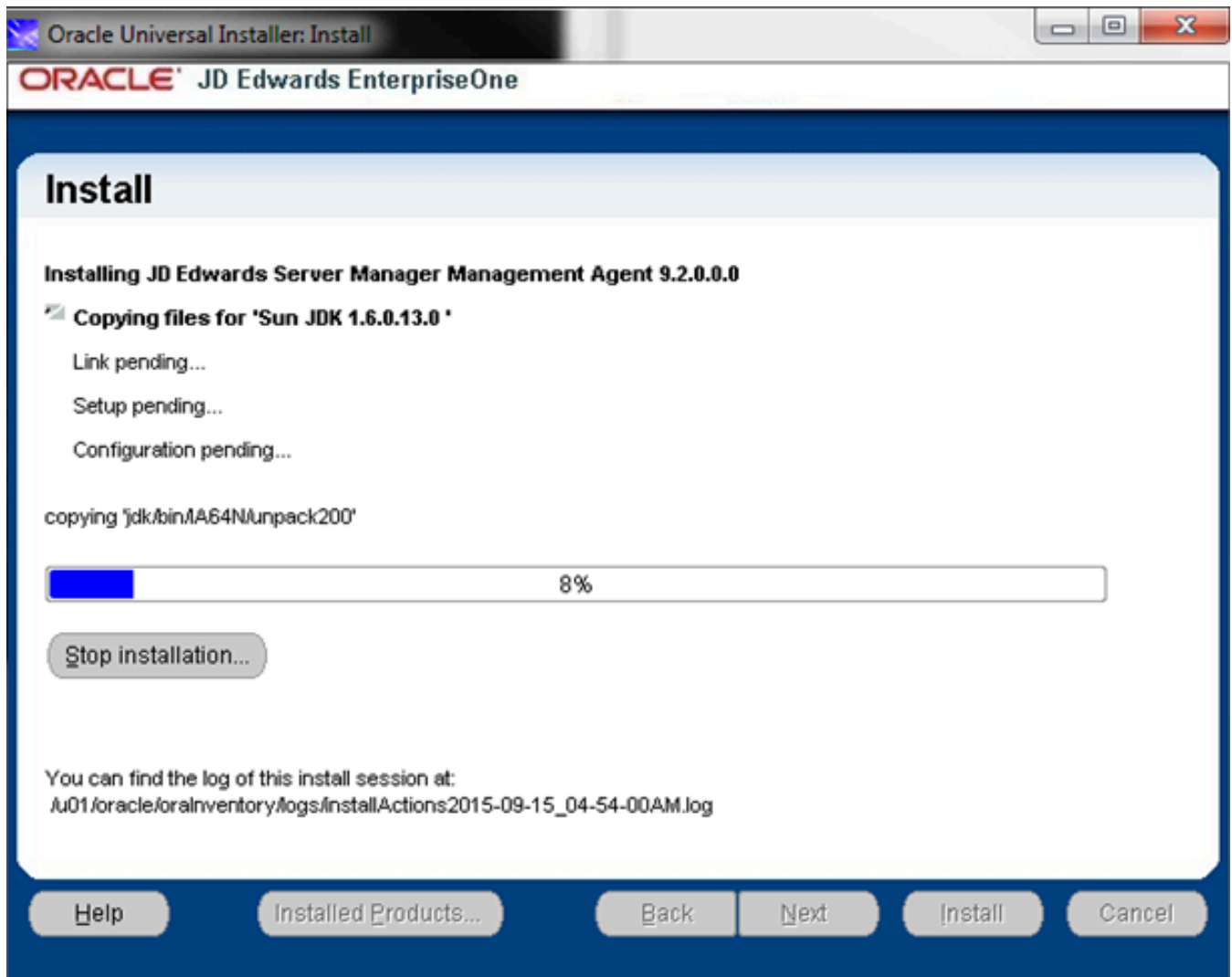
YES - SMC runs on SSL

NO - SMC does not run on SSL

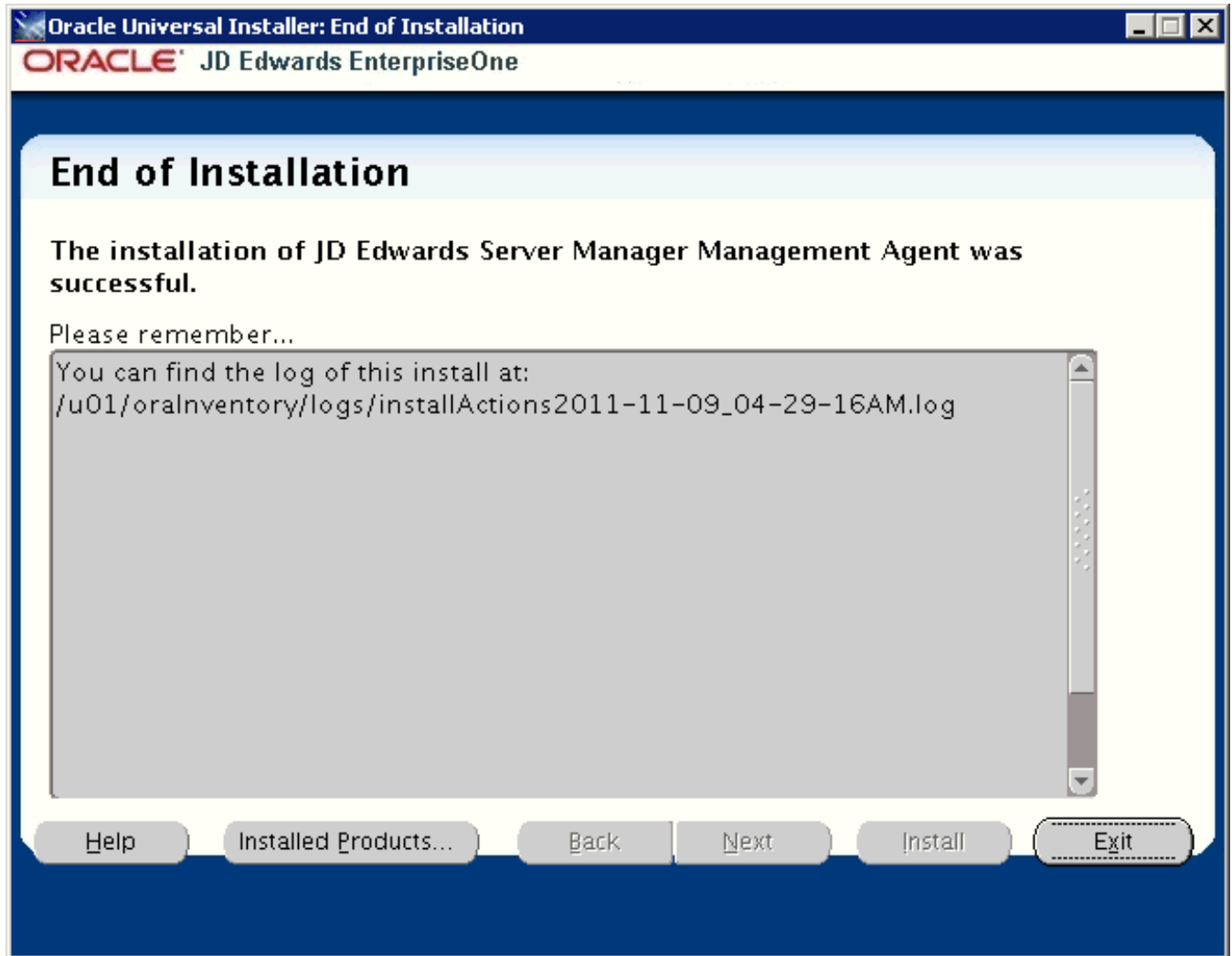
11. Click the **Next** button to verify the machine and port values.



12. On Summary, review the information and click the **Install** button to begin the installation.



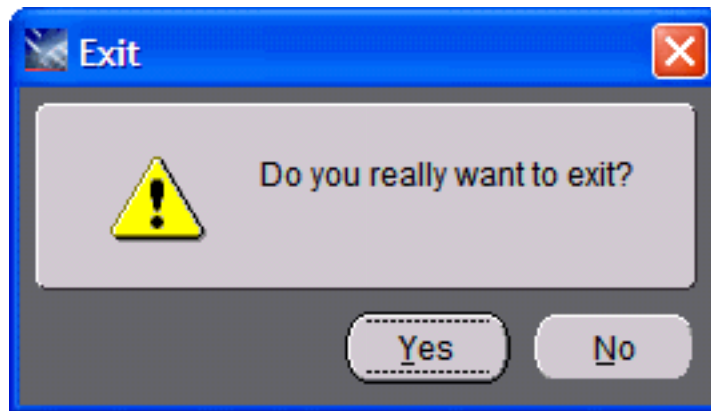
The Management Agent installer displays a panel showing the ongoing status of the installation.



13. When the installation finishes, the End of Installation screen is displayed.

CAUTION: Examine the Installer Logs. This screen also displays the location of the install log. Even though the screen indicates that the installation was successful, you should always check the logs before you attempt to run the Agent. The file name starts with "installActions" and includes a time stamp; it is located in `/u01/oraInventory/logs`. For example: `/u01/oraInventory/logs/installActions2018-11-09_04-29-16AM.log`

14. Click the **Exit** button.



15. On the Exit dialog, click the **Yes** button to confirm you want to exit the Management Agent installer.

Note: After a successful installation, the *Management Agent* automatically starts and connects to the *Server Manager Management Console*. The resulting newly installed *Managed Home* can be viewed in the *Management Dashboard* of the *Management Console*.

IBM i(OS400)

You cannot run the OS400 Management Agent installer directly on the *IBM i* machine. Therefore you must download and extract the Management Agent Installer file on a Microsoft Windows machine as described in the section of this guide entitled: *Distribute and Unzip the Management Agent Installer Application* in the subsection entitled: *(OS400)*. Likewise, you must run the Management Agent installer on a Windows machine, as described in this procedure.

CAUTION: To deinstall the Management Agent from the *IBM i* machine, you must perform the deinstall from this same Microsoft Windows machine. This is because only the machine on which the installer runs contains the requisite information to perform the deinstallation.

Prerequisite

Before you run the Management Agent installer for *IBM i OS/400*, you must ensure that iSeries Navigator is installed on the *IBM i* target machine.

To install the Server Manager Agent on IBMi target machines:

1. Log on to the Windows machine on which you are running the Server Manager Management Agent installer.
2. Change to the directory in which you extracted the Server Manager Agent installer as described in the appropriate subsection of this chapter entitled: *Distribute and Unzip the Management Agent Installer Application* in the subsection entitled: *(OS400)*.
3. Depending on your Tools release, launch the OUI installer according to these notes:

Note:

- **For Tools Release 9.2.2.0 and Greater:** A 64-bit JDK or JRE, version 1.8 or later must be installed on the Microsoft Windows machine before starting the Server Manager Agent installer.
- **For Tools Releases prior to 9.2.2.0:** A JDK is included in the installer. A separate one is not required.
- **For Tools Release 9.2.3.3 and Greater:** Microsoft Visual Studio 2017 and 2013 64-bit Redistributables must be installed prior to running the Server Manager Console installer.
- **For Tools Releases prior to 9.2.3.3:** Microsoft Visual Studio 2010 32-bit Redistributables must be installed prior to running the Server Manager Console installer.

Note: One of the following requirements must be met:

- **For Tools Release 9.2.3.3 and Greater:** You must specify the location of the JDK or JRE on the command line. If the location is not specified, the installer will fail immediately.
- **For Tools Release 9.2.2.0 up to but not including 9.2.3.3:** You can specify the location of the JDK or JRE on the command line. If the location is not specified, you will be prompted for it.
- **For Tools Releases prior to 9.2.2.0:** Because a JDK is included in the installer, you will not be prompted for one.

To specify the location of a JDK or JRE on the command line:

1. Open a Windows Command window with **Run as administrator**.
2. Change directory (cd) to the directory in which you unzipped the installer. For example, if you followed the recommendation in *Distribute and Unzip the Management Agent Installer Application* the command would be:

```
cd C:\SM_Agent\Disk1\install
```

3. Use this command to run `setup.exe` followed by the argument `-jreLoc` and the directory to the JDK or JRE:

```
setup.exe -jreLoc C:\PROGRA~1\Java\JRE18~1.0_1
```

Note: Regarding the above command:

- Include a space after the `-jreLoc` argument.
- The path to the JDK or JRE must be of the Windows short form, which is 8 + 3 format.
- The specified JDK or JRE directory must contain this directory and executable:

```
bin\java.exe
```

To skip specifying the location of a JDK or JRE on the command line:

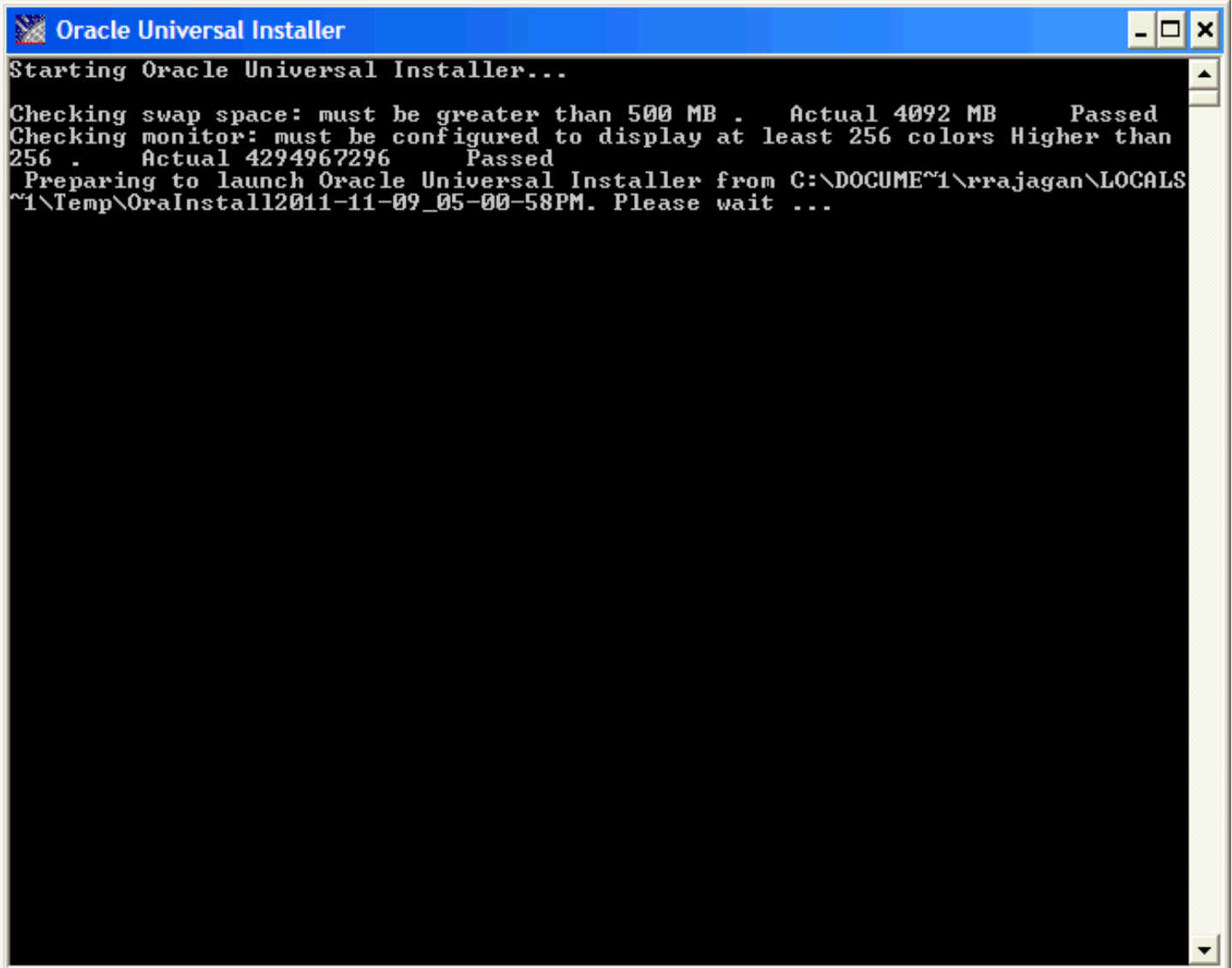
Do one of the following:

1. Follow the instructions above to run from a Windows Command window but without the `-jreLoc` argument.

2. In Windows Explorer, right-click on `setup.exe` in the directory in which you unzipped the installer and select **Run As Administrator**. For example, if you followed the recommendation in *Distribute and Unzip the Management Agent Installer Application* the file will be located in this directory:

`C:\SM_Agent\Disk1\install\setup.exe`

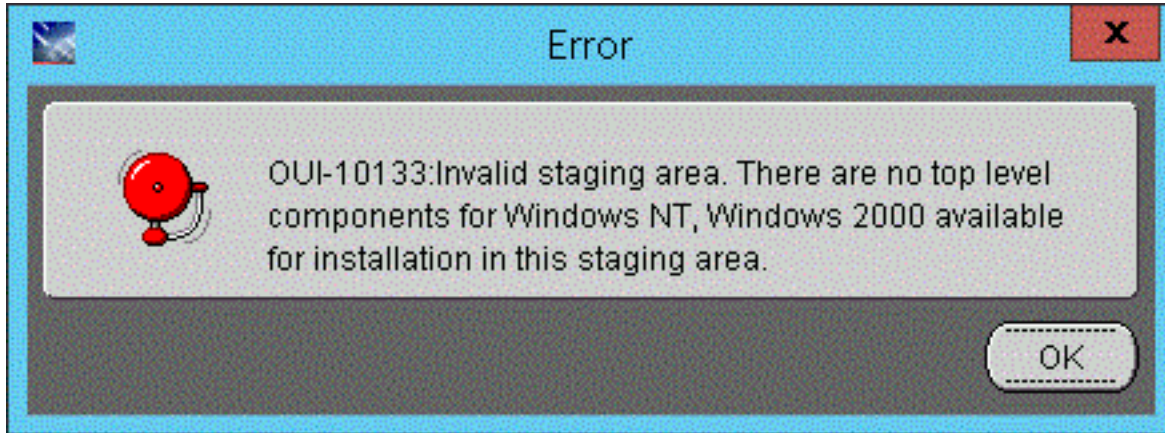
This process opens a Microsoft Windows command window as shown in the below example.

