JD Edwards EnterpriseOne Tools

Server Manager Guide

Release 9.1.x

E18837-18

July 2022

Describes how to administer, deploy, configure, and manage JD Edwards EnterpriseOne.

ORACLE

JD Edwards EnterpriseOne Tools Server Manager Guide, Release 9.1.x

E18837-18

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

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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 xv

Audience xv
Documentation Accessibility xv
Related Documents xv
Conventions xv

1 Concepts and Terminology

1.1 Introduction 1-1
1.2 Features at a Glance 1-1
1.3 Server Manager Architecture 1-3
1.4 Server Manager Components 1-4
1.4.1 Management Console 1-5
1.4.2 Management Agent 1-5
1.4.3 Managed Home 1-6
1.4.4 Managed Instance 1-6
1.4.5 Instance Properties 1-7
1.4.6 Software Component 1-7
1.4.6.1 JD Edwards EnterpriseOne Server Components 1-7
1.4.6.2 JDBC Driver Components 1-7
1.4.7 Server Configuration and Runtime Metrics 1-8

2 Functional Overview

2.1 Centralized Topology Information 2-1
2.2 Standardized Remote Deployment 2-1
2.3 Configuration Management 2-2
2.4 Audit History 2-2
2.5 Remote Troubleshooting 2-2
2.6 Operational Control for Managed Servers 2-3
2.7 Flexible Monitoring 2-3
2.8 Oracle Configuration Manager (OCM) 2-3

3 Working with the Server Manager Management Console

3.1 Accessing the Certifications (Minimum Technical Requirements) 3-1
3.2 Understanding the Server Manager Management Console Installation, Upgrade, and Update for Tools Release 9.1 3-2

3.3 Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2) 3-2
3.4 Understanding the Installation, Upgrade, and Update Strategy for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2) 3-3
3.5 Update Center Components for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2) 3-4
3.6 Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2) 3-4
3.7 Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2) 3-7
3.7.1 Installing the Management Console as an OC4J (Standalone Application Server) 3-7
3.7.1.1 Prerequisites for OC4J 3-8
3.7.1.2 Running the OC4J Installer for the Server Manager Console 3-8
3.7.1.3 Verifying the OC4J Installation 3-16
3.7.2 Installing the Management Console on WebLogic Server Tools (Release 9.1 Update 2) 3-17
3.7.2.1 Prerequisites for WebLogic Server 3-18
3.7.2.2 Running the WebLogic Server Installer for the Server Manager Console 3-21
3.7.2.3 Verifying the Server Manager Console Installation on WebLogic Server 3-30
3.7.2.4 Enable SSL for Server Manager Console on the WebLogic Server 3-33
3.7.2.5 Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore 3-37
3.7.2.6 Troubleshooting the Server Manager Console Installation on WebLogic Server 3-40
3.7.3 Installing the Management Console on WebSphere Application Server (Tools Release 9.1 Update 2 and Update 3) 3-44
3.7.3.1 Starting and Stopping the Server Manager Console on WebSphere on the Microsoft Windows Platform 3-45
3.7.3.2 General Hostname/IP Address Configuration Prerequisites 3-45
3.7.3.3 Creating a Profile for WebSphere Application Server Release 7.0/8.5 3-45
3.7.3.4 Prerequisites for WebSphere Application Server 3-61
3.7.3.5 Running the WebSphere Application Server Installer for the Server Manager Console 3-64
3.7.3.6 Verifying the Server Manager Console Installation on WebSphere Application Server 3-74
3.7.3.7 Enable SSL for Server Manager Console on the WebSphere Application Server 3-75
3.7.3.8 Troubleshooting the Server Manager Console Installation on WebSphere Application Server 3-78
3.7.4 Troubleshoot the Management Console Installation 3-79
3.7.4.1 Installer Fails to Complete 3-79
3.7.4.2 Management Console Will Not Start 3-80
3.7.4.3 Management Console Will Not Save Configuration Settings 3-80
3.8 Upgrade the Server Manager Management Console from a Previous Release to Tools Release 9.1 3-81
3.8.1 Upgrade Sequence 3-82
3.8.2 Running the Management Console Installer in Upgrade Mode 3-83

3.8.3 Post Upgrade Notes 3-91
3.9 Upgrade the Server Manager Management Console with Oracle WebLogic Server 12.1.2 (Release 9.1 Update 4) 3-92
3.9.1 Overview 3-92
3.9.2 Uninstalling Server Manager Console Installed on Oracle WebLogic Server 10.3.6 3-93
3.9.3 Installing Oracle WebLogic Server 12.1.2 3-94
3.9.4 Installing Server Manager Console on WebLogic Server 12.1.2 3-109
3.9.5 Restoring the Previous Server Manager Console Configurations 3-119
3.10 Manually Installing a JDK or JRE on AIX 3-120
3.11 Deinstall the Server Manager Management Console for Tools Release 9.1 3-121

4 Complete the Management Console Setup Wizard

4.1 Access the Management Console 4-1
4.2 Run the Management Console Setup Wizard 4-2

5 Install a Management Agent

5.1 Obtain the Management Agent Installer Application 5-1
5.2 Distribute and Unzip the Management Agent Installer Application 5-3
5.2.1 Microsoft Windows 5-3
5.2.2 UNIX 5-3
5.2.3 IBM i (OS400) 5-4
5.3 Run the Management Agent Installer 5-4
5.3.1 Microsoft Windows 5-4
5.3.2 UNIX 5-12
5.3.2.1 Permissions 5-12
5.3.2.2 /tmp location 5-12
5.3.2.3 Oracle User ID 5-12
5.3.2.4 Oracle Application Server 5-12
5.3.2.5 Enterprise Server 5-13
5.3.2.6 Graphic Mode 5-13
5.3.2.7 AIX and Solaris Operating Systems 5-13
5.3.2.8 Running the Management Agent Installer 5-13
5.3.3 IBM i (OS400) 5-22
5.4 Post Installation Steps for WebLogic 11g, WebLogic 12c, WebSphere 7.0, or WebSphere 8.5 Web Server Instances 5-31
5.4.1 WebLogic 11g 5-31
5.4.1.1 Microsoft Windows 5-31
5.4.1.2 UNIX 5-31
5.4.2 WebLogic 12c 5-32
5.4.2.1 Microsoft Windows 5-32
5.4.2.2 UNIX 5-32
5.4.3 WebSphere 7.0 and WebSphere 8.5 5-32
5.4.3.1 Microsoft Windows 5-32
5.4.3.2 UNIX or IBM i (OS400) 5-33
5.5 Troubleshoot the Management Agent Installation 5-33

5.5.1 Management Agent Installer Failed ... 5-33
5.5.2 Management Agent Does Not Start ... 5-34
5.5.3 Management Agent Dies on Unix or IBM i ... 5-34
5.5.4 Management Agent Cannot Manage Oracle Application Server on Unix ... 5-34
5.5.5 Management Agent Cannot Start or Stop a Unix Enterprise Server ... 5-35
5.5.6 Management Agent Cannot Manage Secure Servers on WebSphere Application Server on IBM i ... 5-36
5.6 Deinstall a Management Agent ... 5-36
5.6.1 Microsoft Windows and UNIX ... 5-36
5.6.2 IBM i OS/400 ... 5-40

6 Start, Stop, and Restart a Management Agent

6.1 Start a Management Agent ... 6-1
6.1.1 Microsoft Windows ... 6-1
6.1.1.1 Start a Management Agent as a Service ... 6-1
6.1.1.2 Start a Management Agent from a Script ... 6-2
6.1.2 UNIX ... 6-2
6.1.3 OS400 (IBM i) ... 6-2
6.2 Stop a Management Agent ... 6-4
6.2.1 Stop a Management Agent from the Management Console ... 6-4
6.2.2 Stop a Management Agent Using a Script ... 6-5
6.2.2.1 Microsoft Windows ... 6-5
6.2.2.2 UNIX ... 6-5
6.2.2.3 OS400 (IBM i) ... 6-5
6.2.3 Stop a Management Agent as a Service (Microsoft Windows only) ... 6-6
6.3 Restart a Management Agent ... 6-6
6.3.1 Microsoft Windows ... 6-6
6.3.2 UNIX ... 6-6
6.3.3 OS400 (IBM i) ... 6-6

7 Start, Stop, and Restart the Management Console

7.1 Start, Stop, and Restart the Management Console as a Service ... 7-1
7.2 Start, Stop, and Restart the Management Console from a Script ... 7-2

8 User Interface for the Management Console

8.1 User Interface Layout ... 8-1
8.1.1 Select Instance Dropdown ... 8-1
8.1.2 Quick Links - What do you want to do? ... 8-2
8.1.3 Views of the Management Console ... 8-3
8.1.3.1 Management Dashboard ... 8-3
8.1.3.2 EnterpriseOne Servers By Type ... 8-4
8.1.3.3 EnterpriseOne Servers By Group ... 8-6
8.1.3.4 Search for User Resources ... 8-8
8.2 User Interface Productivity Hints ... 8-8
8.2.1 Grid Multiple Item Selection ... 8-9
8.2.2 Grid Column Alphanumeric Sorting ... 8-9

8.2.3 State Column Settings - Managed Homes 8-9
8.2.4 State Column Settings - Managed Instances 8-10

9 Configure the Default Server Group Configuration Settings

9.1 Configuring Default Configuration Settings 9-1
9.2 Configuring Default Configuration Settings Based on Existing Instance (Release 9.1, Update 4) 9-3