A screenshot of a Windows command window titled "Oracle Universal Installer". The window has a blue title bar with standard minimize, maximize, and close buttons. The command prompt shows the following text:

```
Starting Oracle Universal Installer...  
Checking swap space: must be greater than 500 MB .   Actual 4092 MB   Passed  
Checking monitor: must be configured to display at least 256 colors Higher than  
256 .   Actual 4294967296   Passed  
Preparing to launch Oracle Universal Installer from C:\DOCUME~1\rrajagan\LOCALS  
~1\Temp\OraInstall12011-11-09_05-00-58PM. Please wait ...
```

Tools Release 9.2.2.0 up to but not including 9.2.3.3. If you did not specify the location of a JDK or JRE using the `-jreLoc` argument, the installer prompts you to specify the location of that at a command prompt.

Note: For the 9.2.2.0 and greater, the installer will fail if the JDK/JRE is not at least Version 1.8. Upon failure it displays the following error:



After the installer validates existence of the JDK in the specified location, the OUI installer user interface appears. All further installer behavior remains the same as previous Tools Releases.

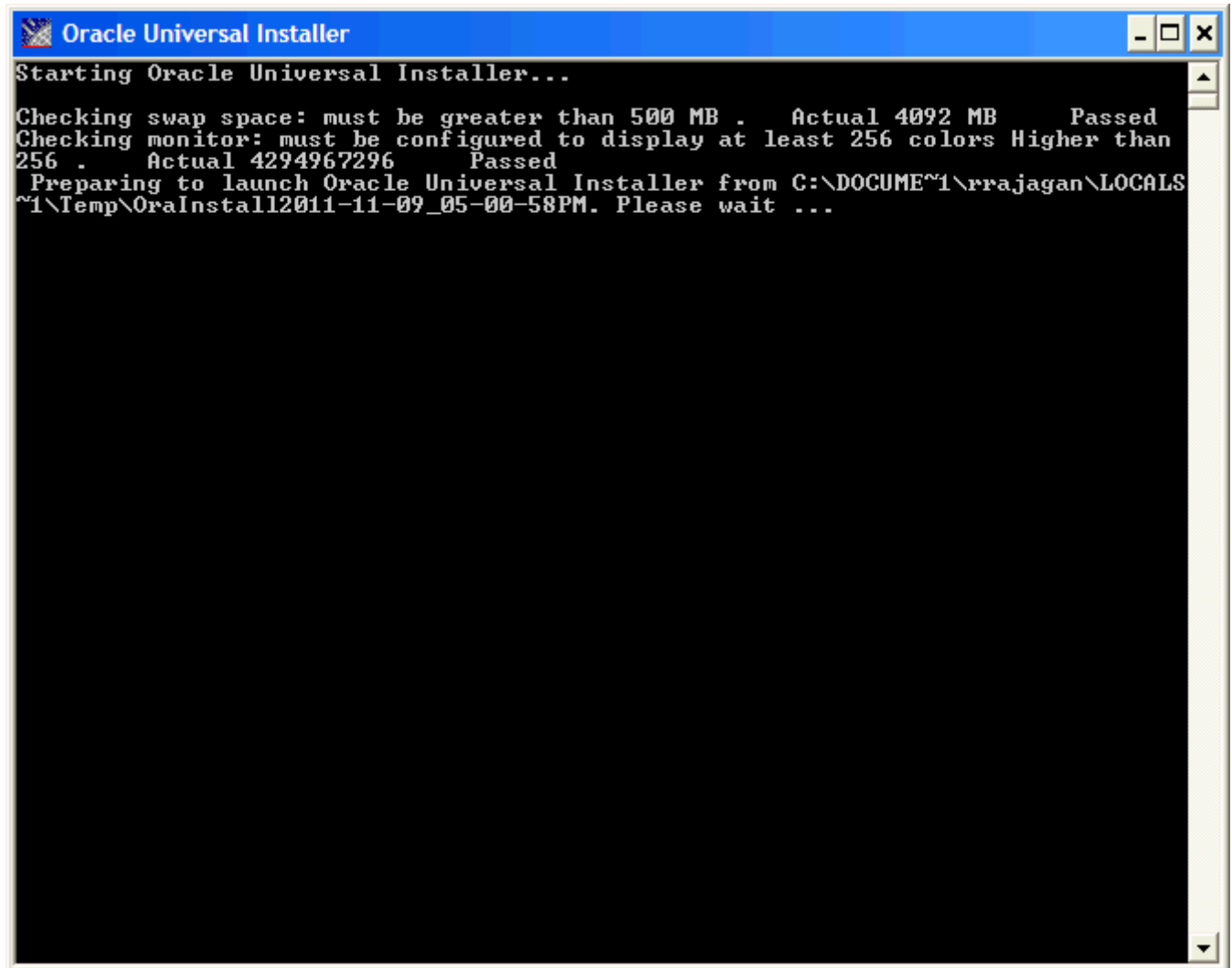
Start Here xxxx

1. On the Microsoft Windows machine where you extracted the `.zip` file, and which is mapped to the *IBM i* machine, run this file:

```
/Disk1/install/setup.exe
```

Note: The unzipped installer files will be in the location specified in the section of this guide entitled: *Distribute and Unzip the Management Agent Installer Application* in the subsection entitled: *(OS400)*.

This process opens a Microsoft Windows command window as shown in the below example.



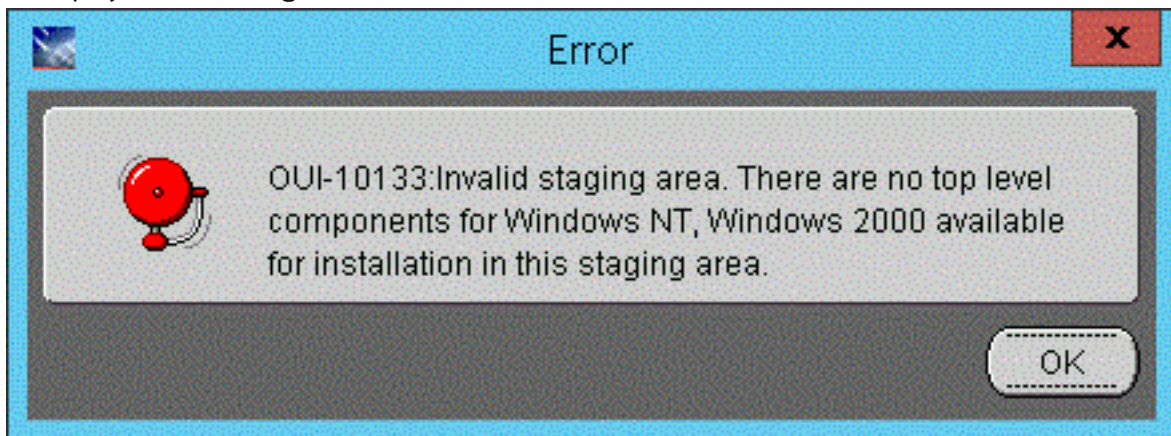
Requirement for Tools Release 9.2.2.0 and Greater. When launching the installer for the Server Manager Agent through `setup.exe` or `runInstaller` that is delivered with Tools Release 9.2.2.0 and greater, a **prerequisite**

to run the installer is that you must have preinstalled a 64-bit JDK or JRE, Version 1.8 or later . The installer prompts you to specify the location of that at a command prompt.

```
$ ./runInstaller
Starting Oracle Universal Installer...

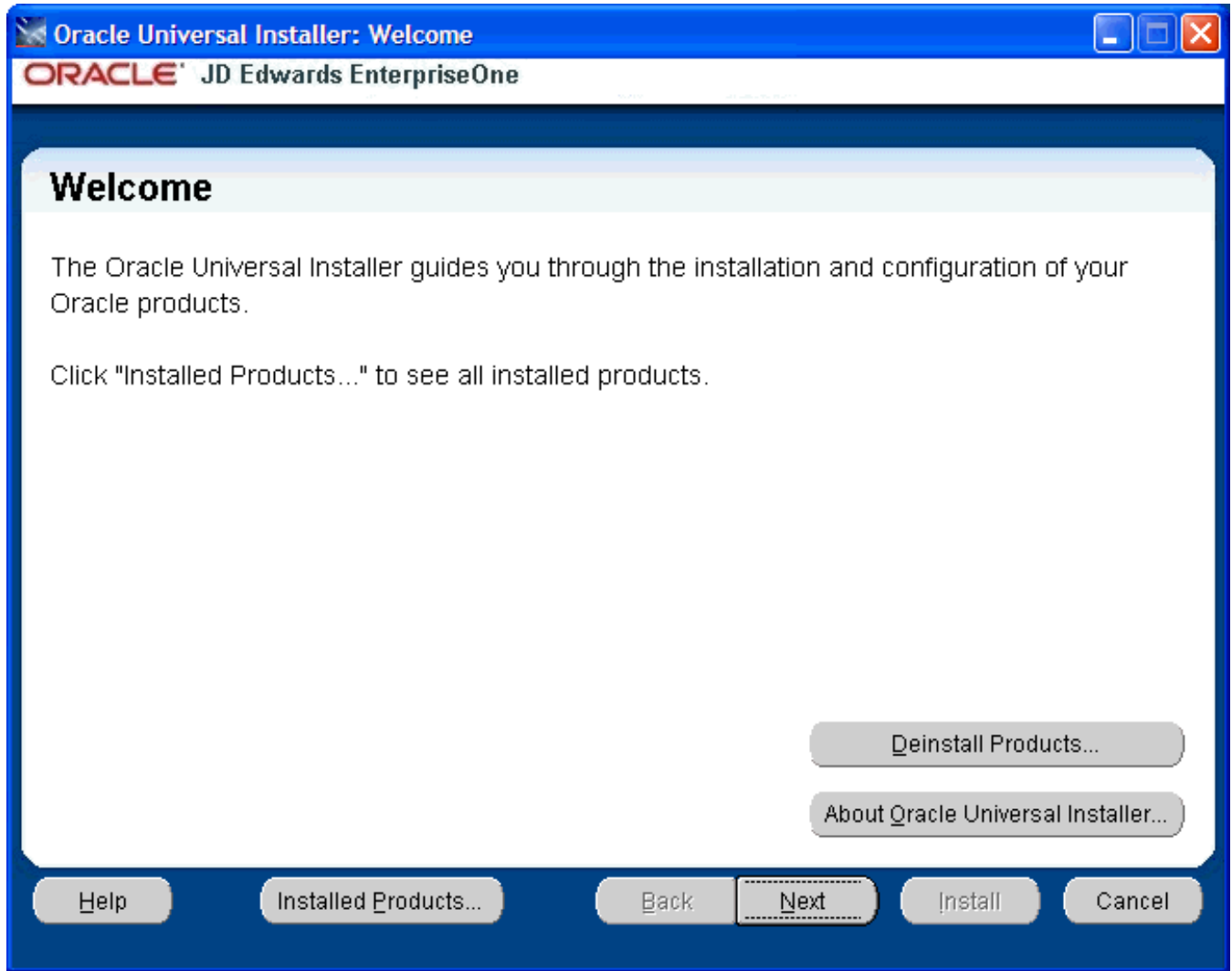
Preparing to launch Oracle Universal Installer from /tmp/OraInstall2017-08-15_09-16-20AM. Please wait ...
Please specify JRE/JDK location ( Ex. /home/jre ), <location>/bin/java should exist :
```

Note: For the 9.2.2.0 installer, as the installer runs, it will fail if the JDK/JRE is not at least Version 1.8. Upon failure it displays the following error:

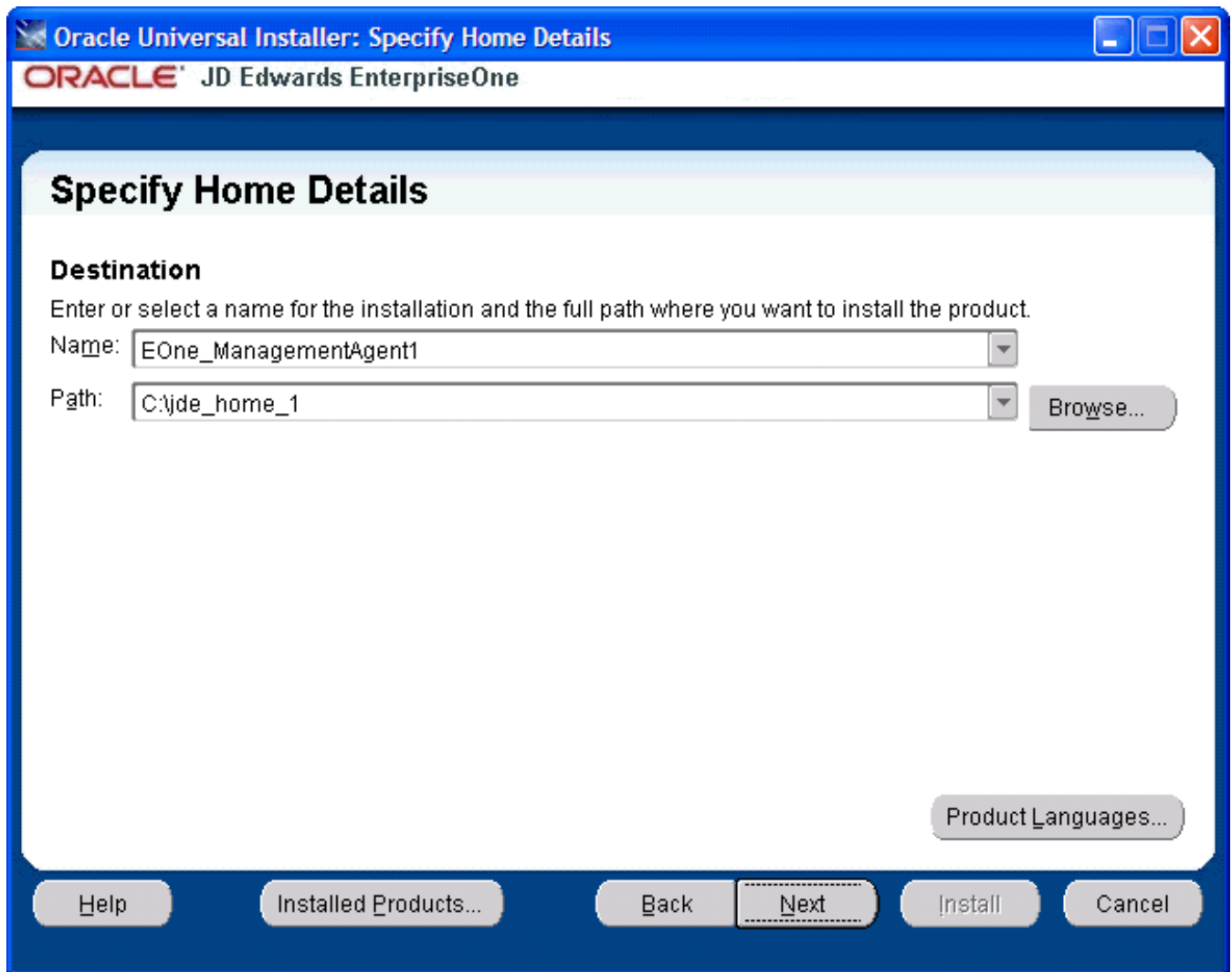


For Tools Release 9.2.2.0 installers, after the installer validates existence of the JDK in the specified location, the OUI installer user interface appears. All further installer behavior remains the same as previous Tools Releases.

After the OUI installer is launched, the command window is closed and the Welcome screen is displayed.



2. On Welcome, click the **Next** button.



3. On Specify Home Details, complete these fields:

- o *Name:*

Enter a name for the Management Agent. The default name is:

EOne_Management_Agent

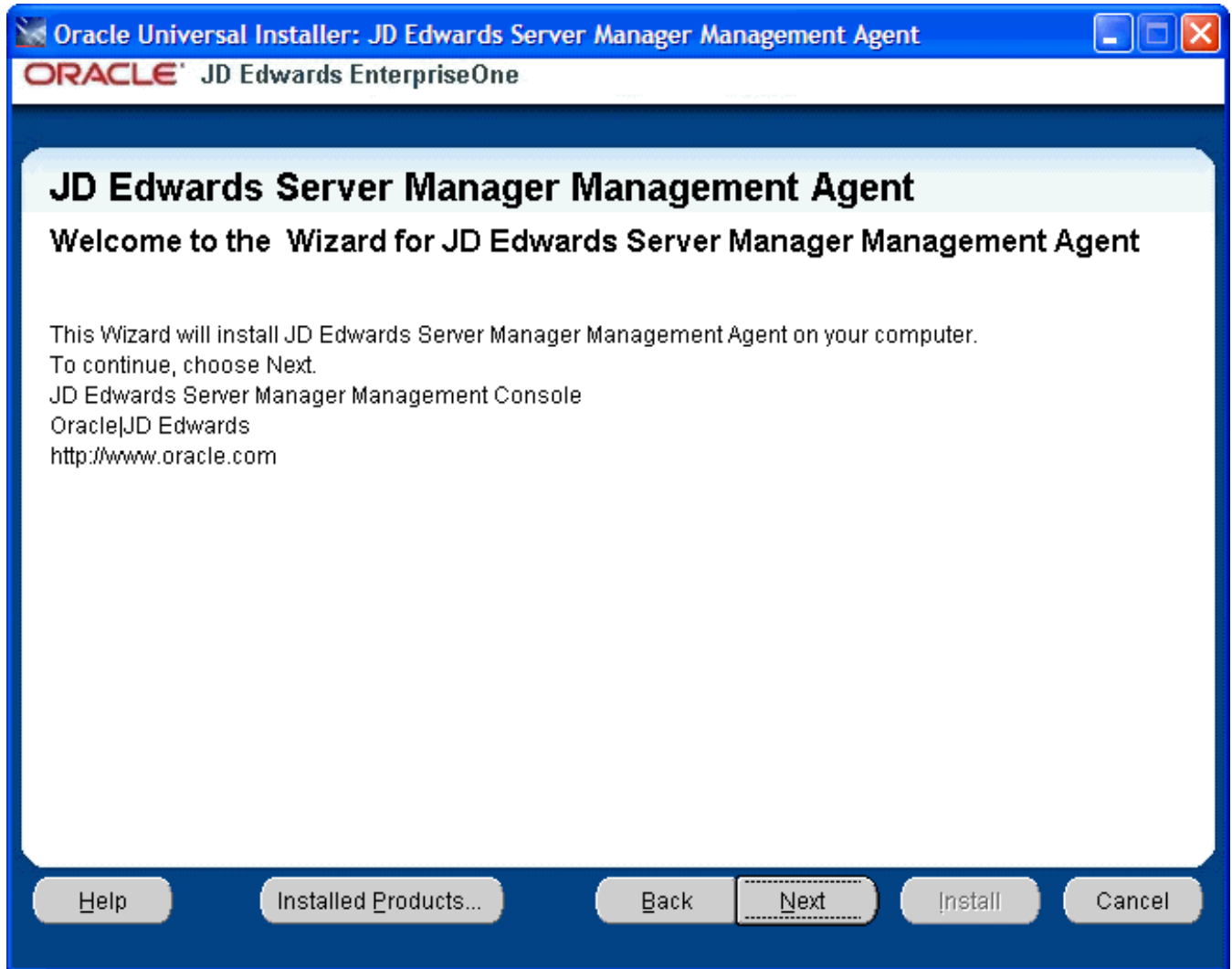
- o *Path:*

The installer automatically detects the root drive location on the Microsoft Windows machine and by default appends this value:

`jde_home`

Note: Although **jde_home** is the default and recommended setting, you can specify any value to replace the default value.

The directory that you specify cannot already exist.



4. On Welcome to Wizard for JD Edwards Server Manager Management Agent, click the **Next** button.

Oracle Universal Installer: IBMi Server and User Profile

ORACLE JD Edwards EnterpriseOne

IBMi Server and User Profile

Server Manager Management Agent

Please enter the following information referring to the IBMi Server you want to use:

IBMi Server Name:

IBMi User Profile:

User Password:

Confirm Password:

IBMi Agent Folder Name:

Help Installed Products... Back Next Install Cancel

5. On IBMi Server and User Profile, complete these fields:

- *IBMi Server Name*

Enter the name of your *IBM i* target server.

- *IBMi User Profile*

Enter the user profile for the *IBM i* target server on which the Management Agent will be installed.

- *User Password*

Enter the password for the *IBM i* user profile specified in the previous field.

- *Confirm Password*

Confirm the password for the *IBM i* user profile specified in the previous field.

- *IBMi Agent Folder Name*

Enter the name of the IBMi Agent Folder.

6. Click the **Next** button.

Oracle Universal Installer: Management Console Information

ORACLE JD Edwards EnterpriseOne

Management Console Information

Server Manager Management Agent

Please enter following information.

Management console machine:

Management console HTTP port:

Management console using SSL:

Note:
If Management console machine URL uses SSL encryption, select YES otherwise select NO

Buttons: Help, Installed Products..., Back, Next, Install, Cancel

7. On Server Manager Management Agent, complete these fields:

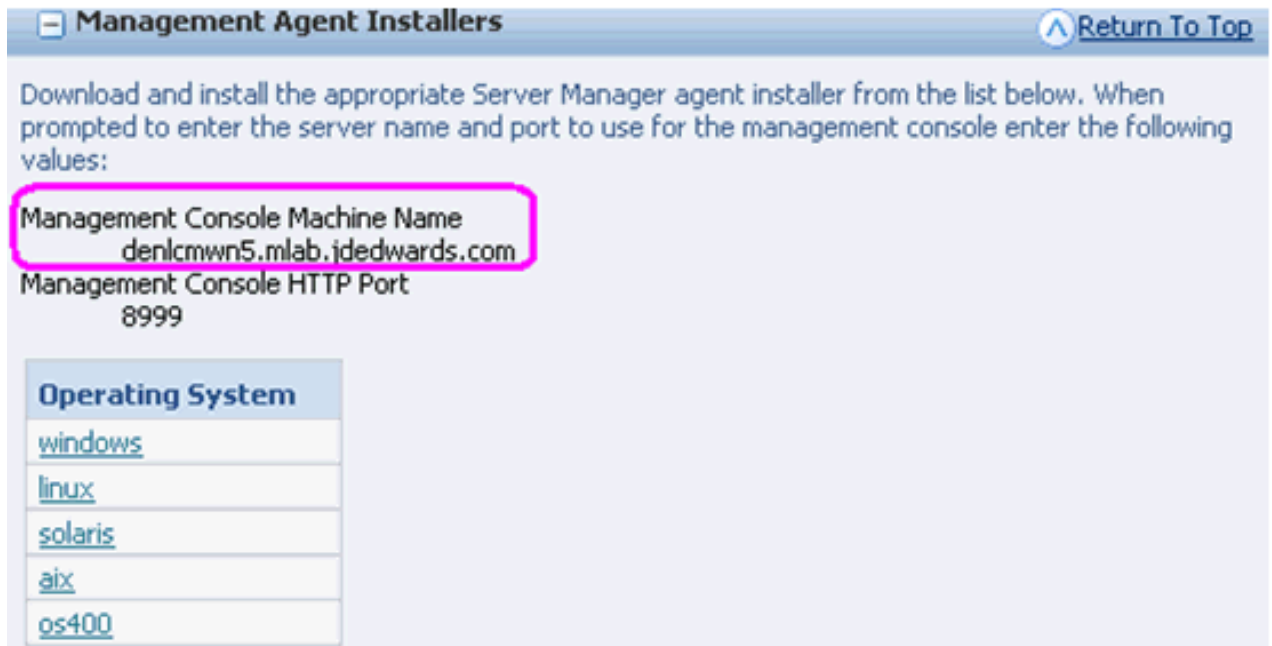
- o *Management console machine*

You must specify the host name of an existing *Management Console* machine.

The installer verifies the connection to the *Management Console* during the install. The *Management Console* machine must be started and the *Management Console* must be running in order to run the installer. In some cases, depending on your machine, operating systems, or network, you might need to

fully qualify your machine name. For example, instead of specifying only `dnrramuv2` you might need to specify `dnrramuv2.mlab.jdedwards.com`.

Tip: You can determine the name of your *Management Console* from the information supplied on the *Management Agent Installers* screen. For navigation, refer to Step 2 in the section entitled: *Obtain the Management Agent Installer Application*. You can also view the `readme.txt` file in the root directory of the *Management Console*.



- o *Management console HTTP port*

You must specify a valid port of an existing *Management Console* machine.

The installer verifies the port connection to the *Management Console*. The machine must be started and the *Management Console* must be running in order to run the installer.

Tip: You can determine the port of your *Management Console* from the information supplied on the *Management Agent Installers* screen. For navigation, refer to Step 2 in the section entitled: *Obtain the Management Agent Installer Application*.

Management Agent Installers [Return To Top](#)

Download and install the appropriate Server Manager agent installer from the list below. When prompted to enter the server name and port to use for the management console enter the following values:

Management Console Machine Name
donlcmwne.mlab.jdedwards.com

Management Console HTTP Port
8999

Operating System
windows
linux
solaris
aix
os400

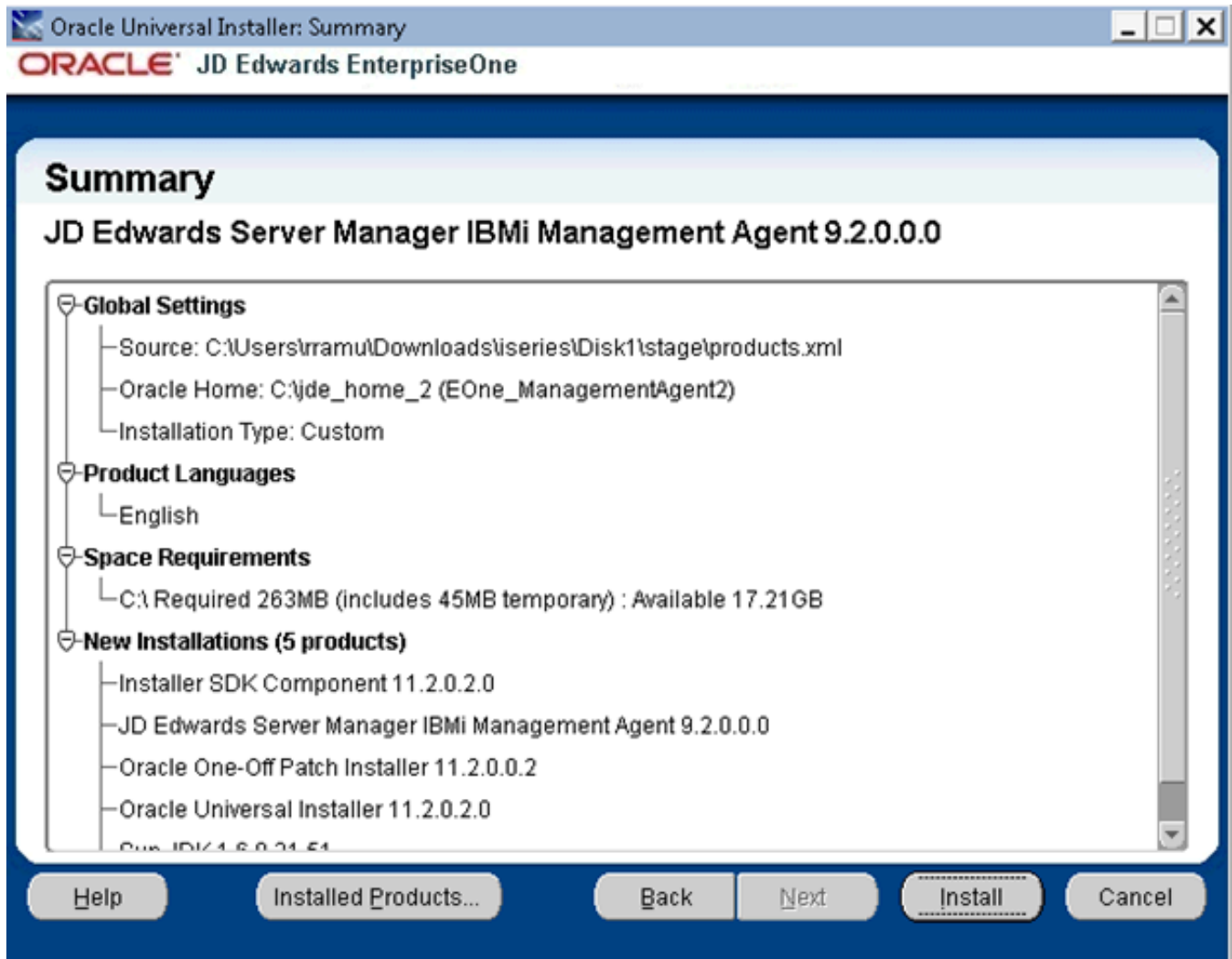
- o *Management console Using SSL*

Select:

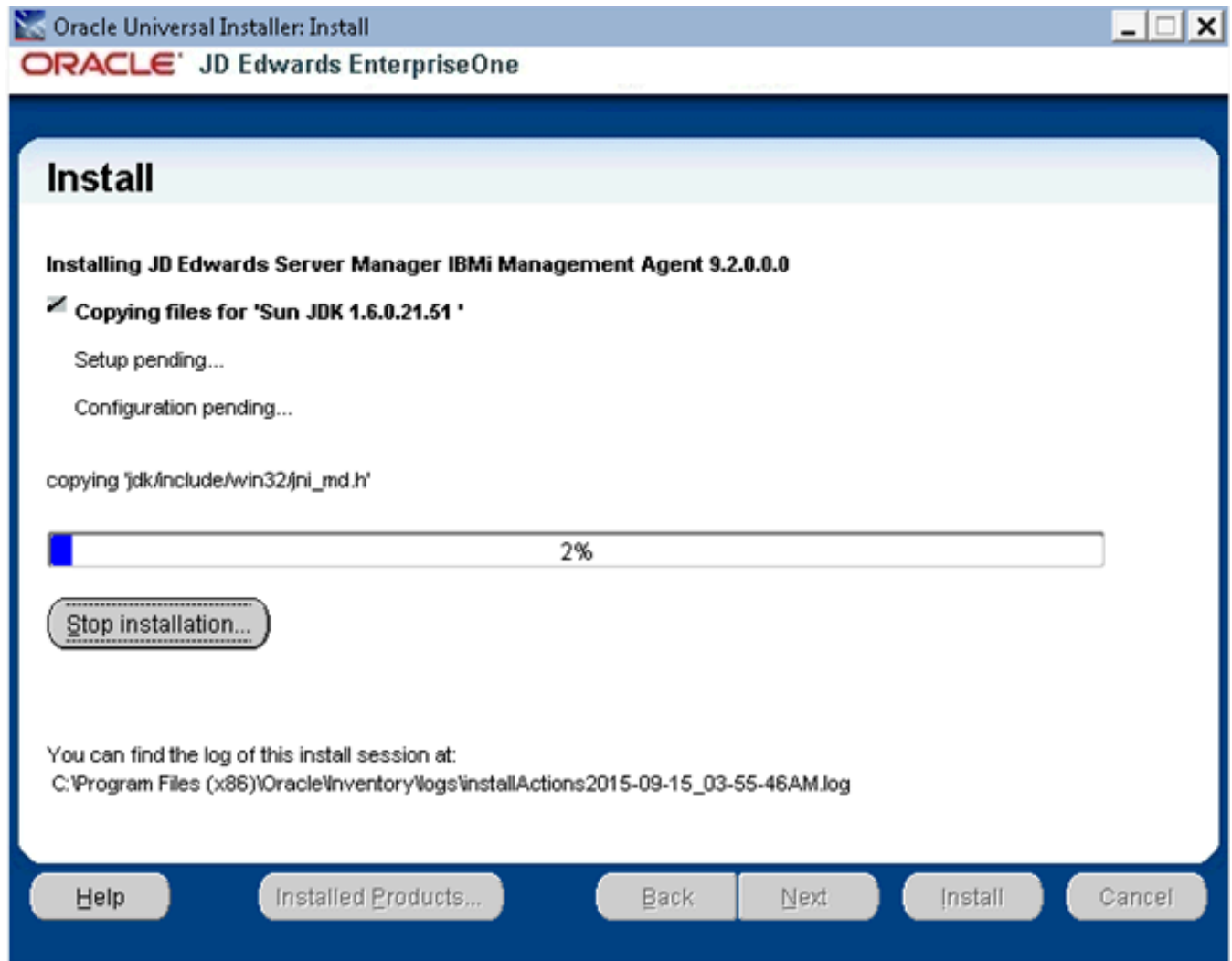
YES - SMC runs on SSL

NO - SMC does not run on SSL

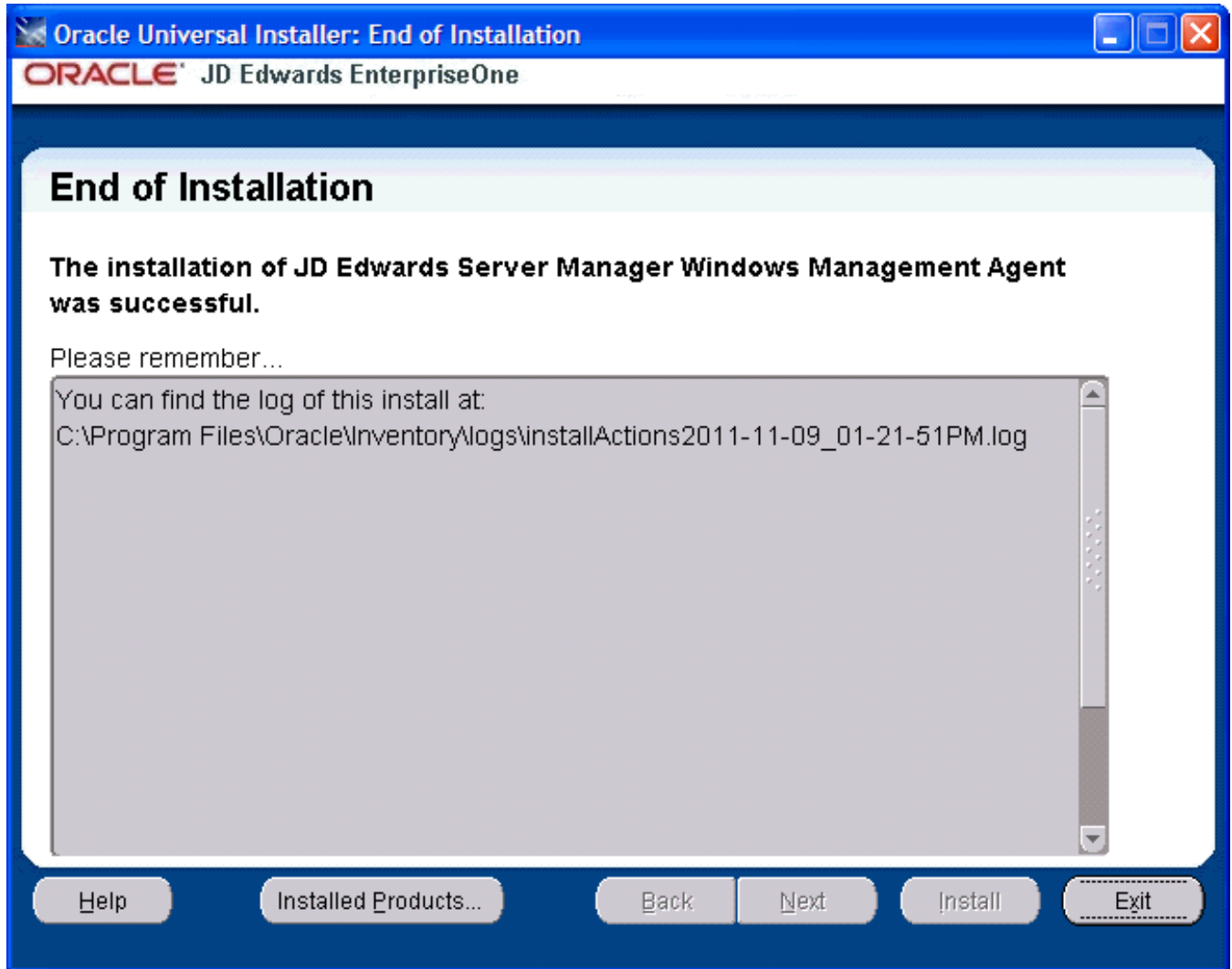
8. Click the **Next** button to verify the machine and port values.