10 Configure Management Console Users

11 Managed Software Components

11.1 Upload Software Components 11-1
11.2 Distribute or Delete Managed EnterpriseOne Software Components 11-3
11.2.1 Distribute Software Components to Managed Homes 11-3
11.2.2 Delete Managed Software Components from the Management Console 11-4
11.2.3 Delete Managed Software Components known to the Management Console 11-5
11.3 Start or Stop a Managed EnterpriseOne Software Component 11-7
11.4 Change a Managed EnterpriseOne Software Component 11-7
11.5 View the Software Release History for a Managed Instance 11-9

12 Manage JDBC Drivers

12.1 Obtain JDBC Drivers 12-1
12.2 Upload JDBC Drivers to the Management Console 12-2
12.3 Install JDBC Drivers to J2EE Servers 12-4
12.4 Uninstall the JDBC Driver from J2EE Servers 12-4
12.5 Install JDBC Drivers to JD Edwards EnterpriseOne Data Access Servers 12-5
12.6 Uninstall JDBC Drivers from JD Edwards EnterpriseOne Data Access Servers 12-6

13 Register an Application Server

13.1 Register an Oracle Application Server, Version 10.1.3.1 13-1
13.2 Register a WebSphere Application Server, Version 7.0 13-6
13.2.1 Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled 13-9
13.3 Register a WebSphere Application Server, Version 8.5 (Tools Release 9.1 Update 2.3) 13-10
13.3.1 Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled 13-14
13.4 Register an Oracle WebLogic Server 11g 13-14
13.5 Register an Oracle WebLogic Server 12c 13-19

14 Create a J2EE Server Container

14.1 Create a J2EE Server Container for the Oracle Application Server (OAS) 14-1
14.2 Create a J2EE Server Container for the WebSphere Application Server (WAS) 14-3
14.3 Create a J2EE Server for an Oracle WebLogic Server Domain 14-5
14.4 Install or Uninstall JDBC Drivers to the J2EE Server (WLS or WAS) 14-8

14.4.1 Install JDBC Drivers to the J2EE Server (WLS or WAS) 14-9
14.4.2 Uninstall JDBC Drivers from the J2EE Server (WLS or WAS) 14-10

15 Manage an Application Server and Related Components

15.1 Manage an Oracle Application Server (OAS) Instance 15-1
15.1.1 Start or Stop the Oracle Application Server 15-2
15.1.2 General 15-2
15.1.3 Instance Properties 15-3
15.1.4 Start, Stop, or Restart the Oracle HTTP Server 15-4
15.1.5 Grid Items for Oracle HTTP Servers 15-4
15.1.6 Start, Stop, Restart, or Delete a J2EE Server Container 15-5
15.1.7 Grid Items for J2EE Server Container 15-6
15.1.8 Available Log Files 15-6
15.2 Manage a WebSphere Application Server (WAS) Instance 15-6
15.2.1 Start, Stop, or Restart the WebSphere Application Server 15-7
15.2.2 Profiles and Servers 15-7
15.2.2.1 Start, Stop, or Restart a WebSphere Application Server 15-7
15.2.2.2 Grid Items for Profiles and Servers 15-8
15.2.3 Start, Stop, or Restart a J2EE Server 15-8
15.2.4 Available Log Files 15-10
15.3 Manage a WebLogic Server Instance 15-10
15.3.1 Start, Stop, or Restart the WebLogic Server 15-11
15.3.2 Instance Properties 15-11

16 Register or Create a JD Edwards Enterprise Server as a New Managed Instance

16.1 Visual Studio Requirements for Microsoft Windows-based Enterprise Servers 16-1
16.2 Prerequisites and Recommended Registration or Creation Sequence for an Enterprise Server as New Managed Instance 16-2
16.3 Register an Existing Enterprise Server as a New Managed Instance 16-2
16.4 Create (Install) an Enterprise Server as a New Managed Instance 16-7

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

17.1 Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances 17-1
17.2 Create a HTML Web Server as a New Managed Instance 17-2
17.2.1 Post Install for a Federated Server in Network Deployment Mode 17-9
17.3 Create a Transaction Server as a New Managed Instance 17-14
17.4 Create a Collaborative Portal Server as a New Managed Instance 17-21
17.5 Create a Business Services Server as a New Managed Instance 17-26
17.5.1 Configuring a Clustered Business Services Server Instance for Consumer Business Services (Release 9.1 Update 5) 17-34
17.6 Create an Application Interface Services (AIS) Server as a New Managed Instance (Release 9.1 Update 4.2) 17-35

18 Install a JD Edwards EnterpriseOne Data Access Driver

18.1 Prerequisites and Recommendation Installation Sequence for the Data Access Driver 18-1
18.2 Create a Data Access Driver 18-2

19 Remove a Managed Instance

19.1 Remove an Application Server Managed Instance 19-1
19.2 Remove a JD Edwards EnterpriseOne Server Instance 19-2

20 Overview of Management Console Administration

21 Administer Management Console Users and User Groups

21.1 Configure the Management Console for User Setup 21-1
21.1.1 Specify the JD Edwards EnterpriseOne Server Used for User Authentication 21-2
21.1.2 Change the jde_admin User Password 21-2
21.2 Manage Management Console Users 21-3
21.2.1 Add a User 21-3
21.2.2 Remove a User 21-3
21.3 Manage User Groups 21-3
21.3.1 Create a User Group 21-4
21.3.2 Delete a User Group 21-5
21.3.3 Assign Users to a User Group 21-5
21.3.4 Remove Users from a User Group 21-5
21.4 Assign Server Manager Permissions 21-6
21.4.1 Understand Server Manager Permissions 21-6
21.4.2 Assign Global Permissions 21-6
21.4.3 Assign Server Group Permissions 21-8
21.5 Run the User Access Report 21-9

22 Monitor JD Edwards EnterpriseOne Servers

22.1 E-Mail Configuration 22-1
22.2 Monitors 22-3
22.2.1 Create a Monitor 22-3
22.2.2 Monitor Configuration 22-4
22.2.2.1 General Properties 22-4
22.2.2.2 Managed Instances 22-4
22.2.2.3 Monitored Events 22-5
22.2.2.4 Notification Hours 22-8
22.2.2.5 E-Mail Subscriptions 22-9
22.2.3 Available Monitors 22-9
22.2.3.1 Start a Monitor 22-10
22.2.3.2 Stop a Monitor 22-10
22.2.3.3 Delete a Monitor 22-10
22.2.3.4 Modify the Monitor Configuration 22-10
22.2.3.5 View a Monitor Report 22-10
22.2.3.6 Create a Duplicate Monitor 22-10

22.2.4 Monitor History 22-11
22.2.4.1 Delete Monitor History 22-11
22.2.4.2 View the Monitor Start Time 22-11
22.2.4.3 View Report 22-11

23 Available Log Files

23.1 Managed Home Log Files 23-1
23.1.1 Managed Home Details 23-2
23.1.2 Agent Log Level 23-2
23.2 Managed Instance Log Files 23-3
23.2.1 View Available Log Files 23-3
23.2.2 Write Log Message [Web Products Only] 23-4
23.2.3 Delete Log Files 23-5
23.2.4 Log File Viewer 23-5
23.2.4.1 Filter Log Files 23-6
23.2.4.2 Criteria 23-6
23.2.4.3 Apply Filter 23-7
23.2.4.4 Save As Favorite 23-8
23.2.4.5 Download 23-8
23.2.4.6 Results 23-9
23.3 jde.properties Logging 23-10
23.3.1 Remove Log Definitions 23-11
23.3.2 Apply Changes 23-11
23.3.3 New Log Configuration 23-12
23.3.4 User Specific Log File Configuration 23-12
23.3.5 Create New User Specific Log File Configuration 23-12

24 Install an Oracle Configuration Manager (OCM) Instance

24.1 Overview 24-1
24.2 Prerequisites 24-2
24.3 Oracle Configuration Manager Manual Install 24-2
24.4 Oracle Configuration Manager Install Using Server Manager 24-6

25 Administer Oracle Configuration Manager (OCM)

25.1 Overview of Oracle Configuration Manager 25-1
25.1.1 How Oracle Configuration Manager Works 25-2
25.1.1.1 Customer-Side Components 25-2
25.1.1.2 Oracle-Side Components 25-3
25.2 Secure Communication Through Oracle Configuration Manager 25-3
25.2.1 Direct Access to the Internet 25-3
25.2.2 Access Through a Proxy Server to the Internet 25-3
25.2.3 Automatic Updates 25-4
25.3 Data Collected by Oracle Configuration Manager 25-4
25.4 Prerequisite 25-5
25.5 Check the Status of Oracle Configuration Manager 25-6
25.6 Test the Connection to Oracle 25-6

25.7 Modify the Collection Interval Settings ... 25-7
25.8 Run a Manual Collection ... 25-7
25.9 Hold or Resume Oracle Configuration Manager on a Managed Home ... 25-7
25.10 View Configuration Data and Log Files ... 25-8
25.10.1 View Raw Configuration Data and Log Files on the Managed Home ... 25-8
25.11 Manually Download Updates to Oracle Configuration Manager ... 25-8
25.12 Examples of Data Collected by Oracle Configuration Manager ... 25-9
25.12.1 Sched.log ... 25-9
25.12.2 Collector.log ... 25-9
25.12.3 Collection .xml File ... 25-9
25.12.4 Targetmap.xml ... 25-10
25.12.5 Upgrade.log ... 25-11