9. On Summary, review the information and click the **Install** button to begin the installation.



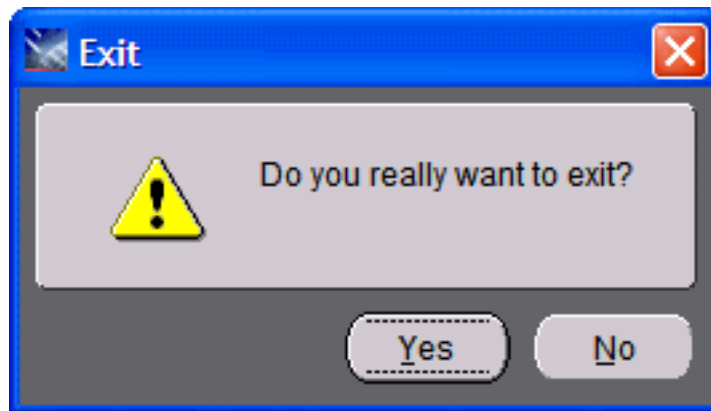
The Management Agent installer displays a panel showing the ongoing status of the installation.



10. When the installation finishes, the End of Installation screen is displayed.

CAUTION: Examine the Installer Logs. This screen also displays the location of the install log. Even though the screen indicates that the installation was successful, you should always check the logs before you attempt to run the Agent. The file name starts with "installActions" and includes a time stamp; it is located in c:\oraInventory\logs directory. For example: `cc:\Program Files\Oracle\Inventory\logs\installActions2018-11-09_01-21-51PM.log`

11. Click the **Exit** button.



12. On the Exit dialog, click the **Yes** button to confirm you want to exit the Management Agent installer.

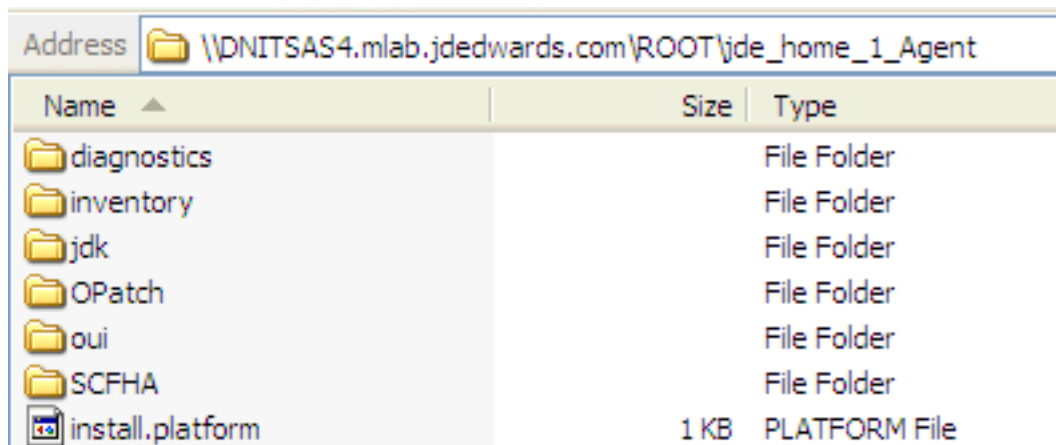
Note:

At the end of the installation of the Management Agent installer for OS/400, an agent installation directory will exist in the IFS directory root on the *IBM i* machine. The name of the directory is:

`jde_home_x_Agent`

where "x", if it exists, is the numeric value to differentiate the `jde_home` if multiple agents exist on this machine.

For example, the IFS structure for the Management Agent install might look like this:



Post Installation Steps for Web Server Instances on WebLogic 11g, WebLogic 12c, WebSphere 7.0, WebSphere 8.5.5.0, or WebSphere 9.0

If you are going to be managing either a WebLogic 11g or 12c Application server or a WebSphere 7.0, 8.5, or 9.0 Application server instance, it is recommended that you to select the same JDK for the Server Manager Agent as the one used by the Application server.

This section describes post installation tasks for these application servers:

- *WebLogic 11g*
- *WebLogic 12c*
- *WebSphere 7.0, WebSphere 8.5, and WebSphere 9.0*

WebLogic 11g

JD Edwards EnterpriseOne applications running under WebLogic Application Server require that the WebLogic server use a 64-bit JVM. In order to successfully manage a WebLogic server, you must select the same JDK for the Server Manager Agent as that being used by Weblogic server.

WebLogic 12c

JD Edwards EnterpriseOne applications running under the WebLogic Application Server require that the WebLogic server use a 64-bit JVM. In order to successfully manage a WebLogic server, you must select the same JDK for the Server Manager Agent as that being used by Weblogic server.

WebSphere 7.0, WebSphere 8.5, and WebSphere 9.0

The WebSphere 7.0 Application server uses version 1.6 JVM. In order to successfully manage a WebSphere 7.0 server, you must select the same JDK for the Server Manager Agent as that being used by the WebSphere 7.0 server.

The WebSphere 8.5.x Application Server uses version 1.7 JVM. In order to successfully manage a WebSphere 8.5.x server, you must select the same JDK for the Server Manager Agent as that being used by the WebSphere 8.5.x server.

The WebSphere 9.0 Application Server uses version 1.8 JVM. In order to successfully manage a WebSphere 9.0 server, you must select the same JDK for the Server Manager Agent as that being used by the WebSphere 9.0 server.

Troubleshoot the Management Agent Installation

This section describes:

- *Management Agent Installer Failed*
- *Management Agent Does Not Start*
- *Management Agent Dies on Unix or IBM i*
- *Management Agent Cannot Manage the Application Server on Unix*
- *Management Agent Cannot Start or Stop a Unix Enterprise Server*
- *Management Agent Cannot Manage Secure Servers on WebSphere Application Server on IBM i*
- *Management Agent Install Handshake Exception*

Management Agent Installer Failed

If the Management Agent installer fails to complete, an exception screen is displayed. For details, examine the log file located in the `oracle\Inventory\logs` directory:

Tip:

The log file location is displayed on the End of Installation screen for the Management Agent installer. Refer to the section of this guide entitled: *Run the Management Agent Installer*.

For example, the complete path and log file name might be:

```
C:\Program Files\Oracle\Inventory\logs\installActions2018-10-18-02-15-14PM.log
```

Management Agent Does Not Start

If the *Management Agent* does not start, verify that the port that the home agent is using is not used by another application. To determine the port that the home agent is using, view the `e1agent_0.log` file that is located in the root of specified installation drive in the installation directory of the *Managed Home* (the default value is `JDE_HOME`). This location is shown on the End of Installation screen when you installed the Management Console. For example:

```
C:\Program Files\Oracle\Inventory\logs\installActions2018-10-18-02-15-14PM.log
```

The log file should contain this message:

```
INFO: Starting the management agent listener on port 'xxxxx'
```

Management Agent Dies on Unix or IBM i

You must use the `&` switch when invoking the `startAgent` script to start the *Management Agent* as a background job. If you do not use the `&` switch, the *Management Agent* process terminates when the shell is exited on UNIX or shell is exited on *IBM i*.

Management Agent Cannot Manage the Application Server on Unix

Ensure that you have installed the *Management Agent* with the same user and group as the Application Server. Use a directory listing to confirm that this is the case.

For example, this listing illustrates that the *Management Agent* was installed with `user=oracle` and `group=oinstall`:


```
[root@denlcm1x2 u02]# ls -al oas-home-agent/
total 68
drwxr-xr-x   14 oracle   oinstall   4096 Sep 17 09:29 .
drwxrwxrwx   11 root     root       4096 Sep 12 09:37 ..
-rw-r--r--    1 oracle   oinstall    6 Sep 17 09:29 agent.pid
drwxrwxrwx    2 oracle   oinstall   4096 Jul 31 14:28 bin
drwxrwxrwx    7 oracle   oinstall   4096 Jul 31 14:28 ocr
drwxr-xr-x    2 oracle   oinstall   4096 Sep 12 10:47 components
drwxr-xr-x    2 oracle   oinstall   4096 Jul 31 14:27 config
drwxr-xr-x    2 oracle   oinstall   4096 Sep 17 09:29 data
drwxrwxrwx    6 oracle   oinstall   4096 Jul 31 14:28 jdk
drwxr-xr-x    4 oracle   oinstall   4096 Jul 31 14:27 _jvm
drwxr-xr-x    3 oracle   oinstall   4096 Sep 18 15:23 lib
drwxr-xr-x    2 oracle   oinstall   4096 Sep 17 09:29 logs
drwxr-xr-x    2 oracle   oinstall   4096 Jul 31 14:27 META-INF
-rw-r--r--    1 oracle   oinstall  7996 Jul 31 14:28 smha_is_install.log
drwxr-xr-x    7 oracle   oinstall   4096 Sep 19 14:24 targets
drwxr-xr-x    2 oracle   oinstall   4096 Jul 31 14:28 _uninst
[root@denlcm1x2 u02]#
```

If the *Management Agent* is not installed as the correct user or group, use the `chown` command to change the owner or group of the *Management Agent* . For example:

```
chown R oracle:oinstall /u02/JDE_HOME
```

Management Agent Cannot Start or Stop a Unix Enterprise Server

If you are using the *Management Agent* to manage a Unix Enterprise Server, you must install the *Management Agent* with the same user and group as the Unix Enterprise Server. Use a directory listing to confirm that this is the case.

For example, this listing illustrates that the *Management Agent* was installed with `user=jde812` and `group=jde812`:

```
[root@denlcmly2 u02]# ls -al management-agent/
total 68
drwxr-xr-x 14 jde812  jde812      4096 Sep 17 09:30 .
drwxrwxrwx 11 root    root      4096 Sep 12 09:37 ..
-rw-rw-r-- 1 jde812  jde812        6 Sep 17 09:30 agent.pid
drwxrwxrwx 2 jde812  jde812      4096 Sep 12 10:45 bin
drwxrwxrwx 7 jde812  jde812      4096 Jul 12 10:26 ocr
drwxr-xr-x 2 jde812  jde812      4096 Sep 12 10:39 components
drwxr-xr-x 2 jde812  jde812      4096 Jul 31 13:19 config
drwxr-xr-x 2 jde812  jde812      4096 Sep 17 09:30 data
drwxrwxrwx 6 jde812  jde812      4096 Jul 12 10:26 jdk
drwxr-xr-x 4 jde812  jde812      4096 Jul 12 10:25 _jvm
drwxr-xr-x 3 jde812  jde812      4096 Sep 12 10:32 lib
drwxr-xr-x 2 jde812  jde812      4096 Sep 17 09:30 logs
drwxr-xr-x 2 jde812  jde812      4096 Jul 12 10:25 META-INF
-rw-r--r-- 1 jde812  jde812     8007 Jul 12 10:26 scfha_is_install.log
drwxr-xr-x 4 jde812  jde812      4096 Sep 12 09:58 targets
drwxr-xr-x 2 jde812  jde812      4096 Jul 12 10:26 _uninst
```

If the *Management Agent* is not installed as the correct user or group, use the `chown` command to change the owner or group of the *Management Agent* . For example:

```
chown R jde900:jde900 /u02/JDE_HOME
```

Management Agent Cannot Manage Secure Servers on WebSphere Application Server on IBM i

If you have trouble connecting to servers in a WAS profile for which administrative security is set to *enabled*, ensure that you have JDK 1.5 installed on the *IBM i* machine. The *Management Agent* needs security libraries from JDK 1.5 to connect to secure servers in WebSphere Application Server.

Tip:

The typical location for the JDK is:

```
/QIBM/ProdData/java400/jdk15
```

Management Agent Install Handshake Exception

You must enable the SSL/TLS for the Server Manager Console in the WebLogic Server if the exception `javax.net.ssl.SSLHandshakeException` is displayed while installing the Server Manager Management Agent.

User this procedure to enable TLS/SSL for the Server Manager Console in the WebLogic Server:

1. Access the WebLogic Admin Console in the browser for the WebLogic domain in which the Server Manager Console is installed.

The following is an example URL:

```
https://denpbds11.example.com:7001/console
```

2. Login to the WebLogic Admin Console using your WebLogic administrative credentials.
3. Navigate to Environments > Servers.
4. Click on this server: **Server Manager Console**.

Note: The example screen shot in this section shows the **SMC_Server_EOne_ManagementConsole1_Console**.

5. Click the **Lock and Edit** option if available.
6. Verify that you are in the General > Server Start tab.
7. Select the **Arguments** text box.

8. Add the following argument: `-Dweblogic.security.SSL.minimumProtocolVersion=TLSv1` Refer to the following example.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled "Settings for SMC_Server_EOne_ManagementConsole1_Console" and is under the "Server Start" tab. The "Arguments" field is populated with the command: `e:/SCFMC -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1`. Other visible fields include "Java Home", "Java Vendor", "BEA Home", "Root Directory", "Class Path", "Security Policy File", "User Name", and "Password". The left sidebar shows the "Domain Structure" tree and "System Status" section.

9. Click the **Save** button.

ORACLE WebLogic Server Administration Console 12c

Change Center

View changes and restarts

Pending changes exist. They must be activated to take effect.

Domain Structure

- jde_domain
 - Environment
 - Servers
 - Clusters
 - Coherence Clusters
 - Machines
 - Virtual Hosts
 - Work Managers
 - Startup and Shutdown Classes
 - Deployments
 - Services
 - Security Realms
 - Interoperability
 - Diagnostics

How do I...

- Configure startup arguments for Managed Servers
- Start Managed Servers from the Administration Console
- Shut down a server instance

System Status

Health of Running Servers

	Failed (0)
	Critical (0)
	Overloaded (0)
	Warning (0)
	OK (2)

Home Log Out Preferences Record Help

Home > Summary of Servers > SMC_Server_EOne_ManagementConsole1_Console

Messages

Settings updated successfully.

Settings for SMC_Server_EOne_ManagementConsole1_Console

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Health Monitoring **Server Start** Web Servi

Node Manager is a WebLogic Server utility that you can use to start, suspend, shut down, and restart servers in normal or unexpected conditions. Use this page to configure the

Java Home:

Java Vendor:

BEA Home:

Root Directory:

Class Path:

Arguments:

```
-Djde.home=/u01/SMConsole/SCFMC -Dweblogic.security.SSL.mini
```

10. Click the **Activate Changes** button.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled 'Settings for SMC_Server_EOne_ManagementConsole1_Console' and is under the 'Server Start' tab. A message at the top states: 'All changes have been activated. No restarts are necessary.' Below this, there are several configuration fields: 'Java Home', 'Java Vendor', 'BEA Home', 'Root Directory', 'Class Path', and 'Arguments'. The 'Arguments' field contains the text: '-Djde.home=/u01/SMConsole/SCFMC -Dweblogic.security.SSL.mini'. On the left side, the 'Change Center' panel is visible, showing 'View changes and restarts' and 'Lock & Edit' buttons. The 'System Status' panel shows 'Health of Running Servers' with a bar chart indicating 2 OK servers.

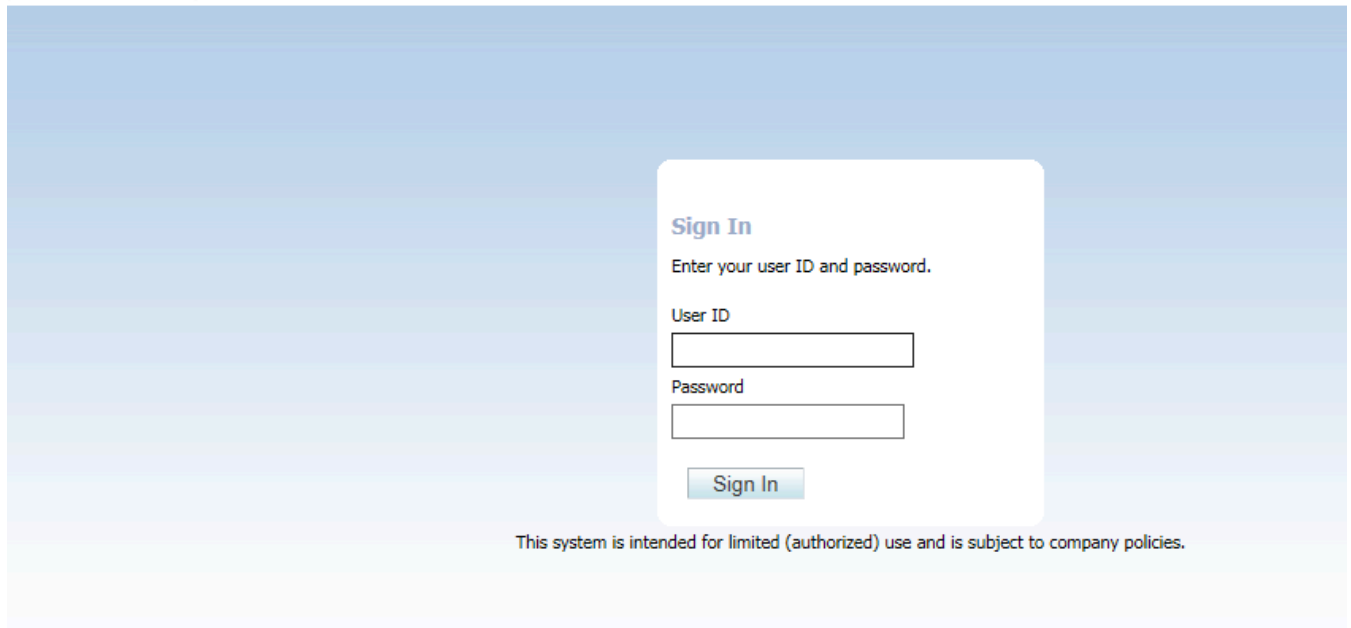
11. Restart the Server Manager Console j2ee server if required.
12. Stop and then start the Server Manager Console J2ee server if required.

13. Access the Server Manager Console in the browser using an HTTPS/SSL based URL. For example: `https://<Server_Manager_Console_HostName>:<SSL_Listen_Port>/manage/home`

In the following screenshot the URL is:

`https://denpbds11.example.com:9000/manage/home`

ORACLE JD Edwards EnterpriseOne Server Manager



14. Install the Server Manager Management Agent over this SSL port.

Deinstall a Management Agent

Any *Managed Instances* registered or installed with a *Managed Home* must be removed before the *Managed Home* itself can be deinstalled. For instructions on removing an instance, refer to the chapter of the *Server Manager Guide* guide entitled: *Remove a Managed Instance*.

You must deinstall a *Management Agent* running the Oracle Universal Installer on the same machine that was originally used to install it.

This section describes deinstallation of the Management for these platforms:

- *Microsoft Windows and UNIX*
- *IBM i OS/400*

Microsoft Windows and UNIX

Use this procedure to deinstall the Management Agent from Microsoft Windows and UNIX target machines. The Oracle Universal Installer must be used to properly deinstall the Management Agent.

CAUTION: You must deinstall a *Management Agent* using the Oracle Universal Installer on the same machine that was originally used to install it.

CAUTION: If you will no longer use Server Manager on the machine on which you wish to deinstall the agent, before you deinstall the agent you should first deinstall any Server Manager-installed software components. Otherwise once the agent is deinstalled you will no longer be able to deinstall those components.

Note: The JRE or JDK that was specified during installation was copied to the Oracle Home (for example, installation directory); the deinstaller uses that same JRE or JDK when it is run so no `-jreLoc` argument is needed.

1. Launch Oracle Universal Installer:

- o **Microsoft Windows**

`Disk1/install/setup.exe`

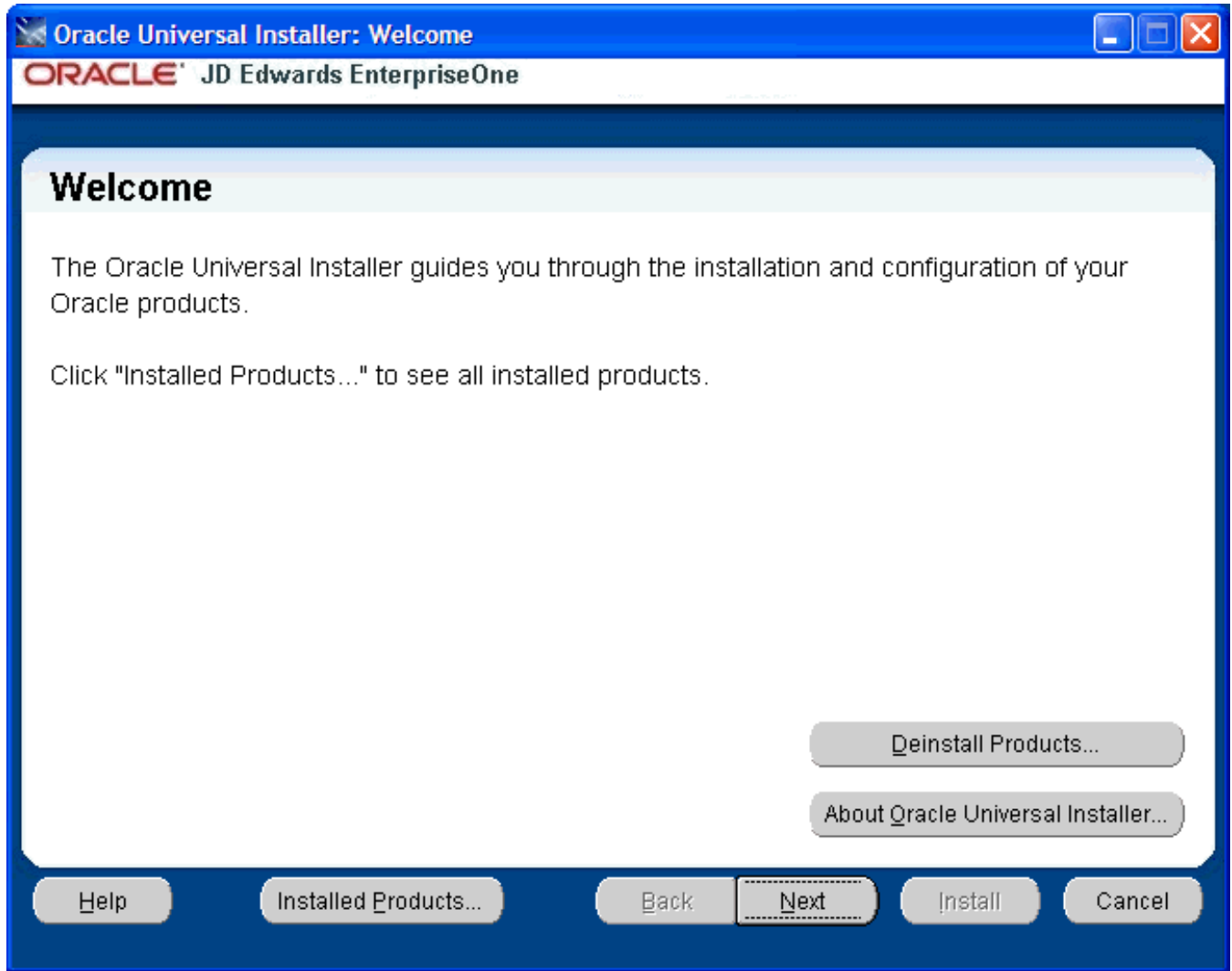
Alternately, you can navigate Start > Oracle - E1_Management_Agent_x > Oracle Installation Products > Universal Installer

where "x", if it exists, is the numeric value of the Management Agent that you want to deinstall.

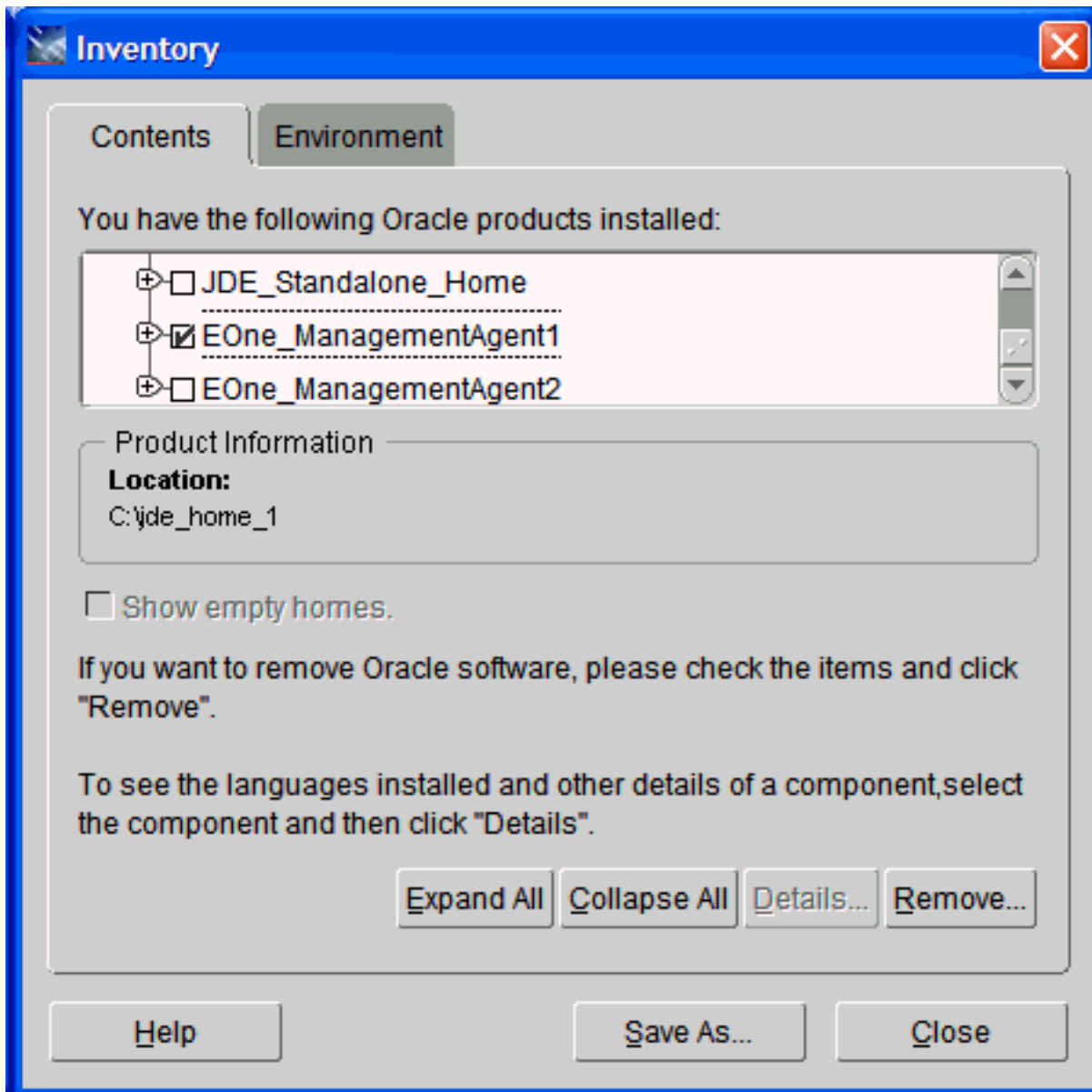
- o **UNIX**

`/<installation_home>/oui/bin/runInstaller.sh`

After the OUI installer is launched, the Welcome screen is displayed.



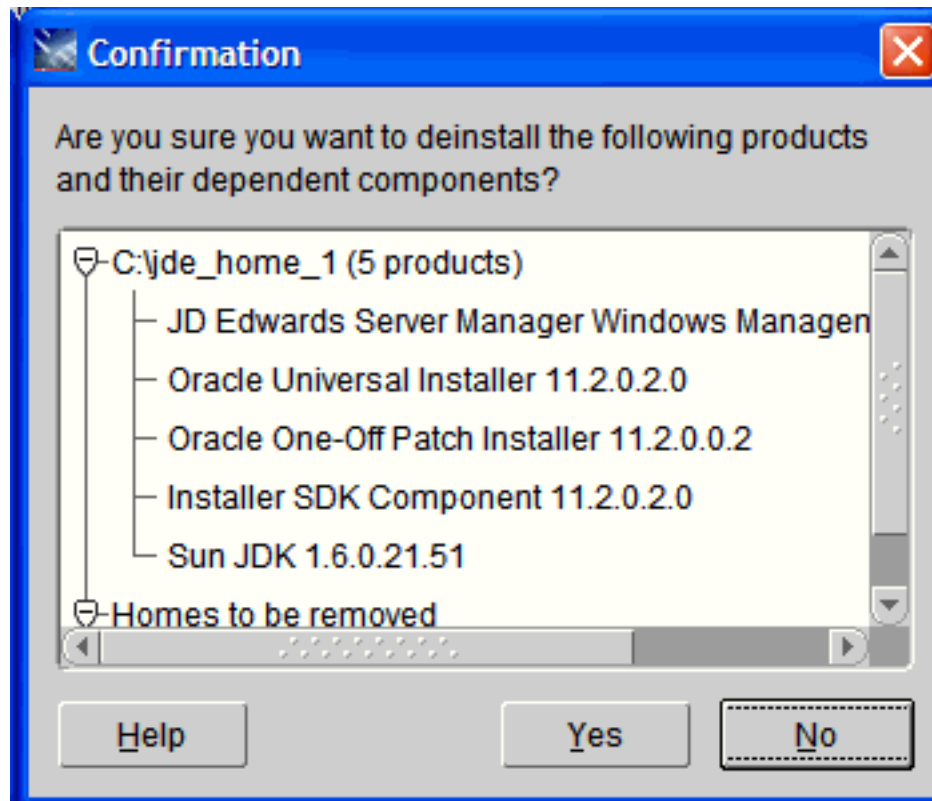
2. On Welcome, click the **Deinstall Products...** button.



3. On Inventory, with the Contents tab selected, select the check box for the Management Agent that you want to deinstall. For example:

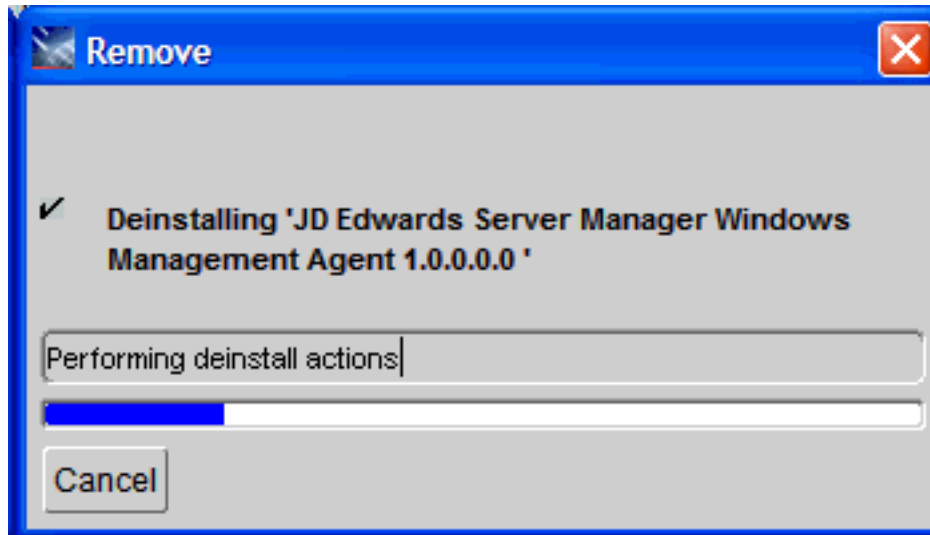
EOne_ManagementAgent1

4. Click the **Remove** button.

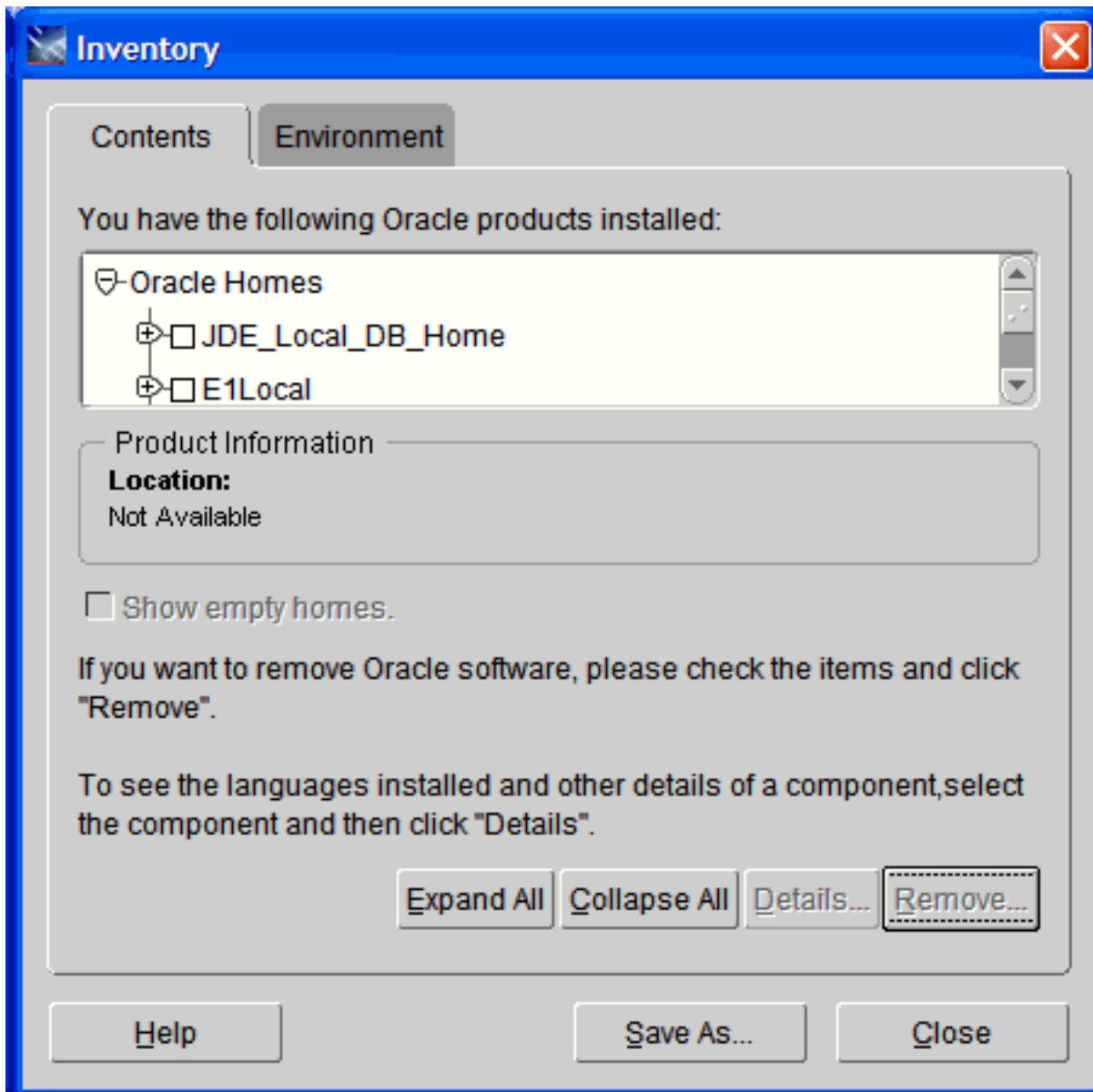


5. On Confirmation, ensure the selected **jde_home** on the target machine is that of the Management Agent that you want to install, and click the **Yes** button.