26 Update Server Manager

26.1 Update the Management Console ... 26-1
26.2 Update a Management Agent ... 26-3
26.3 Troubleshooting an Unsuccessful Management Console Update ... 26-5

27 Create a JD Edwards EnterpriseOne Data Access Server as a New Managed Instance

27.1 Prerequisites and Recommended Installation Sequence for Managed Instances for Data Access Server Instance ... 27-1
27.2 Create a Data Access Server as a New Managed Instance ... 27-2

28 Configure an Oracle Application Server

29 View Runtime Metrics for a Managed Instance

29.1 Enterprise Server Runtime Metrics ... 29-1
29.1.1 General ... 29-2
29.1.2 Process Detail ... 29-2
29.1.2.1 A Process Summary ... 29-3
29.1.2.2 A Batch Summary ... 29-3
29.1.2.3 A Process Table ... 29-3
29.1.3 Environment Variables ... 29-9
29.1.4 Disk Space Usage ... 29-9
29.1.5 Kernel Ranges ... 29-10
29.1.5.1 Network Listener Jobs (JDENET_N) ... 29-10
29.1.5.2 Kernel Process Jobs (JDENET_K) ... 29-11
29.1.6 Audit History ... 29-11
29.1.6.1 Report Configuration ... 29-12
29.1.6.2 Deployment History ... 29-12
29.1.6.3 Changed Metrics ... 29-13
29.2 EnterpriseOne Web-based Servers Runtime Metrics ... 29-13
29.2.1 User Sessions (HTML Server Only) ... 29-14
29.2.1.1 Terminate ... 29-15
29.2.1.2 Send Message ... 29-15

29.2.2 CallObject Stats 29-15
29.2.2.1 CallObject Table 29-16
29.2.3 JDBj Database Caches 29-17
29.2.3.1 JDBj Service Caches 29-18
29.2.3.2 Clear Cache 29-19
29.2.4 Database Connections 29-19
29.2.4.1 JDBj Pooled Database Connections 29-19
29.2.4.2 Prepared Statement Cache Detail 29-20
29.2.5 JDBj Runtime 29-20
29.2.5.1 Properties 29-20
29.2.5.2 Apply 29-21
29.2.6 JDENET Stats 29-21
29.2.6.1 JDENET Connections 29-22
29.2.6.2 JDENET Connection Pools 29-22
29.2.6.3 JDENET Socket Connections 29-23
29.2.7 Java Environment 29-24
29.2.7.1 Java Environment Runtime Detail 29-24
29.2.7.2 Java Memory Usage 29-25
29.2.7.3 Run Garbage Collection 29-25
29.2.7.4 Java Thread Information 29-25
29.2.7.5 Java System Properties 29-26
29.3 Application Interface Services Server Runtime Metrics (Release 9.1 Update 5) 29-26
29.3.1 AIS Information 29-26
29.3.2 Login Metrics 29-27
29.3.3 User Info Metrics 29-27
29.3.4 Runtime Configuration 29-27
29.3.5 Form Metrics 29-27
29.3.6 Session Metrics 29-27
29.3.7 Java Environment 29-27
29.4 Transaction Server Administration 29-27
29.4.1 Failed Events 29-27
29.4.1.1 Select [Failed Events] 29-27
29.4.1.2 Delete Failed Events 29-28
29.4.1.3 Delete All Failed Event 29-28
29.4.2 Subscribers 29-28
29.4.2.1 Select [Subscriber] 29-28
29.4.2.2 Purge Subscriber Queued Messages 29-29
29.4.3 Event Metrics 29-29

30 Configure EnterpriseOne Server Instances

30.1 Configuration Overview (Release 9.1, Update 4) 30-1
30.1.1 Save or Restore 30-3
30.1.2 Configuration Summary 30-3
30.2 General and Instance Properties 30-3
30.3 Instance Properties 30-4
30.4 Available Log Files 30-4
30.5 Configuration Groups 30-5

30.5.1 EnterpriseOne Enterprise Server 30-5
30.5.2 EnterpriseOne HTML Server 30-5
30.5.3 EnterpriseOne Business Services Server 30-6
30.5.4 EnterpriseOne Application Interface Services Server (Release 9.1 Update 5) 30-6
30.5.5 EnterpriseOne Transaction Server 30-6
30.5.6 EnterpriseOne Data Access Server 30-6
30.5.7 EnterpriseOne Data Access Driver 30-7
30.6 Configuration Items 30-7
30.6.1 Help 30-7
30.6.2 History 30-8
30.7 Compare Instances 30-8
30.7.1 Create Comparison 30-9
30.7.2 Comparison Results 30-9
30.7.2.1 Results 30-10
30.7.2.2 Modifications 30-10
30.8 Troubleshooting the Configuration of EnterpriseOne Server Instances 30-10
30.8.1 Permission Denied 30-11

31 Administer Server Groups

31.1 Overview of Server Groups 31-1
31.1.1 Server Group Security 31-2
31.2 Manage Server Groups 31-2
31.2.1 Create Server Group 31-2
31.2.2 Modify Server Group 31-3
31.2.2.1 Add Server Group Members 31-3
31.2.2.2 Delete Server Group 31-3

32 Clear Table Cache (Tools Release 9.1 Update 2)

32.1 Understanding Clear Table Cache 32-1
32.2 Using the Clear Table Cache Feature 32-1
32.2.1 Clear Table Cache by Environment 32-2
32.2.2 Clear All Tables Caches in All Environments 32-4

A Best Practices

A.1 Multiple Management Consoles A-1
A.2 Management Agents A-2
A.2.1 One Agent Per Application Server Installation A-2
A.2.2 Management Agents on OAS A-2
A.2.3 Management Agents on JD Edwards EnterpriseOne Enterprise Servers A-3
A.3 Multiple Agents on a Single Machine A-3
A.4 Multiple WebSphere Application Servers A-3
A.5 Separate WAS Profiles A-3
A.6 Verify HTTP Ports A-4
A.7 HTTP Ports on UNIX Operating Systems A-4
A.8 Setting Up Windows Firewall in Windows Server 2008 ..... A-4

B Using SSL with Standalone OC4J

B.1 Configuring HTTPS/SSL on the Server Manager Console on OC4J B-1
B.1.1 Create a Keystore B-1
B.1.2 Export a Certificate File B-2
B.1.3 Update the OC4J Configuration B-2
B.1.4 Import the New Certificate B-3
B.2 Configure Server Manager Agents to work successfully with HTTPS/SSL Server Manager Console B-4
B.2.1 Importing the custom Certificate into the cacerts file of the SM Agent Machine(s) JRE B-4
B.2.1.1 For Windows Platform: B-5
B.2.1.2 For UNIX Platforms (including Linux): B-5
B.2.1.3 For AS/400 Platforms as QSECOFR (or equivalent user profile): B-5
B.2.2 Exceptions B-5

Preface

Welcome to the *JD Edwards EnterpriseOne Tools Server Manager Guide*.

> **Note:** This guide has been updated for JD Edwards EnterpriseOne Tools 9.1 Update 2, Update 3, and Update 5 releases. For details on documentation updates, refer to the *JD Edwards EnterpriseOne Net Change for Installation and Upgrade Documentation Library*.

Audience

This guide is intended for system administrators and technical consultants who are responsible for deploying, configuring, and managing JD Edwards EnterpriseOne.

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 Documents

You can access related documents from the Oracle Technology Network (OTN) by using this link:

http://www.oracle.com/technetwork/documentation/jdedent-098169.html

Conventions

The following text conventions are used in this document:

Convention	Meaning
Bold	Indicates field values.
Italics	Indicates emphasis and JD Edwards EnterpriseOne or other book-length publication titles.

Convention	Meaning
`Monospace`	Indicates a JD Edwards EnterpriseOne program, other code example, or URL.
>**Tutorial**	Indicates a link to a recording of the described feature. These recordings are in MP4 format so ensure that you have an appropriate player installed. Access to these recordings requires a valid Oracle account.

1

Concepts and Terminology

This chapter discusses:

- Section 1.1, "Introduction"
- Section 1.2, "Features at a Glance"
- Section 1.3, "Server Manager Architecture"
- Section 1.4, "Server Manager Components"

1.1 Introduction

Server Manager for JD Edwards EnterpriseOne is a web based application used to manage the complete life cycle of the JD Edwards EnterpriseOne server products. It is delivered with the JD Edwards EnterpriseOne Tools Release 8.97 and later releases and supports the same JD Edwards EnterpriseOne associated application releases that are supported by the tools releases.

1.2 Features at a Glance

Server Manager provides:

- Web Based System Management

  You can securely access and manage your JD Edwards EnterpriseOne installation from anywhere using a standard web browser.

- Remote Deployment and Upgrades

  You can install, uninstall, and update your JD Edwards EnterpriseOne servers regardless of their physical location or platform.

- Remote Operational Control

  You can start and stop any of your JD Edwards EnterpriseOne servers, Oracle J2EE application servers, or supported third party J2EE application servers directly from the Management Console.

- Secure Administrative Tasks

  Server Manager permits you to specify which existing JD Edwards EnterpriseOne users have access to the Management Console control which JD Edwards EnterpriseOne servers the user may view, and specify which administrative tasks the user may perform on those servers.

- Configuration Management

Server Manager provides a web-based interface for managing the configuration of all managed servers. The application presents each configuration item along with integrated help describing the configuration setting.