A deinstallation progress panel is displayed:

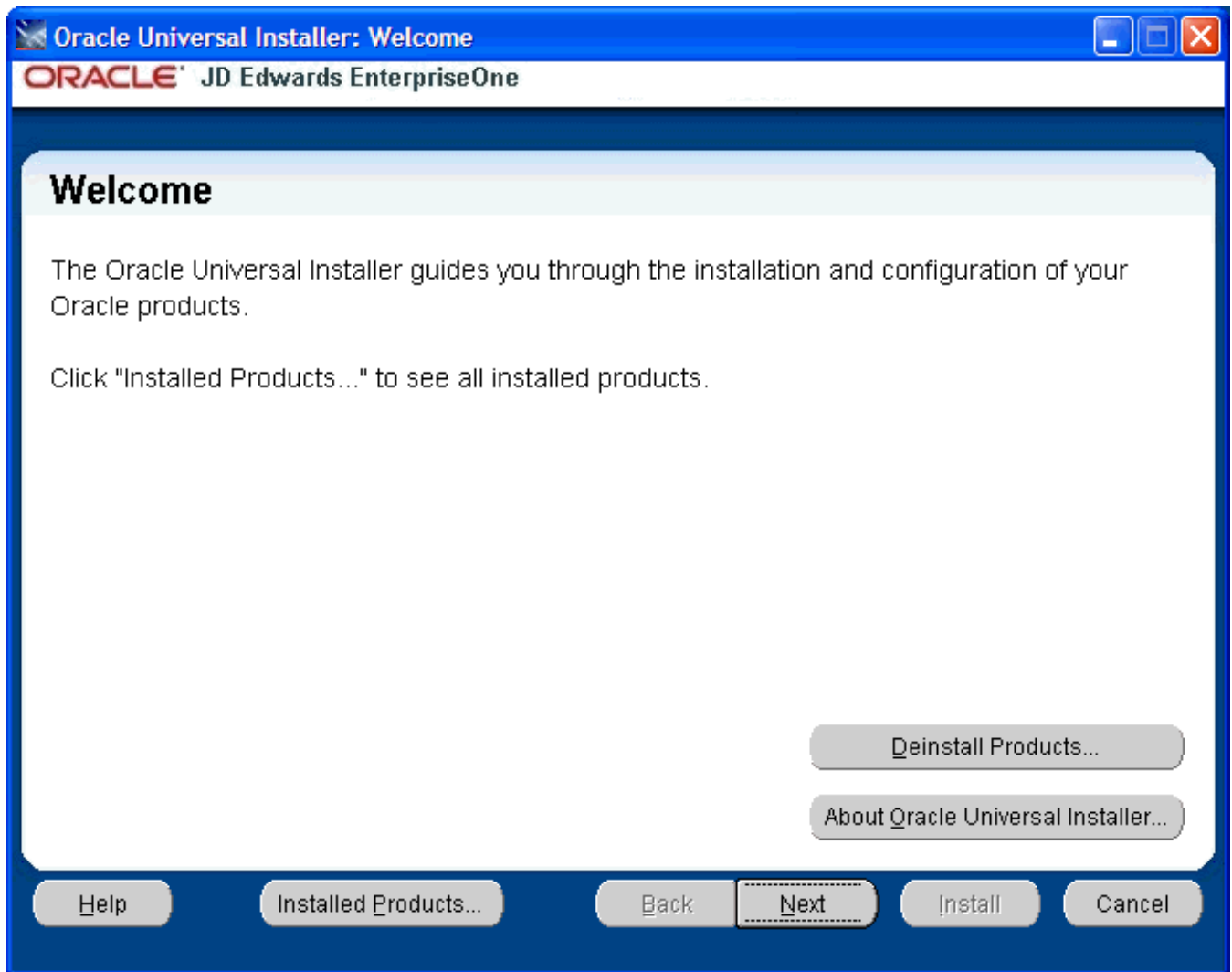


When the deinstallation complete, the Inventory screen is displayed.

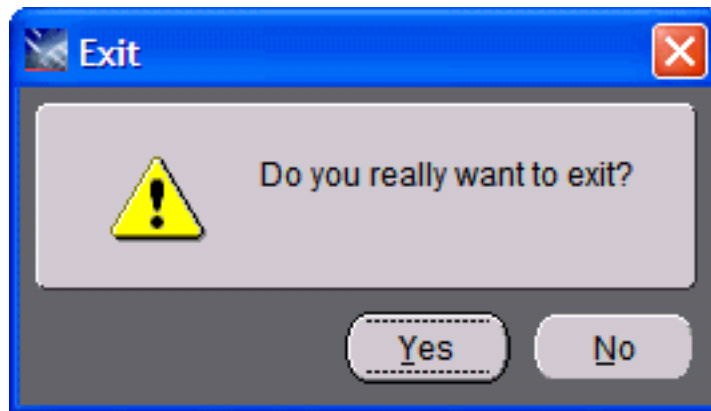


6. On Inventory, verify that the selected home for the Management Agent that you deinstalled is not displayed.

7. Click the **Close** button to close the Inventory panel and return to OUI.



8. On Welcome, click the **Cancel** button to exit the installer.



9. On the Exit dialog, click the **Yes** button to confirm you want to exit the installer.

IBM i OS/400

Use this procedure to deinstall the Management Agent from *IBM i OS/400* target machines. The Oracle Universal Installer must be used to properly deinstall the Management Agent.

CAUTION: You must deinstall a *Management Agent* running the Oracle Universal Installer on the same Microsoft Windows machine that was originally used to install it.

CAUTION: If you will no longer use Server Manager on the machine on which you wish to deinstall the agent, before you deinstall the agent you should first deinstall any Server Manager-installed software components. Otherwise once the agent is deinstall you will no longer be able to deinstall those components.

Note: The JRE or JDK that was specified during installation was copied to the Oracle Home (for example, installation directory); the deinstaller uses that same JRE or JDK when it is run so no `-jreLoc` argument is needed.

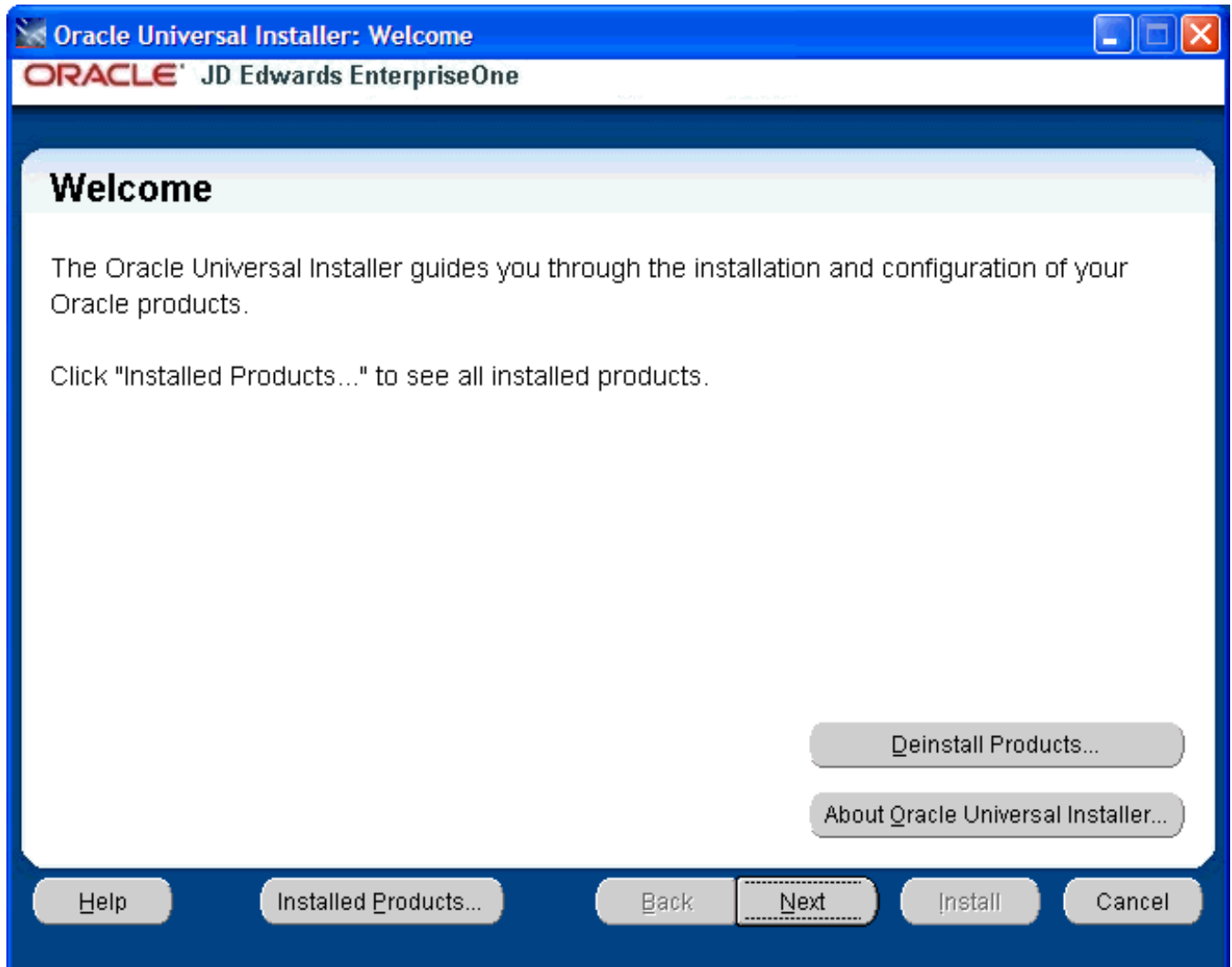
1. Launch Oracle Universal Installer from this location:

Disk1/install/setup.exe

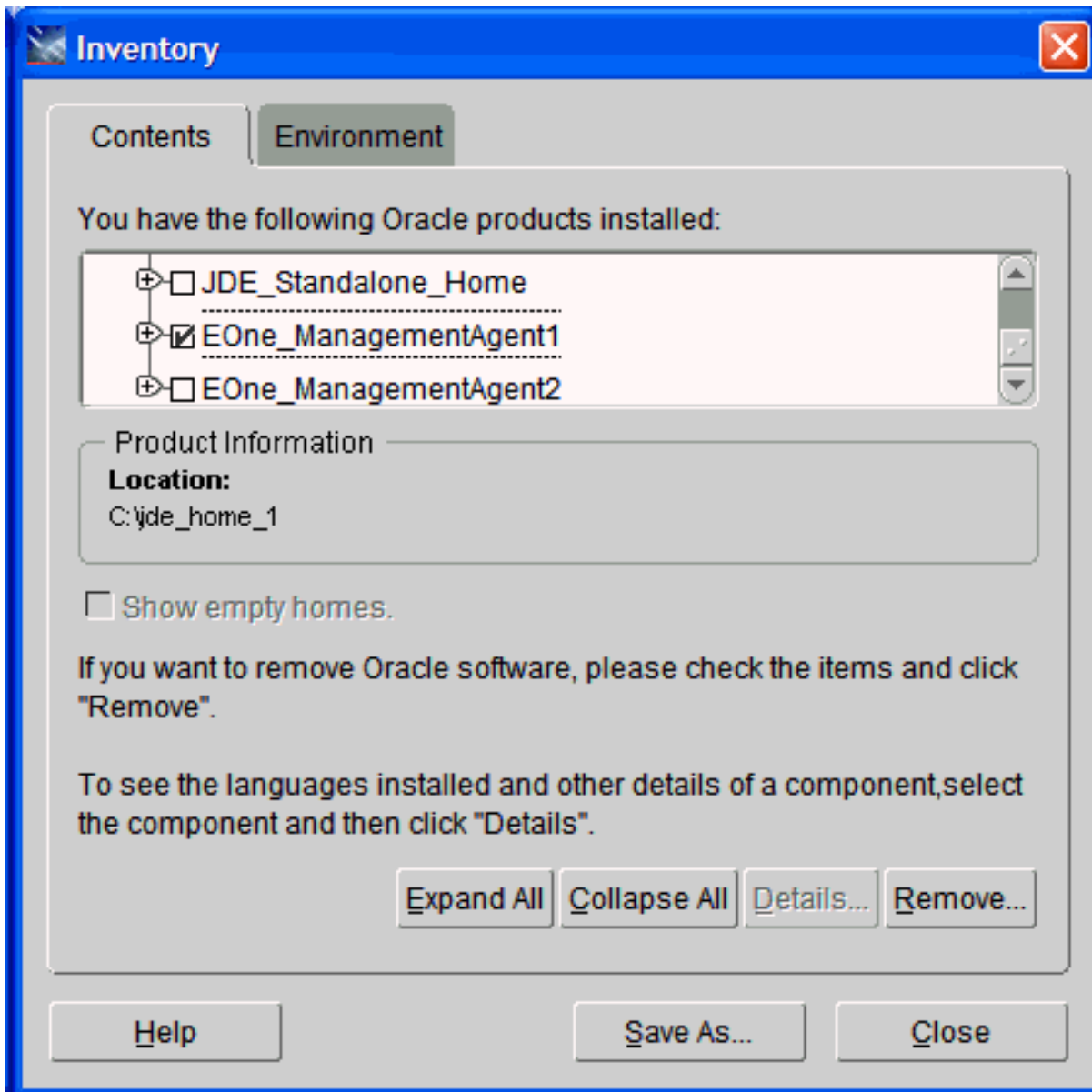
Alternately, you can navigate Start > Oracle - E1_Management_Agent_x > Oracle Installation Products > Universal Installer

where "x", if it exists, is the numeric value of the Management Agent that you want to deinstall.

After the OUI installer is launched, the Welcome screen is displayed.



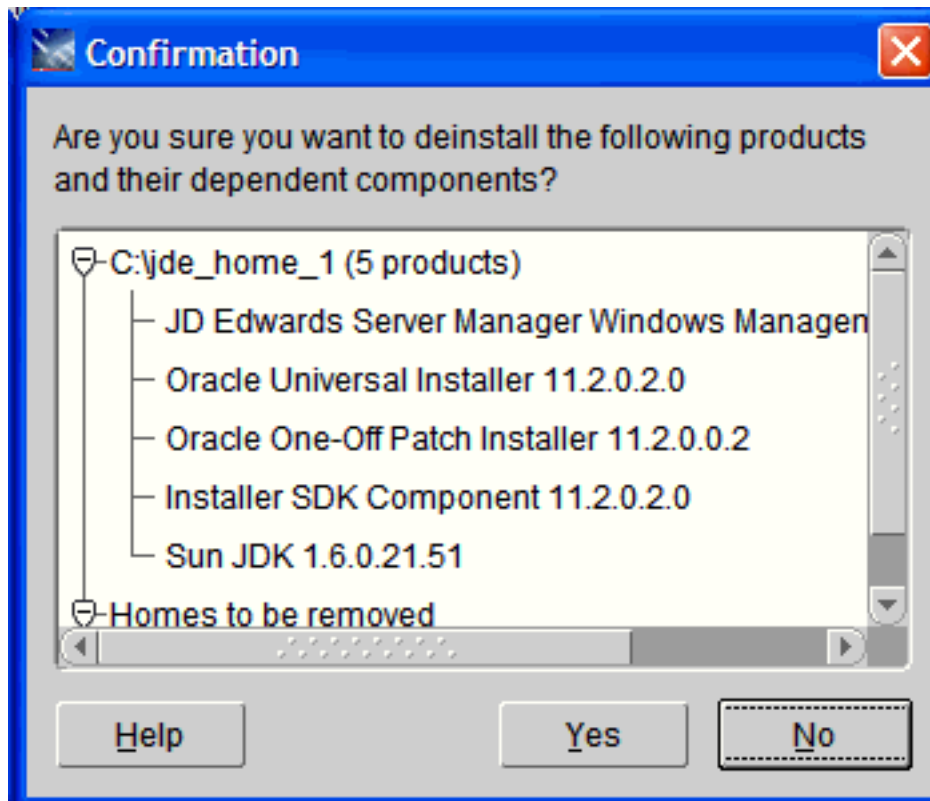
2. On Welcome, click the **Deinstall Products...** button.



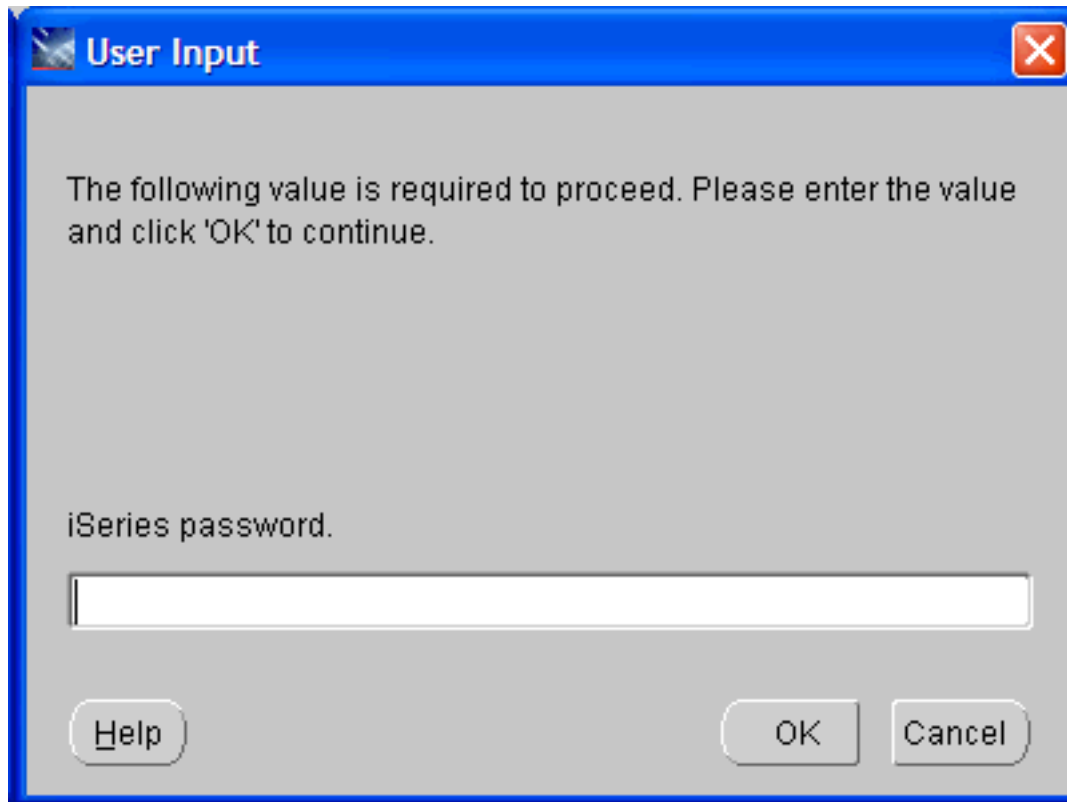
3. On Inventory, with the Contents tab selected, select the check box for the Management Agent that you want to deinstall. For example:

EOne_ManagementAgent1

4. Click the **Remove** button.

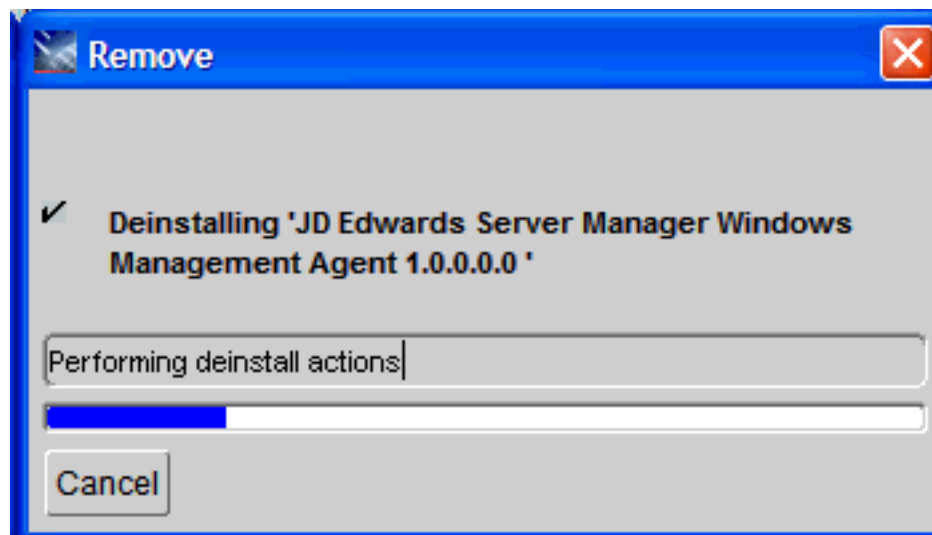


5. On Confirmation, ensure the selected **jde_home** on the target machine is that of the Management Agent that you want to install, and click the **Yes** button.

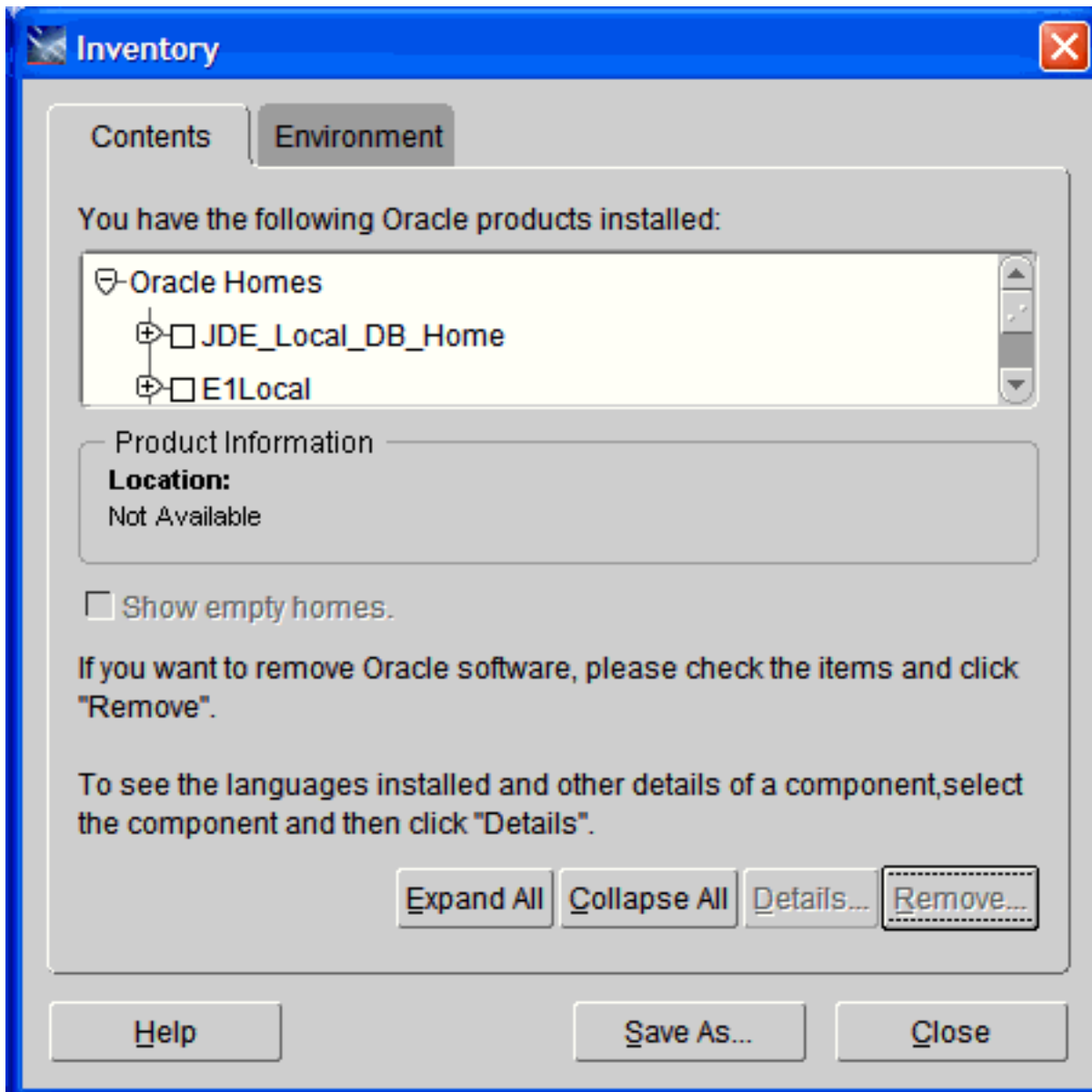


6. On the User Input dialog, enter the iSeries password.
7. Click the **OK** button.

A deinstallation progress panel is displayed:

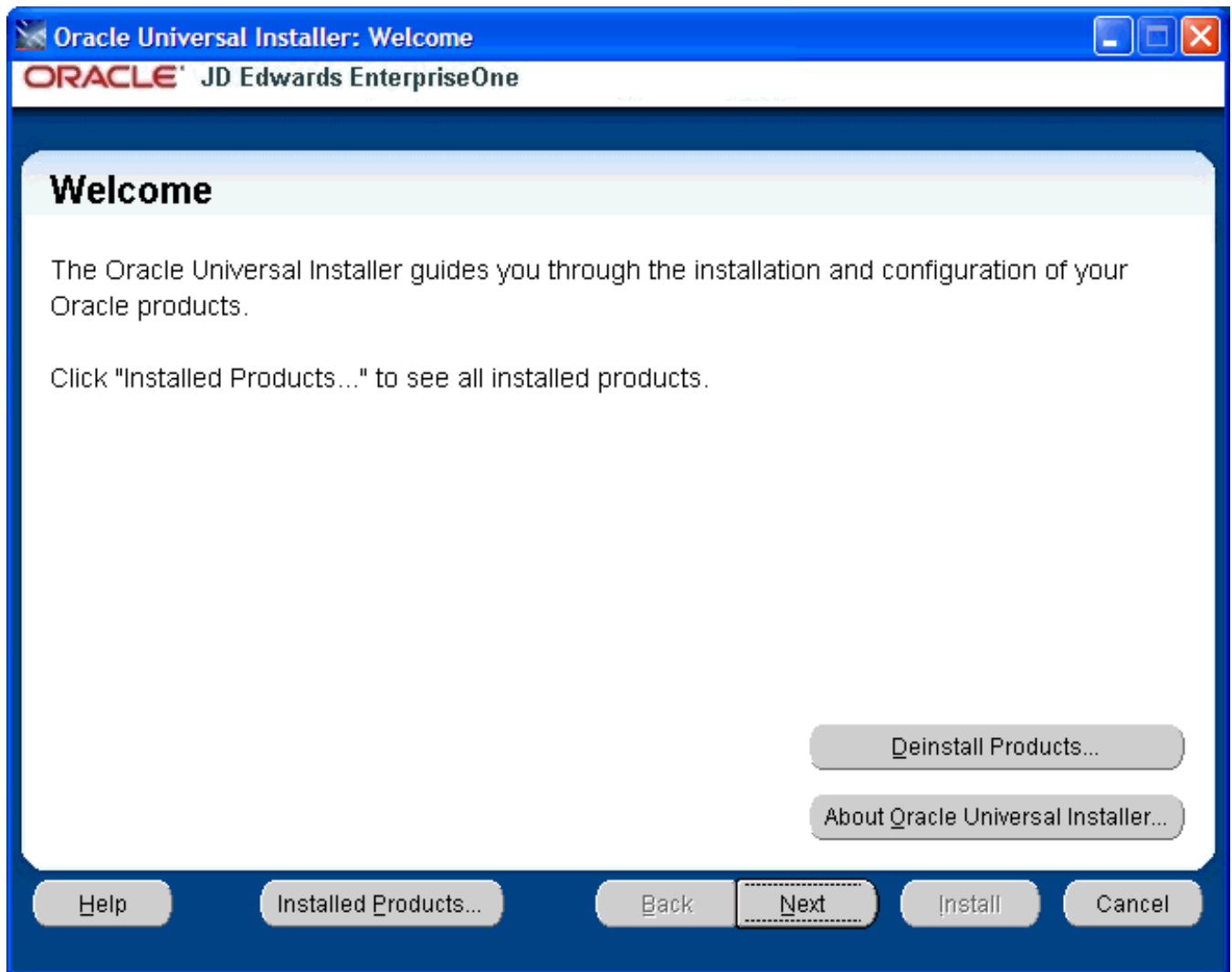


- When the deinstallation complete, the Inventory screen is displayed.

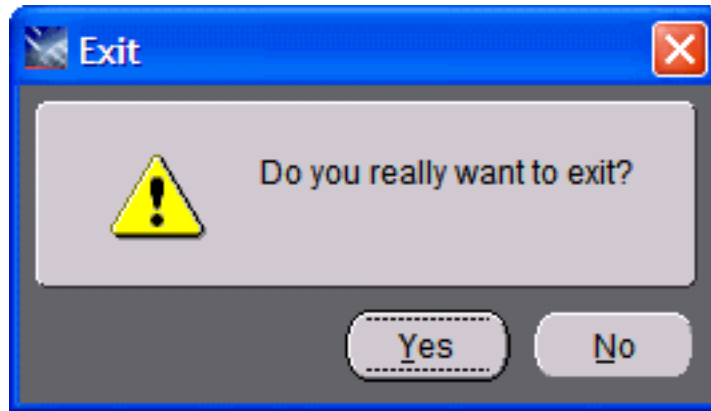


- On Inventory, verify that the selected home for the Management Agent that you deinstalled is not displayed.

10. Click the **Close** button to close the Inventory panel and return to OUI.



11. On Welcome, click the **Cancel** button to exit the installer.



12. On the Exit dialog, click the **Yes** button to confirm you want to exit the installer.

3 Uninstall the Server Manager Management Console

Uninstall the Server Manager Management Console

CAUTION: If you uninstall the Management Console, you can no longer remotely manage servers associated with that Management Console. Without the Management Console, you cannot deploy updates to servers associated with that Management Console.

CAUTION:

Important Prerequisites. Prior to running the deinstaller/uninstaller, verify the following prerequisites.

WebLogic

Verify that the WebLogic AdminServer and the Nodemanager of the WebLogic Domain is running.

WebSphere

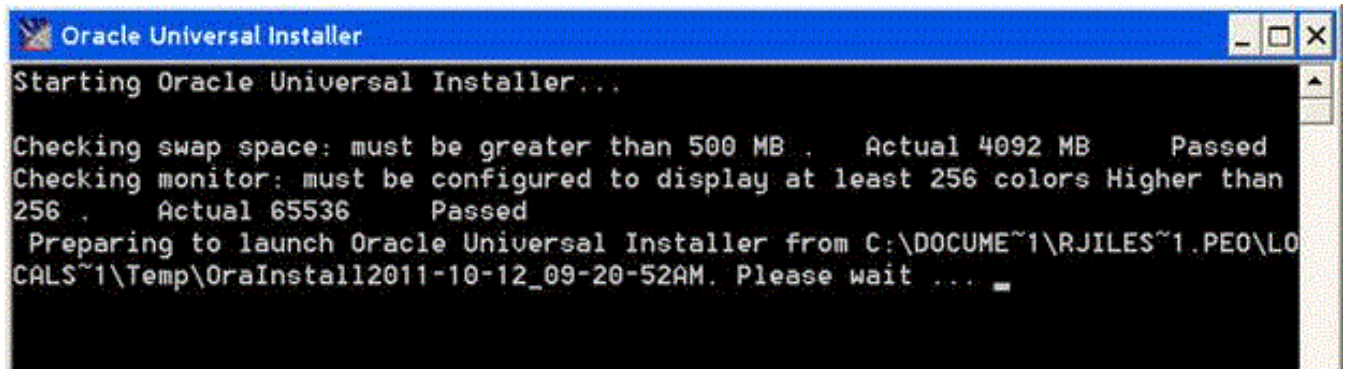
Ensure the Administration Server (or deployment manager) of the WAS Profile is running.

1. Once launched the deinstallation steps are the same for Microsoft Windows and Linux/Solaris platforms. The invocation methods are listed below:

Microsoft Windows

Go to Start > All Programs > Oracle - JDE_Standalone_Home > Oracle Installation Products > Universal Installer.

The Windows Command window starts indicating Windows is preparing to launch OUI.

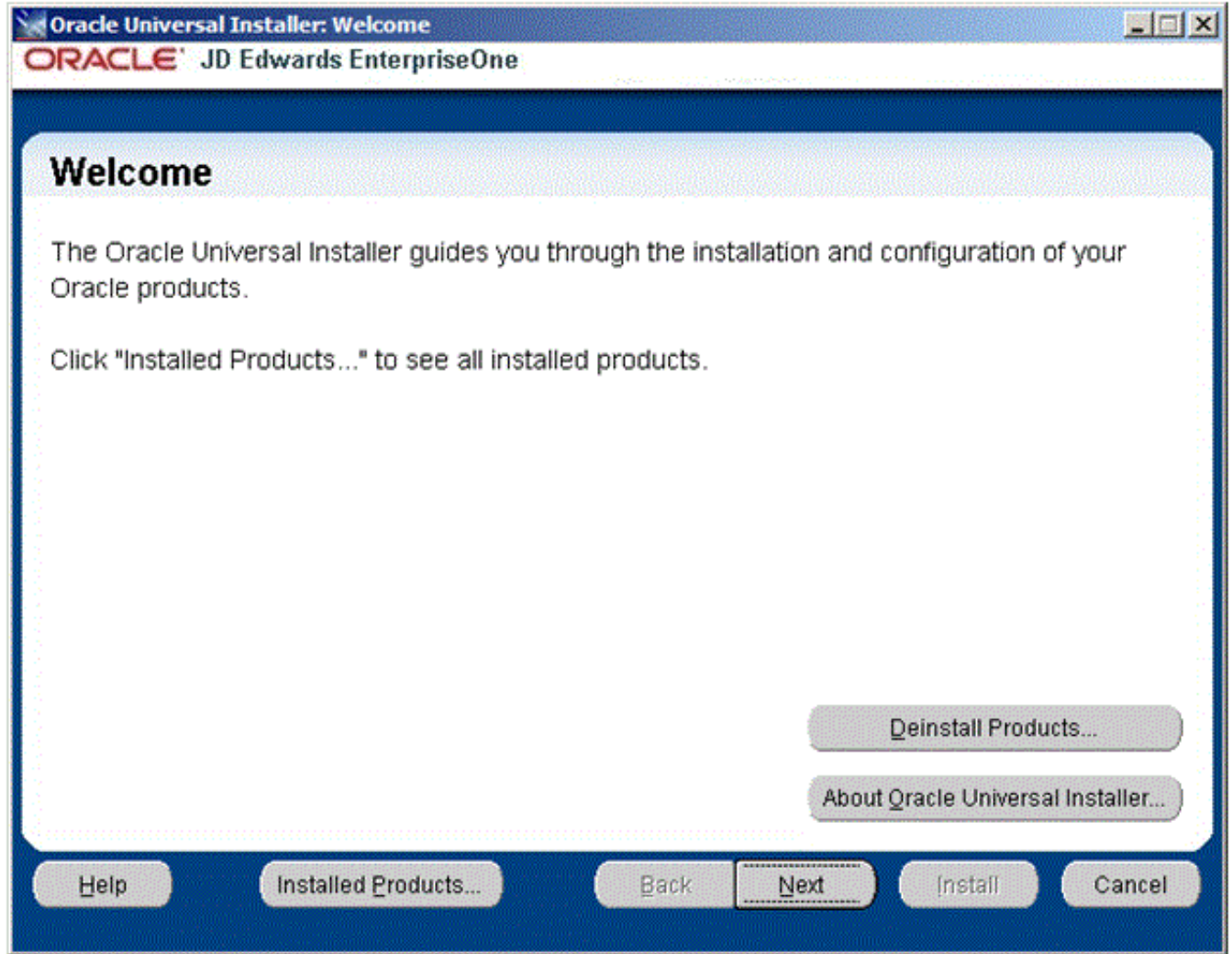


```
Oracle Universal Installer
Starting Oracle Universal Installer...
Checking swap space: must be greater than 500 MB .   Actual 4092 MB   Passed
Checking monitor: must be configured to display at least 256 colors Higher than
256 .   Actual 65536   Passed
Preparing to launch Oracle Universal Installer from C:\DOCUME~1\RJILES~1\PEO\LO
CAL~1\Temp\OraInstall2011-10-12_09-20-52AM. Please wait ...
```