Note: Beginning with the availability of Server Manager, it is strongly advised that all changes to configuration files (such as jde.ini, jas.ini, jdbj.ini, jdelog.properties, etc.) for any JD Edwards EnterpriseOne server managed by Server Manager be accomplished using only the Management Console interface of Server Manager. In addition to providing usability improvements, using Server Manager reduces the risk of introducing configuration errors by providing dropdowns that contain only valid values where applicable. Further, the tool provides a useful Audit History for any modifications made to configurations using Server Manager.

- Configuration Comparison

  Use Server Manager to compare the configuration of two or more servers to identify configuration differences. You can compare configurations through the Management Console application regardless of the platform or location of the actual JD Edwards EnterpriseOne server. You can also compare individual servers with the default configuration of the corresponding server groups to which the servers belong.

- Audit History

  Server Manager maintains a history of changes made to the managed servers. This includes a history of each configuration change, each server start and stop, and each tools release update, including the user that performed the change or operation. The Management Console application provides mechanisms to query and view the audit history that is maintained.

- Integrated EnterpriseOne Software Management

  Use Server Manager to centrally maintain all your JD Edwards EnterpriseOne server tools releases, including the ability to copy the software to the remote server machines.

- Logical Server Grouping

  Server Manager allows you to group servers with a similar purpose. These groups can include any of the server types such as Enterprise Server, HTML Web Server, and so on. A default, or template, configuration is maintained for each server group.

- Application Release Independence

  Server Manager is delivered with JD Edwards EnterpriseOne Tools Release 8.97 (and later) and is compatible with any supported JD Edwards EnterpriseOne application release beginning with Application Release 8.9 through the currently supported release. No electronic software updates (ESUs) are required to support Server Manager.

- Self-Contained Installation

  The installation of Server Manager delivers all components that are required by the Management Console application. There are no third party requirements regardless of your existing or intended middleware topology (for example, Oracle Application Server, WebSphere Application Server, or no application server).

- Tools Release Independence

  Newer versions of the Server Manager application will continue to support the management of earlier tools releases back to JD Edwards EnterpriseOne its initial release in Tools Release 8.97.

1.3 Server Manager Architecture

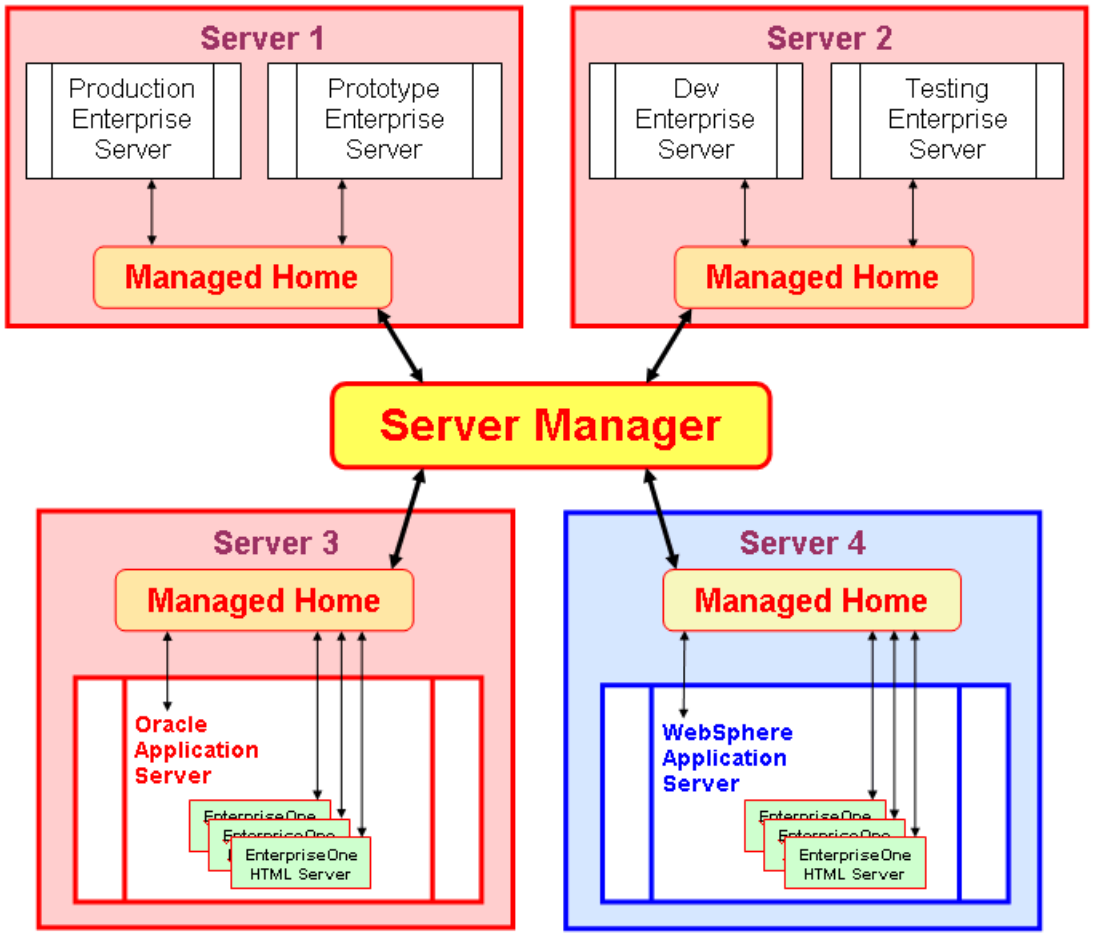
The key benefits of the Server Manager architecture include:

- An integrated, web-based Management Console application.
- Management Agents that are installed on the JD Edwards EnterpriseOne servers.
- Use of Java Management Extensions (JMX) technology by the Management Agents running on the servers to run as background processes that interact with the Management Console web application.
- Secure and encrypted network communication between the Management Console and Management Agents.

The design goal of Server Manager is to reduce the total cost of ownership of JD Edwards EnterpriseOne server products from installation and configuration, to ongoing maintenance and troubleshooting. Server Manager manages these JD Edwards EnterpriseOne servers:

- Enterprise Servers
- HTML Web Servers
- Transaction Servers
- Collaborative Portal Servers
- Business Services Servers
- Oracle Configuration Manager (OCM)

A high level view of the architecture is illustrated by this diagram:



1.4 Server Manager Components

This section discusses:

- Section 1.4.1, "Management Console"
- Section 1.4.2, "Management Agent"
- Section 1.4.3, "Managed Home"
- Section 1.4.4, "Managed Instance"
- Section 1.4.5, "Instance Properties"
- Section 1.4.6, "Software Component"
- Section 1.4.7, "Server Configuration and Runtime Metrics"

1.4.1 Management Console

The central element of the Server Manager architecture is the Management Console, a web-based application. The Management Console is responsible for:

- Hosting the HTML-based interface accessed using a standard web browser.
- Communicating with Management Agents installed on remote machines.
- Monitoring the runtime operation of the JD Edwards EnterpriseOne servers.

Server Manager is required for all JD Edwards EnterpriseOne installations that use Tools Release 8.97 (and later) tools releases. The Management Console is a J2EE application with a web-based user interface that is accessed by the end user through a browser. For the management user, this interface is the only means of directly accessing any servers managed by Server Manager.

Releases Prior to 9.1 Update 2

The Management Console must be installed on a Microsoft Windows-based machine.

For Release 9.1 Update 2 and above

The Management Console can be installed on either a Windows-based or Linux-based machine. Refer to the section of this guide entitled: Section 3.3, "Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)".

Typically the most suitable machine within the JD Edwards EnterpriseOne architecture is the Deployment Server, although the Management Console can be installed on any server that meets the JD Edwards EnterpriseOne Certifications (MTRs) of the Deployment Server (for details refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide). The Management Console uses an integrated J2EE application container to host the application.

The installation of the Management Console does not require application server products such as WebLogic Server (WLS) or WebSphere Application Server (WAS). The Management Console is installed as a Microsoft Windows service. Updates to the Management Console are performed using the Management Console web application itself.

Optionally, the Management Console can be configured to use the secure protocols of HTTPS/SSL.

See Also

- For an illustration of the role of the Management Console within Server Manager, refer to Section 1.3, "Server Manager Architecture".

1.4.2 Management Agent

Server Manager uses Management Agents that are installed on the physical machines that run JD Edwards EnterpriseOne server products. These Management Agents communicate directly with the Management Console and are instructed to perform operations as a result of user actions in the Management Console web application.

The Management Agent is based on the JMX Java management specifications. Management Agents interact only with the Management Console web application; however, much of the work, such as starting and stopping servers, is actually performed by the Management Agent.

The JD Edwards EnterpriseOne server products contain an embedded variant of the Management Agent. This Management Agent is responsible for providing the runtime information about an active server instance to the Management Console web application.

The Managed Home Agent is a standalone Management Agent which functions as an installed daemon process.

The responsibilities of the Management Agent within Server Manager include:

- Creating, registering, uninstalling, and updating the EnterpriseOne servers.
- Starting and stopping any managed EnterpriseOne server.
- Managing the configuration files used by the EnterpriseOne server.
- Providing access to the log files generated by the EnterpriseOne server.

- Providing basic management of the third-party application servers on which the web-based EnterpriseOne server products run.
- Transferring and managing a local copy of EnterpriseOne server software components (that is, the Tools Releases).

The Server Manager Management Console web application determines whether the Management Agent should be updated. If so, the Management Agents are updated using the Management Console.

1.4.3 Managed Home

The location in which the managed home agent is installed is a Managed Home. Similar to the concept of an ORACLE_HOME, the Managed Home is the deployment location of the standalone Management Agent and a structured file system containing the constituent parts of managed JD Edwards EnterpriseOne servers.

The Managed Home is created by the installation of the standalone Management Agent. The structured nature of the Managed Home simplifies the installation and maintenance of JD Edwards EnterpriseOne software and enables integration with Oracle Configuration Manager (OCM).

You must install at least one Managed Home on each physical machine before installing or managing any JD Edwards EnterpriseOne servers. It is possible for a machine to host more than one Managed Home that might not use the same Management Console. Each unique Managed Home is associated with exactly one Management Console.

See Also

- For an illustration of the role of the Managed Home within Server Manager, refer to Section 1.3, "Server Manager Architecture".

1.4.4 Managed Instance

Each EnterpriseOne server, Oracle Application Server, or WebSphere Application Server is referred to as a Managed Instance. A Managed Instance is a particular instantiation of a software component on a physical machine. Each Managed Instance is identified by an instance name that name is unique to the machine on which the Managed Instance resides. The instance name is supplied by the user who either created or registered the server with the Management Console.

Each Managed Instance is associated with a Managed Home on the same physical machine.

1.4.5 Instance Properties

Instance Properties are the unique characteristics needed to identify an individual managed instance. For example, only a a single instance property might have been defined for an Enterprise Server:

- Installation path

As another example, an HTML Web Server software component might define two instance properties:

1. Instance name of the application server under which it runs.
2. J2EE container within the application server target instance.

1.4.6 Software Component

The JD Edwards EnterpriseOne Tools Releases are downloaded as a portable archive (.PAR) and are referred to as Software Components in Server Manager. The JDBC driver implementations (JAR files) are also Software Components in Server Manager.

This section describes:

- Section 1.4.6.1, "JD Edwards EnterpriseOne Server Components"
- Section 1.4.6.2, "JDBC Driver Components"

See Also

- For an illustration of the role of the Software Component within Server Manager, refer to Section 1.3, "Server Manager Architecture".

1.4.6.1 JD Edwards EnterpriseOne Server Components

These Server Components are a subset of the Software Components that can be deployed and managed by Server Manager:

- JD Edwards EnterpriseOne Enterprise Server
- JD Edwards EnterpriseOne HTML Web Server
- JD Edwards EnterpriseOne Transaction Server
- JD Edwards EnterpriseOne Collaborative Portal Server
- JD Edwards EnterpriseOne Business Services Server
- JD Edwards EnterpriseOne Data Access Server

1.4.6.2 JDBC Driver Components

Server Manager can also distribute and deploy JDBC Drivers to:

- J2EE containers that run the JD Edwards EnterpriseOne web-based server products

  These drivers are required components on the JD Edwards EnterpriseOne HTML Web Server and any other JD Edwards EnterpriseOne server component that requires JDBC database connectivity that is not natively provided by the underlying application server.

- RMI java application that runs on the JD Edwards EnterpriseOne Data Access Server

  The JDBC driver for this server is required to provide native database connectivity for the application (such as Oracle BI Publisher) or program that is accessing the Data Access Server.

1.4.7 Server Configuration and Runtime Metrics

Server Configuration and Runtime Metrics are a grouping of related managed resources. A Software Component defines the configuration and metrics that an instance contains. For example, a section from the`jas.ini` file can be defined as a configuration metric for the Software Component for the JD Edwards EnterpriseOne HTML Web Server.

Runtime metrics provided insight into the current state of a running Managed Instance. For example, the active user sessions are a runtime metric provided by the JD Edwards EnterpriseOne HTML Web Server.

For details, refer to these chapters and sections within this guide:

- Configuration

For details refer to the chapter in this guide entitled: Chapter 30, "Configure EnterpriseOne Server Instances".

- Runtime Metrics

  For details refer to the chapter in this guide entitled: Chapter 29, "View Runtime Metrics for a Managed Instance".

2

Functional Overview

This section discusses:

- Section 2.1, "Centralized Topology Information"
- Section 2.2, "Standardized Remote Deployment"
- Section 2.3, "Configuration Management"
- Section 2.4, "Audit History"
- Section 2.5, "Remote Troubleshooting"
- Section 2.6, "Operational Control for Managed Servers"
- Section 2.7, "Flexible Monitoring"
- Section 2.8, "Oracle Configuration Manager (OCM)"

2.1 Centralized Topology Information

Before the introduction of Server Manager, the only mechanism to obtain an enterprise-wide view of the JD Edwards EnterpriseOne topology was through the machine key applications (application tables F9650 and F9651) and Support Assistant, which uses the same tables to obtain topology information. Functionally, these mechanisms did not provide insight into the actual topology because their accuracy was not enforced, especially regarding web-based products. In addition some products, such as Transaction Server Components (such as RTE and Performance Monitor), were not tracked at all.

Server Manager provides an accurate depiction of the true topology through the managed deployment of all server software. The integration of the Oracle Configuration Manager leverages this accuracy (see Section 2.8, "Oracle Configuration Manager (OCM)").

2.2 Standardized Remote Deployment

Using Server Manager through the web-based Management Console, the JD Edwards EnterpriseOne administrator can create a new JD Edwards EnterpriseOne server on a remote machine. The JD Edwards EnterpriseOne software used for installation is stored on the Management Console machine after being downloaded from the Customer Connection website or using Change Assistant.

The software may be distributed, or copied, to the remote machine from the Management Console. This server software (JD Edwards EnterpriseOne Tools Release) can now be used to create new JD Edwards EnterpriseOne server. The Management Home Agent performs the installation of the specific server type and automatically performs the requisite default configuration. After it is successfully installed, the server can be maintained entirely through

the Management Console. This deployment process is similar for all JD Edwards EnterpriseOne server types.

2.3 Configuration Management

Server Manager provides a complete configuration management system for all server types. Each configuration entry from the `.INI` and `.properties` files has been defined in metadata contained within the Management Console. It is no longer necessary to directly edit any of these configuration files, or even to know where they exist.

The configuration items are grouped into logical configuration topics. These topics are presented on the management page for each JD Edwards EnterpriseOne Managed Instance. Selecting a configuration topic displays all the individual configuration items contained within. These items are further grouped and displayed for viewing or editing. Each configuration item is displayed with a plain text description. Configuration items with a list of allowed values are displayed using drop down boxes.

A link to display context sensitive help is displayed next to each configuration item. Clicking this link displays the name of `.INI` file that is being viewed, the section and entry name in the file to which the `.INI` pertains, the default value of the setting, and a full description of the configuration item. For items with an associated list of allowed values each value is displayed in the help text.

The contents of the contextual help for each setting are also available in reference form in the Management Console documentation.

Through the Server Manager Management Console, a JD Edwards EnterpriseOne administrator can compare configurations for each remote Managed Instance, even if they reside on separate physical machines. This capability significantly reduces the effort required to ensure consistency among configurations, especially for those installations containing numerous JD Edwards EnterpriseOne servers.

2.4 Audit History

Before the introduction of Server Manager, many of steps in the software life cycle were not logged by any JD Edwards EnterpriseOne mechanism. With Server Manager, the Management Console records and makes available an audit trail of actions, such as:

- Installing or changing tools releases on a JD Edwards EnterpriseOne Enterprise Server.
- Installing or changing runtime code on a JD Edwards EnterpriseOne HTML Web Server.
- Changing to configuration items of Server Metrics.
- Recording implemented notifications (for example, for a critical failure).

2.5 Remote Troubleshooting

An administrator can use the Management Console to troubleshoot any of the Managed Instances within the management domain. Troubleshooting includes:

- Retrieving and modifying configuration entries of managed servers.
- Retrieving log files.
- Comparing configurations of a particular instance with any other

Before Server Manager, some of this functionality was available through the Server Administration Workbench (SAW) web interface. However, Server Manager greatly enhances the capability of the administrator by extending this ability to managing all JD Edwards

EnterpriseOne server-based products (for a list of supported servers, refer to Section 1.4.6.1, "JD Edwards EnterpriseOne Server Components"). Additionally, unlike the previous SAW implementation, which was directly embedded in the product, the Server Manager configuration management and troubleshooting tools are available even if the target instance is not running or fails to start.

2.6 Operational Control for Managed Servers

Using Server Manager, the JD Edwards EnterpriseOne administrator can remotely start any Managed Instance through the browser-based Management Console. This functionality reduces the effort required perform configuration or performance tuning changes by removing the necessity to have physical access to the machine.

2.7 Flexible Monitoring

Due to its inherent knowledge of the registered topology, Server Manager can accurately determine and subsequently monitor all entities constituting an EnterpriseOne installation. As such, Server Manager provides enterprise-wide views rather than machine specific views, which eliminates the potential for inaccurate monitoring of general information. For example, Server Manager contains real-time data for user sessions, Java memory usage, JDBj connection cache, and prepared statement configurations. Without Server Manager, such information is not available.