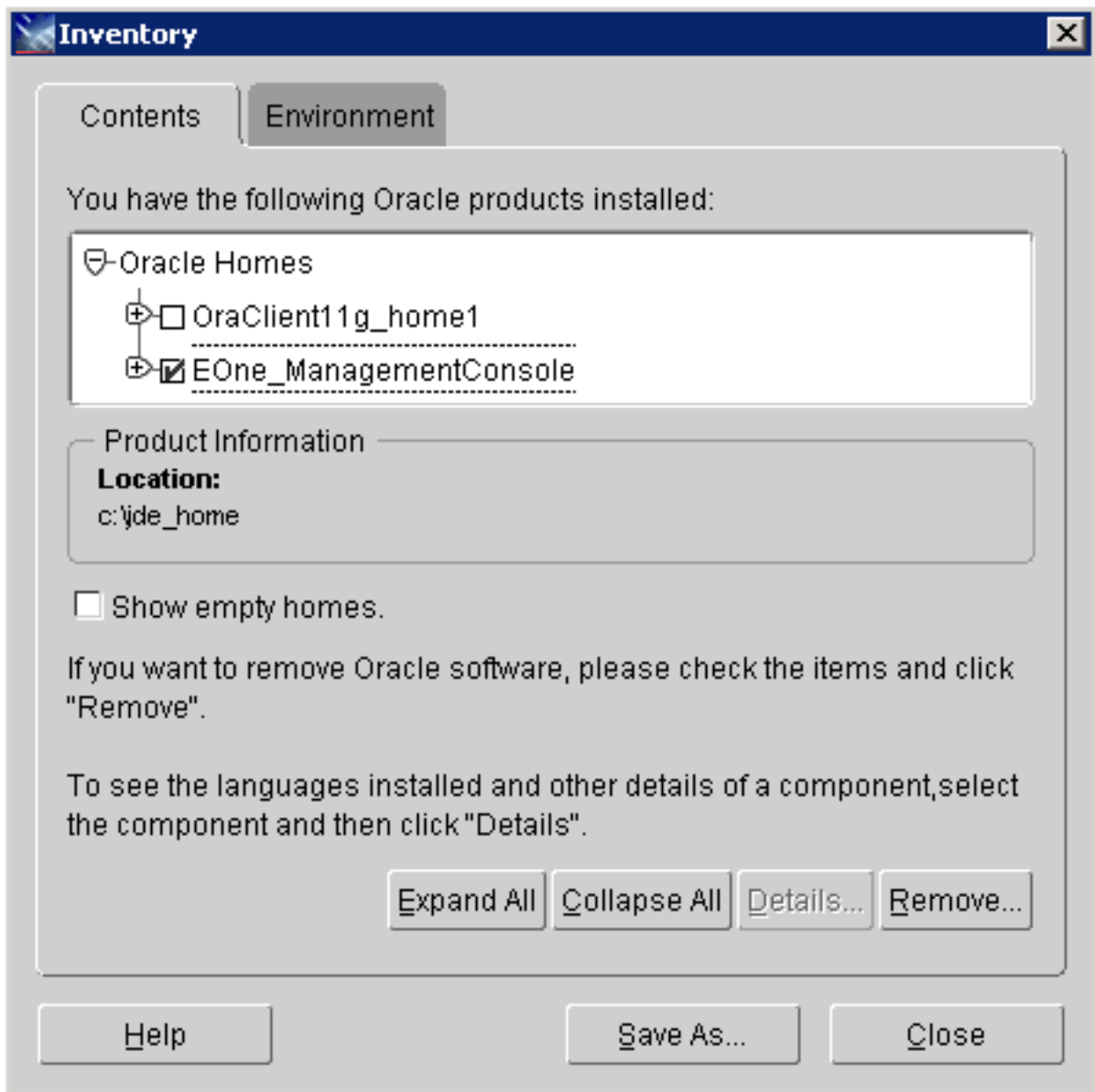
Linux and Solaris

You can invoke the deinstaller/uninstaller by re-running the Server Manager Console installer. If the installer software has been deleted, you can still launch it using this command: `$ORACLE_HOME/oui/runInstaller`

It will take a minute or so for the initialization to complete. Upon completion the OUI Welcome panel displays:

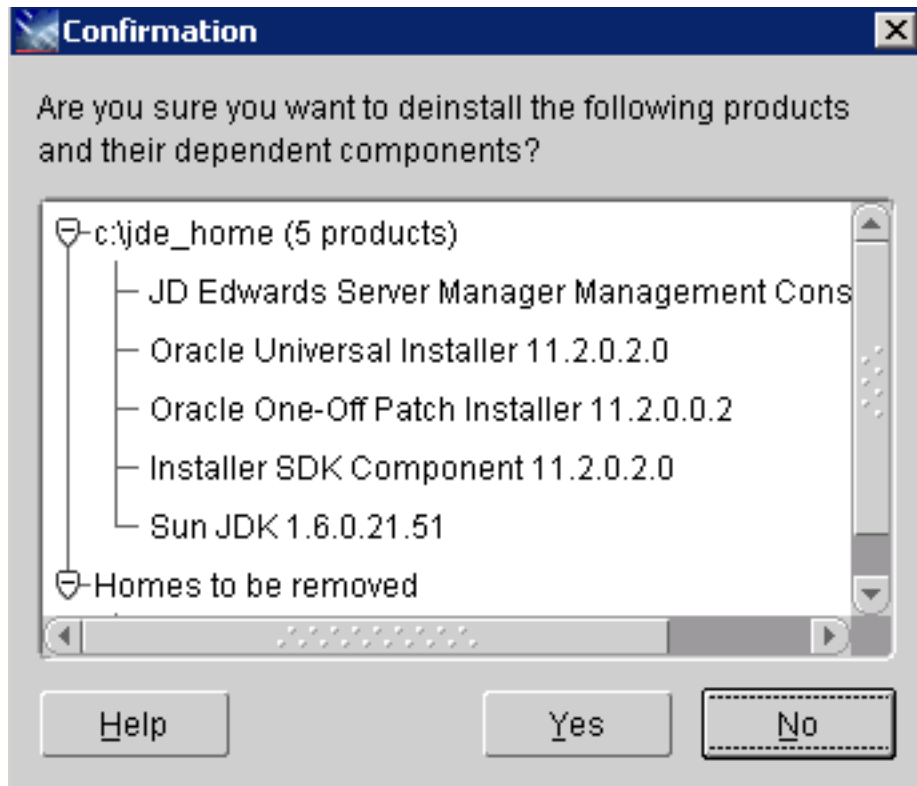


2. On Welcome, click the Deinstall Products ... button.



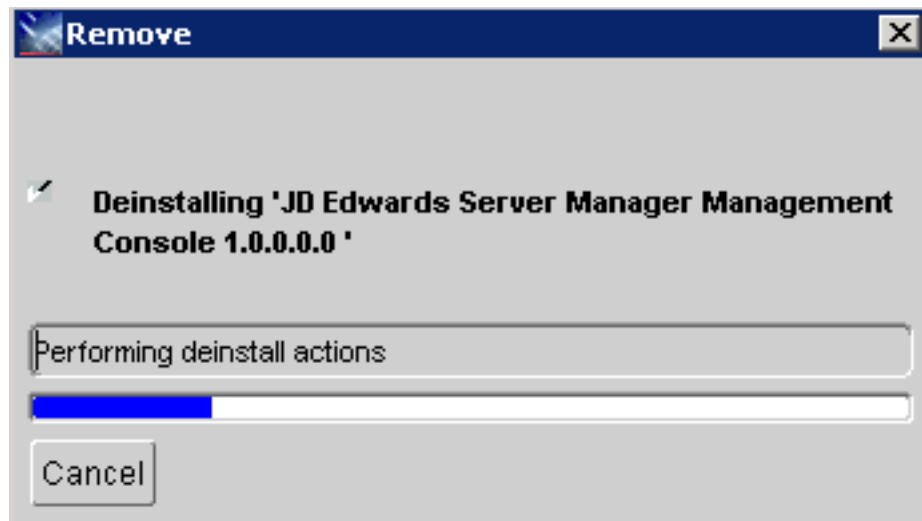
3. On Inventory, select the node under Oracle Homes that corresponds to your Server Manager Management Console installation. For example: EOne_ManagementConsole
4. Once the component to be deinstall is selected, verify the **Location** in the **Product Information** portion of the screen.

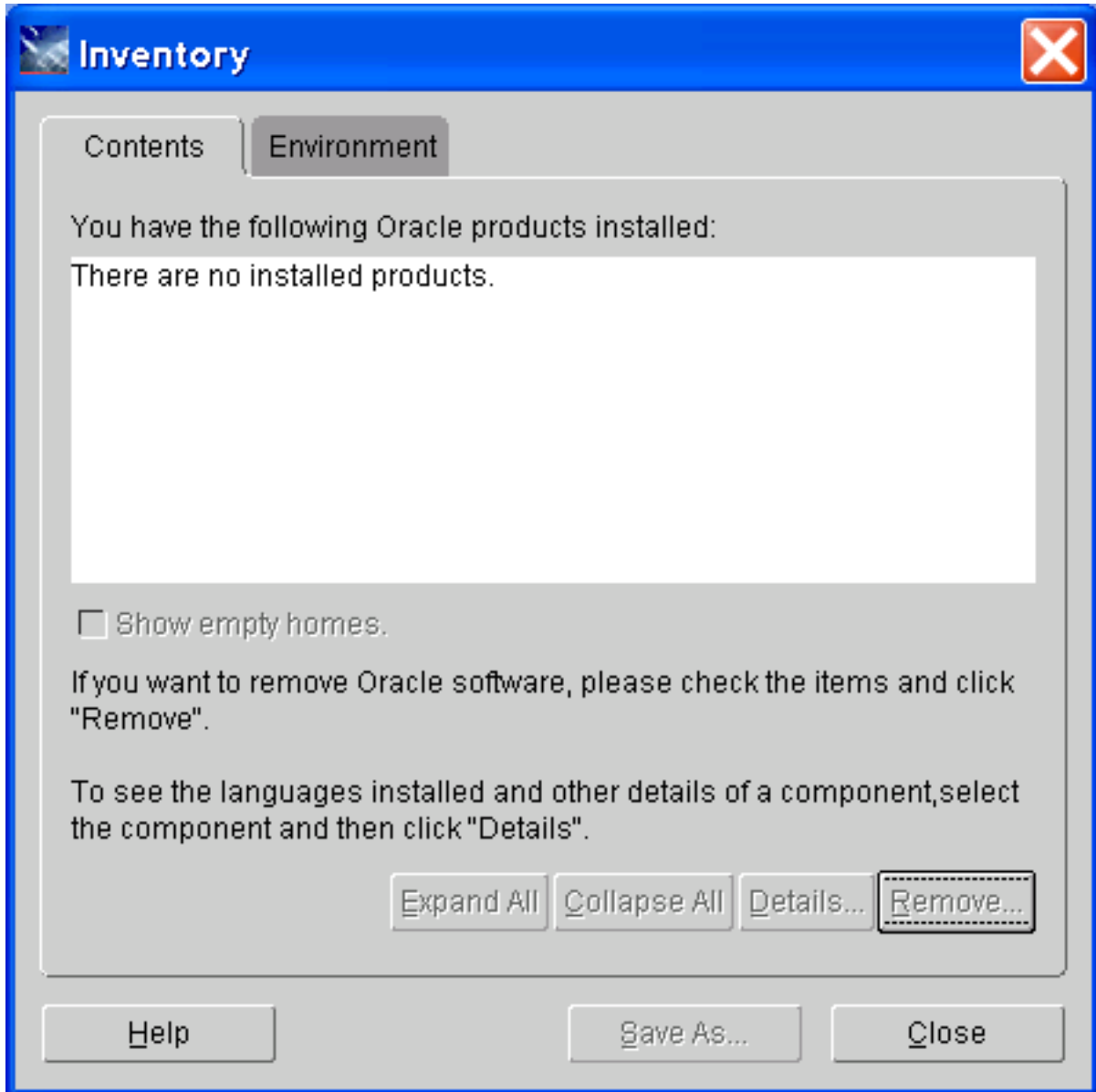
5. On Inventory, with the Contents tab selected, if the selected Oracle Home is correct, click the **Remove...** button.



6. On Confirmation, click **Yes** to begin the deinstallation of the selected Oracle Home.

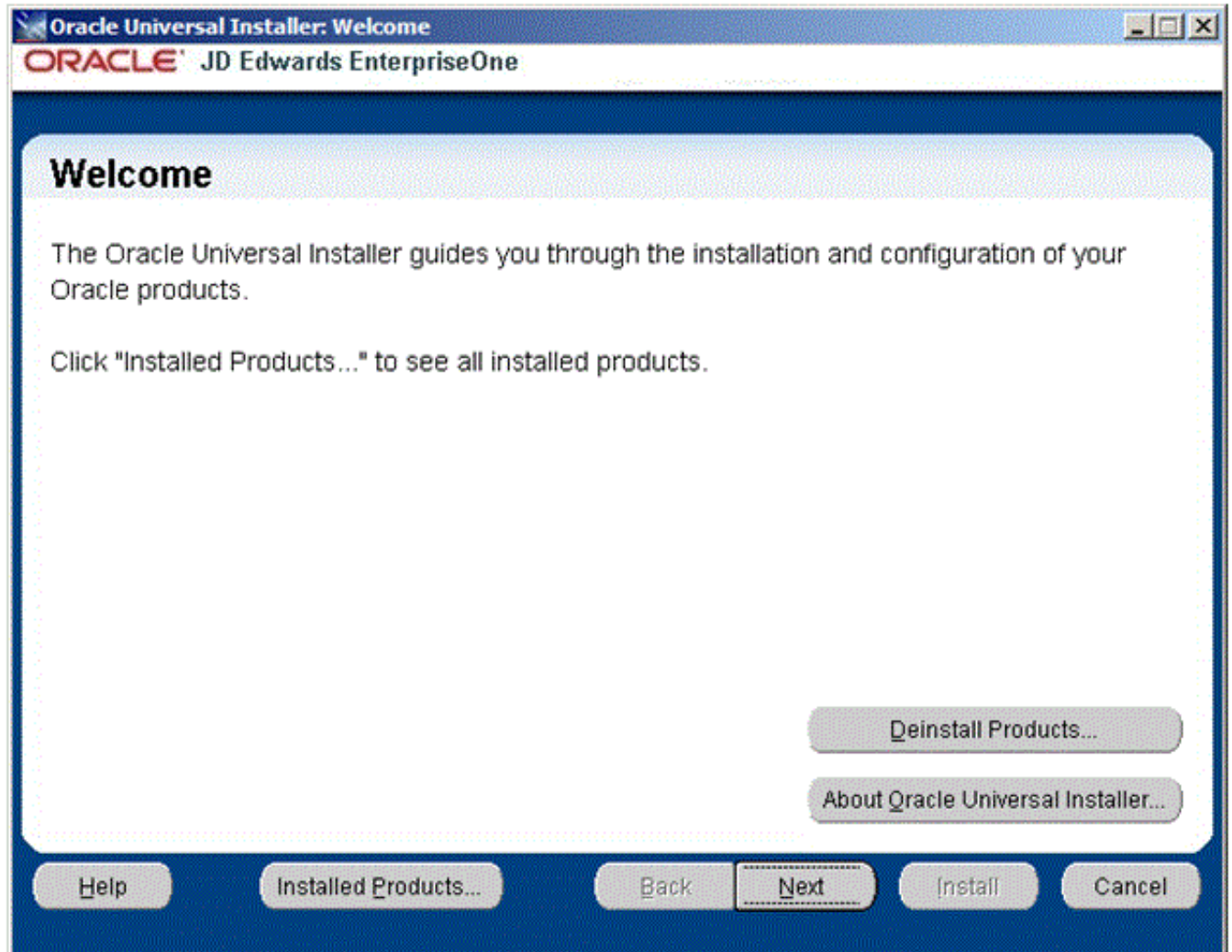
The Remove progress dialog is displayed:



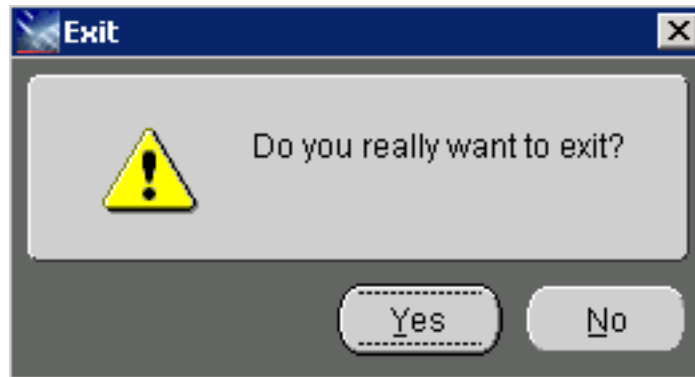


7. On Inventory, verify the selected Oracle Home is no longer displayed.

8. On Inventory, click the **Close** button.



9. On the Welcome screen, click the **Cancel** button to exit the Oracle Universal Installer.



10. On the Exit dialog, click the **Yes** button to OUI.