See Also

- Section 2.1, "Centralized Topology Information"
- Chapter 29, "View Runtime Metrics for a Managed Instance"

2.8 Oracle Configuration Manager (OCM)

Oracle created Oracle Configuration Manager (OCM) for capturing and uploading customer configuration and diagnostic data. This data is primarily obtained for Oracle installed products and is stored in a central repository at Oracle. Relative to Server Manager, the Oracle Configuration Manager refers to the incorporation of an interface with JD Edwards EnterpriseOne so that similar information can be captured and uploaded. As such, functionally Oracle Configuration Manager is another type of Managed Resource.

Oracle Configuration Manager can be installed only by Oracle customers who have an Oracle Customer ID and an ID for My Oracle Support.

Note: The OCM product does not run natively on IBM i machines. The majority of JD Edwards EnterpriseOne configuration data for IBM i machines can be obtained from the JD Edwards EnterpriseOne Microsoft Windows-based Deployment Server. In order for OCM to collect configuration and diagnostic data, you must have a Management Console or a Management Agent installed on your Deployment Server.

As an exception, specific Server Metrics information for JD Edwards EnterpriseOne on IBM i servers is not available through Oracle Configuration Manager. Such non-available information includes configuration information extracted from .INI files, Service Pack information, and web product information.

3

Working with the Server Manager Management Console

This chapter contains these sections:

- Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)"
- Section 3.2, "Understanding the Server Manager Management Console Installation, Upgrade, and Update for Tools Release 9.1"
- Section 3.3, "Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)"
- Section 3.4, "Understanding the Installation, Upgrade, and Update Strategy for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)"
- Section 3.5, "Update Center Components for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)"
- Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)"
- Section 3.7, "Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)"
- Section 3.8, "Upgrade the Server Manager Management Console from a Previous Release to Tools Release 9.1"
- Section 3.9, "Upgrade the Server Manager Management Console with Oracle WebLogic Server 12.1.2 (Release 9.1 Update 4)"
- Section 3.10, "Manually Installing a JDK or JRE on AIX"
- Section 3.11, "Deinstall the Server Manager Management Console for Tools Release 9.1"

3.1 Accessing the Certifications (Minimum Technical Requirements)

Customers must conform to the supported platforms for the release as detailed in the JD Edwards EnterpriseOne Certifications (MTRs). In addition, JD Edwards EnterpriseOne may integrate, interface, or work in conjunction with other Oracle products. Refer to the following link for cross-reference material in the Program Documentation for Program prerequisites and version cross-reference documents to assure compatibility of various Oracle products.

`http://www.oracle.com/corporate/contracts/index.html`

Access the current JD Edwards EnterpriseOne Certifications (MTRs) from My Oracle Support (`https://support.oracle.com`) by searching the “JD Edwards Server Manager” product.

See document 745831.1 (JD Edwards EnterpriseOne Minimum Technical Requirements Reference) on My Oracle Support.

3.2 Understanding the Server Manager Management Console Installation, Upgrade, and Update for Tools Release 9.1

For Tools Release 9.1, you can run the Server Manager Management Console installer in installation or upgrade mode. The installer automatically runs in Installation mode for new installations. In Upgrade mode, the installer automatically detects an existing installation that can be upgraded and gives you the option to upgrade that installation from the previous release to the latest version that is compatible with Tools Release 9.1.

Caution: Beginning with Tools Release 9.1, the Upgrade mode is new functionality that is different than the existing Update function. You must follow the proper sequence to first Upgrade and then Update your Server Manager Agents running on target machines as described in the section of this guide entitled: Upgrade the Server Manager Management Console from a Previous Release to Tools Release 9.1.

- 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 (Release 9.1 Update 2)

- Upgrade

  Use this mode to upgrade an existing installation of the Management Console onto a machine on which Server Manager Console has previously been installed by a release of JD Edwards EnterpriseOne prior to Tools Release 9.1. The Upgrade mode is described in the section of this guide entitled: Upgrade the Server Manager Management Console from a Previous Release to Tools Release 9.1.

- Update

  Use the Server Manager Update to update an existing installation of the Management Console to the latest dot release of JD Edwards EnterpriseOne Tools. For example, from 9.1.0.0 to 9.1.0.1. The Update mode is described in the section of this guide entitled: Update Server Manager.

3.3 Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)

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 Release 9.1 Update 2. Refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide for details on determining the supported release levels for each product and platform.

Application Server and JDK	Platform	Notes
Oracle WebLogic Server with JRockit or Oracle JDK	1. Windows Server 2008 and Windows Server 2008 R2 64-bit only 2. Oracle Linux & Red Hat Linux x86 64-bit only 3. Oracle Solaris SPARC x86 not supported 64-bit only	Require the pre-installation of WebLogic Server. Unique installers are available per supported platform.
IBM WebSphere Application Server IBM JDK	Windows Server 2008 and Windows Server 2008 R2 64-bit only	Requires the pre-installation of the Websphere Application Server. The IBM iSeries platform is not supported.
Oracle Container for Java (OC4J) with JDK	Windows Server 2008 and Windows Server 2008 R2 64-bit only	Does not require the pre-installation of an application server. This is a self-contained “light” version of the Oracle Application Server that is pre-packaged with the installer. Previous to 9.1 Update 2, this was the only supported Application Server for Server Manager.

3.4 Understanding the Installation, Upgrade, and Update Strategy for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)

This section describes the installation, upgrade, and update strategy for JD Edwards EnterpriseOne Tools Release 9.1 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: Section 3.3, "Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)".

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 to Release 9.1.2. 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	9.1.x	Must Update using existing standard self-update functionality.

Platform	Application Server	Current Release	Upgrade Release	Update Release	Notes
Windows Linux Solaris	WebLogic	9.1.2	9.1.x	9.1.x	For a WebLogic server, you must perform a fresh install using the Release 9.1 Update 2 or Update 3 installer. Future Updates possible using standard Update functionality. There is no Upgrade from OC4J. There is no Upgrade from one platform or application server to another.
Windows Linux Solaris	WebSphere	9.1.2	9.1.x	9.1.x	For a WebSphere server, you must perform a fresh install using the Release 9.1 Update 2 or Update 3 installer. Future updates possible using standard Update functionality. There is no Upgrade from OC4J. There is no Upgrade from one platform or application server to another.

3.5 Update Center Components for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)

For JD Edwards EnterpriseOne Tools Release 9.1 Update 2, in support of the matrix of products onto which the Server Manager Console can be installed and run (as described in the previous section entitled: Section 3.3, "Matrix of Supported Application Servers, JDKs, and Platforms for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)"), the following components are available for download from the JD Edwards EnterpriseOne Update Center:

- Server Manager Console Installer 9.1.3 for Microsoft Windows (the same installer is used for all supported application servers)
- Server Manager Console Installer 9.1.3 for Linux
- Server Manager Console Installer 9.1.3 for Solaris
- Server Manager Console Update 9.1.3 (the same installer is used for all supported platforms)

3.6 Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)

To obtain and extract the Server Manager Console:

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. Access the Oracle Software Delivery Cloud site, continue through the screens, and select these values on the Media Pack Search screen:

   Microsoft Windows

   - Select a Product Pack: **JD Edwards EnterpriseOne**
   - Platform: **JD Edwards EnterpriseOne Tools 9.1 Update 3 Media Pack for Microsoft Windows x64 (64-bit)**

   Linux

   - Select a Product Pack: **JD Edwards EnterpriseOne**
   - Platform: **JD Edwards EnterpriseOne Tools 9.1 Update 3 Media Pack for Linux x64 (64-bit)**

   Solaris

   - Select a Product Pack: **JD Edwards EnterpriseOne**
   - Platform: **JD Edwards EnterpriseOne Tools 9.1 Update 3 Media Pack for Solaris (64-bit)**

4. Click the Go button to display the results.

5. In the results grid, click the radio button next to the proper description. There are not separate downloads for English and non-English languages. The description is entitled:

   Microsoft Windows

   - **JD Edwards EnterpriseOne 9.1.3 Server Manager Installer Windows (1/2)**
   - **JD Edwards EnterpriseOne 9.1.3 Server Manager Installer Windows (2/2)**

   Linux

   - **JD Edwards EnterpriseOne 9.1.3 Server Manager Installer Linux**

   Solaris

   - **JD Edwards EnterpriseOne 9.1.3 Server Manager Installer Solaris**

6. Click the **Download** button next to the item that you wish to download.

   Note: Multiple Parts Downloads. Due to the maximum file size restrictions for downloads on Oracle Software Delivery Cloud, you will need to download multiple parts for a selected part number.

7. Save the `.zip` file to the temporary installation directory you created in Step 2. If you followed the recommendation, the directory is named

   Microsoft Windows

   `C:\SM_Console`

Linux or Solaris

```
/u01/SM_Console
```

8. **Microsoft Windows**

   After you finish downloading the first item, labeled (1/2), select the corresponding row for the second item labeled (2/2) and click the Download button.

   Linux or Solaris

   Proceed to Step 10.

9. Again, save the `.zip` file to the same directory where you saved the previous `.zip` file.

10. After you finish downloading all parts of 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
    ```

11. 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	Size	Packed Size
Disk1	174 313 360	171 868 931
Disk2	1 774 591 046	1 775 128 456
META-INF	53	54
9.1.3.0-Server-Manager_06_25.html	405 027	84 519
manifest.xml	543 078	90 754
udc.xml	8 651	1 344

3.7 Install the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)

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 9.1 Update 2 or Update 3 version of Server Manager Console uses the corresponding 9.1 Update 2 or Update 3 versions of the agents.

This section describes these topics:

- Section 3.7.1, "Installing the Management Console as an OC4J (Standalone Application Server)"
- Section 3.7.2, "Installing the Management Console on WebLogic Server Tools (Release 9.1 Update 2)"
- Section 3.7.3, "Installing the Management Console on WebSphere Application Server (Tools Release 9.1 Update 2 and Update 3)"

3.7.1 Installing the Management Console as an OC4J (Standalone Application Server)

Note: This installation process is the same for both the base and Update 2 and Update 3 release of JD Edwards EnterpriseOne Tools Release 9.1. The installer bundles a standalone application server and the Server Manager Console on Microsoft Windows platforms only. The only difference between the OC4J installer for base Tools Release 9.1 and Tools Release 9.1 Update 2 and Update 3 is the addition of a selection screen for the Application Server Types. Otherwise the installers are functionally identical.

This section discusses these topics:

- Section 3.7.1.1, "Prerequisites for OC4J"
- Section 3.7.1.2, "Running the OC4J Installer for the Server Manager Console"
- Section 3.7.1.3, "Verifying the OC4J Installation"

3.7.1.1 Prerequisites for OC4J

The TEMP and TMP Environment Variables should be configured and should point to valid paths on the machine and should have enough of disk space to perform the installation. The

Admin user running the Server Manager Console installer should have read/write access to the directories pointed by TEMP and TMP Environment Variables.

3.7.1.2 Running the OC4J Installer for the Server Manager Console

To install the Server Manager Console:

1. Change to the directory in which you extracted the Server Manager Console installer as described in the previous section of this chapter entitled: Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)".

2. 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 Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)":

   ```
   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.

   Linux or Solaris

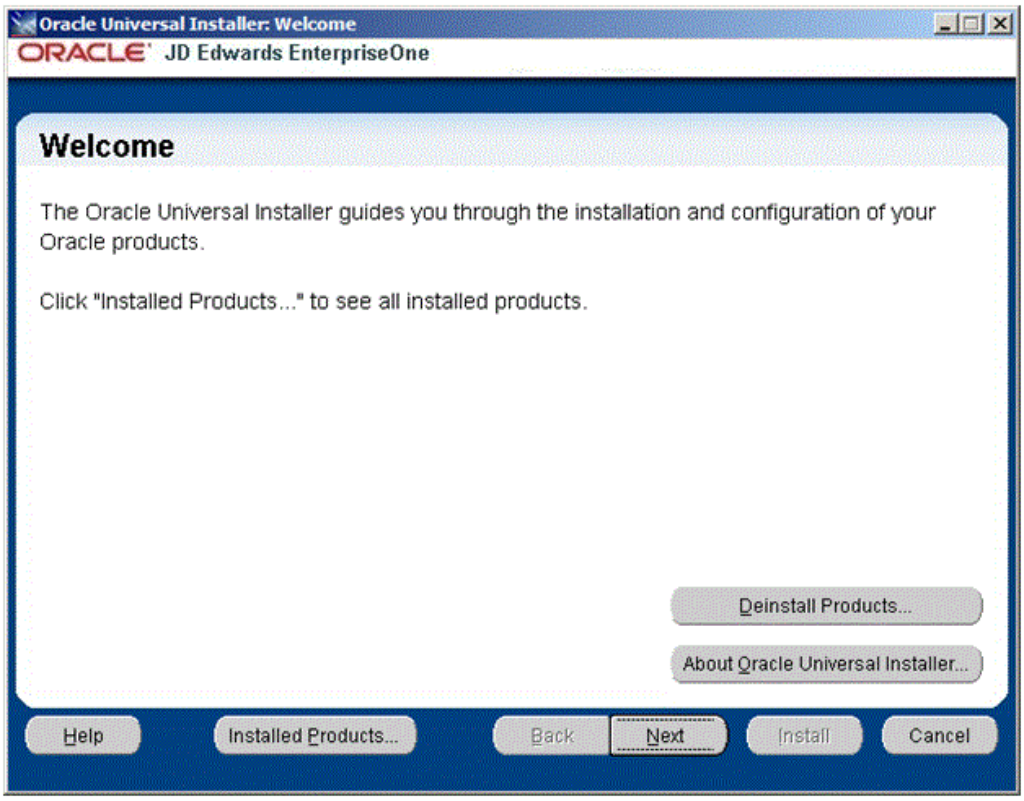
   Execute `runInstaller` from the directory in which you unzipped the installer. For example, if you followed the recommendation in Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)":

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

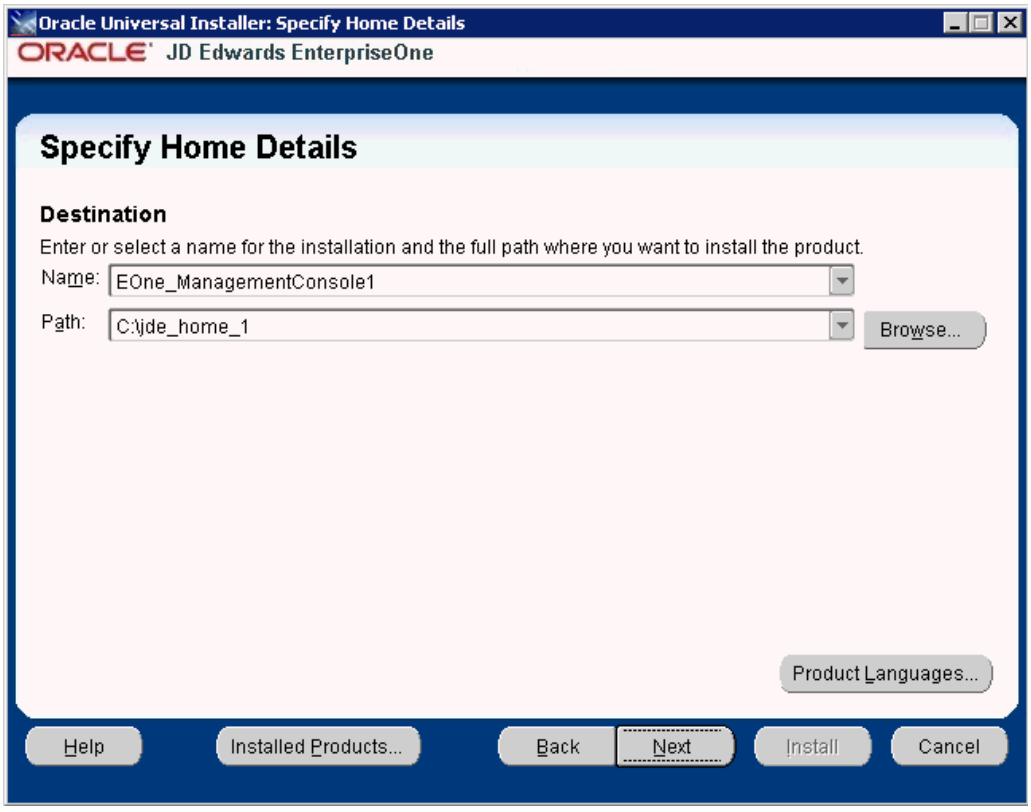
   All Platforms

   As the setup program launches, the Oracle Universal Installer (OUI) Wizard begins to initialize and prepare the bundled JVM for the JD Edwards EnterpriseOne Management Console installer. Although this may take a few minutes to completely initialize, you can view the progress on the Command window dialog that appears on your screen or Task Bar. When the initialization is complete, a new and separate JD Edwards EnterpriseOne Management Console installer window is displayed.

   It will take a minute or so for the initialization to complete. Upon completion the OUI Welcome panel displays:



3. On Welcome, click the Next button.



4. On Specify Home Details, complete these fields:

- *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.

- *Path*

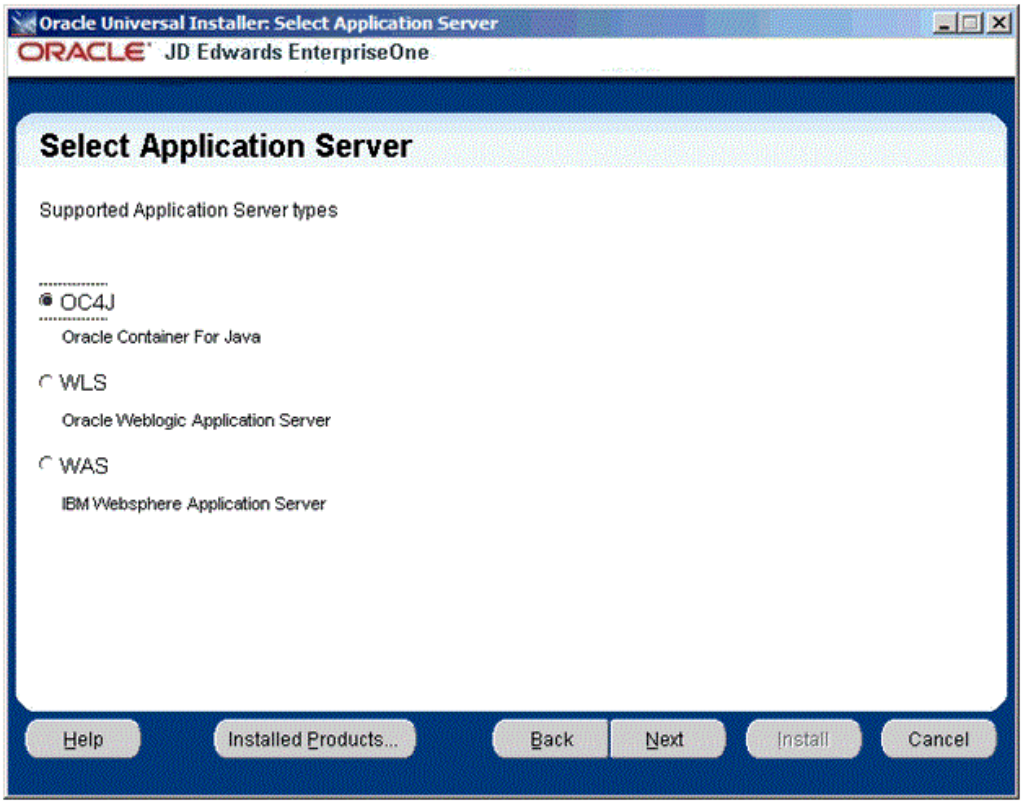
  Enter the drive and directory where you want the files installed on your Management Console. The JD Edwards EnterpriseOne Management Console installer automatically detects the root drive location on the Microsoft Windows machine and by default appends this value:

  jde_home

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

5. Click the Next button.

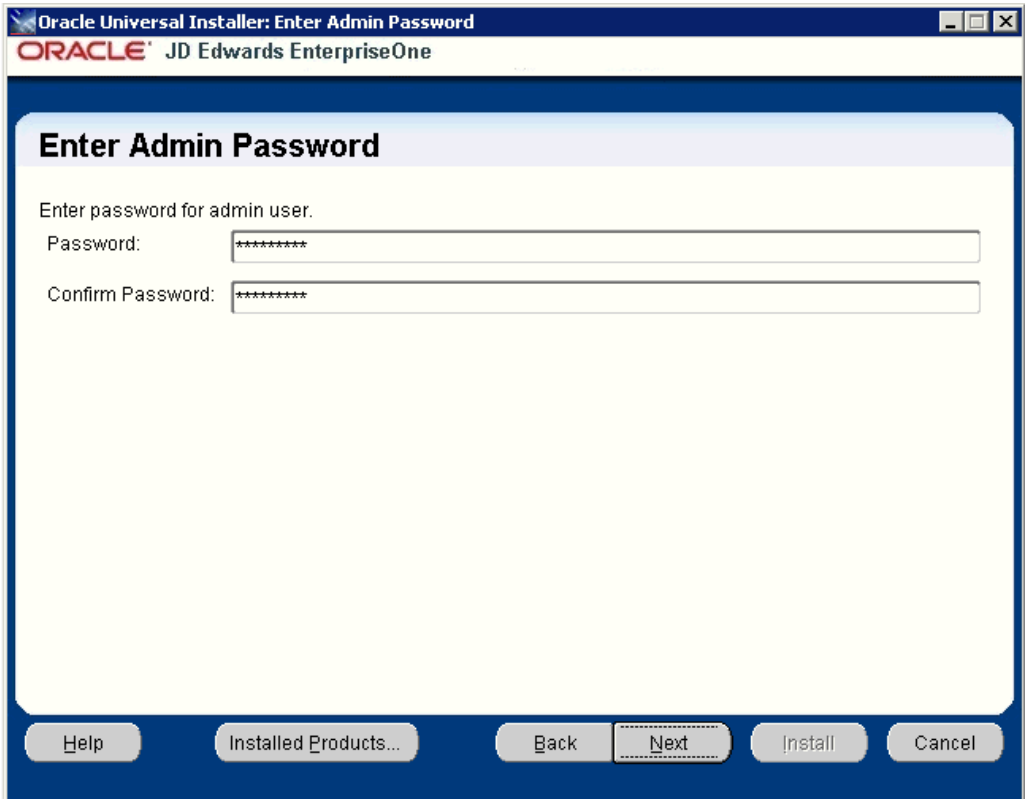


6. On Select Application Server, select this radio button:

   OC4J

   Oracle Container For Java

7. Click the Next button.



8. 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: ! @ # $ _.

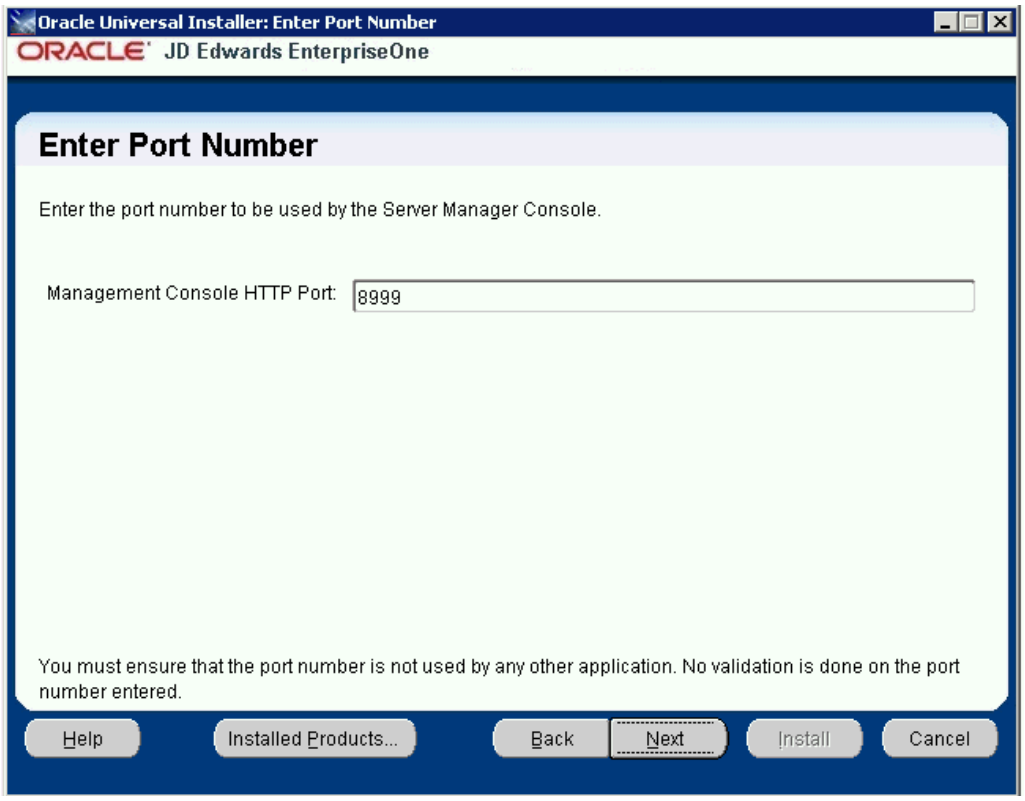
Note: The default value for the user named jde_admin is automatically populated by the Management Console installer and cannot be altered. This is the administrative user account that is associated with the Management Console.

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.

9. Click the Next button.



10. On Enter Port Number, complete this field:

- Management Console HTTP Port

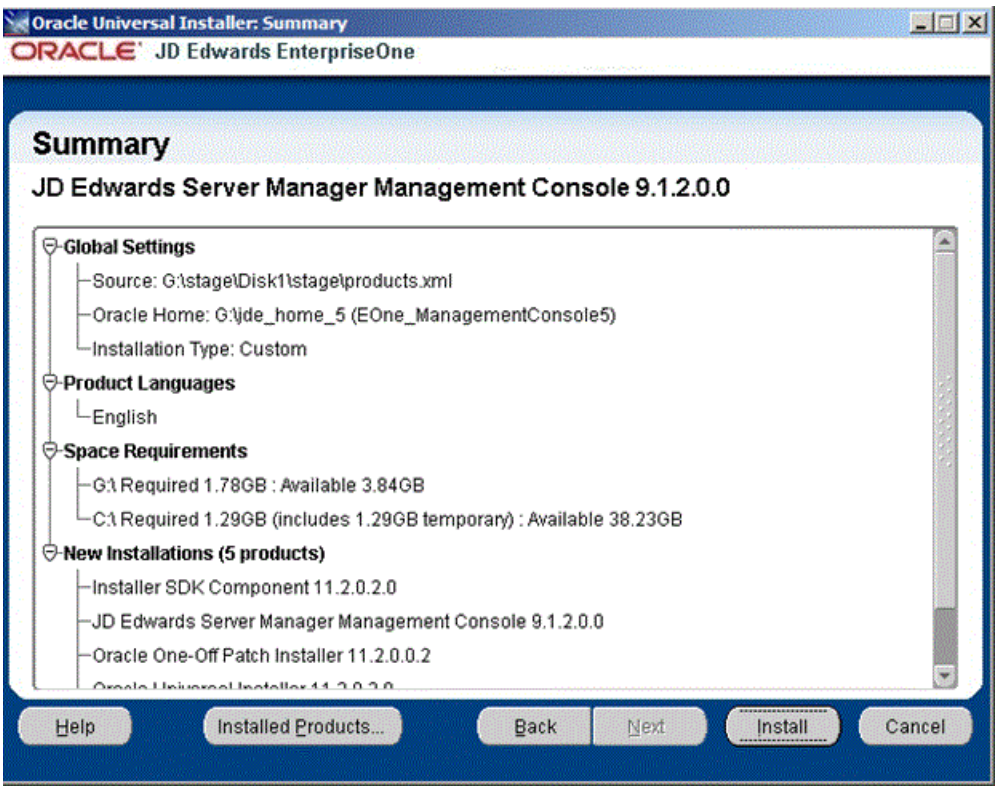
  Enter valid unused port number for use by the Management Console.

  The default value is 8999.

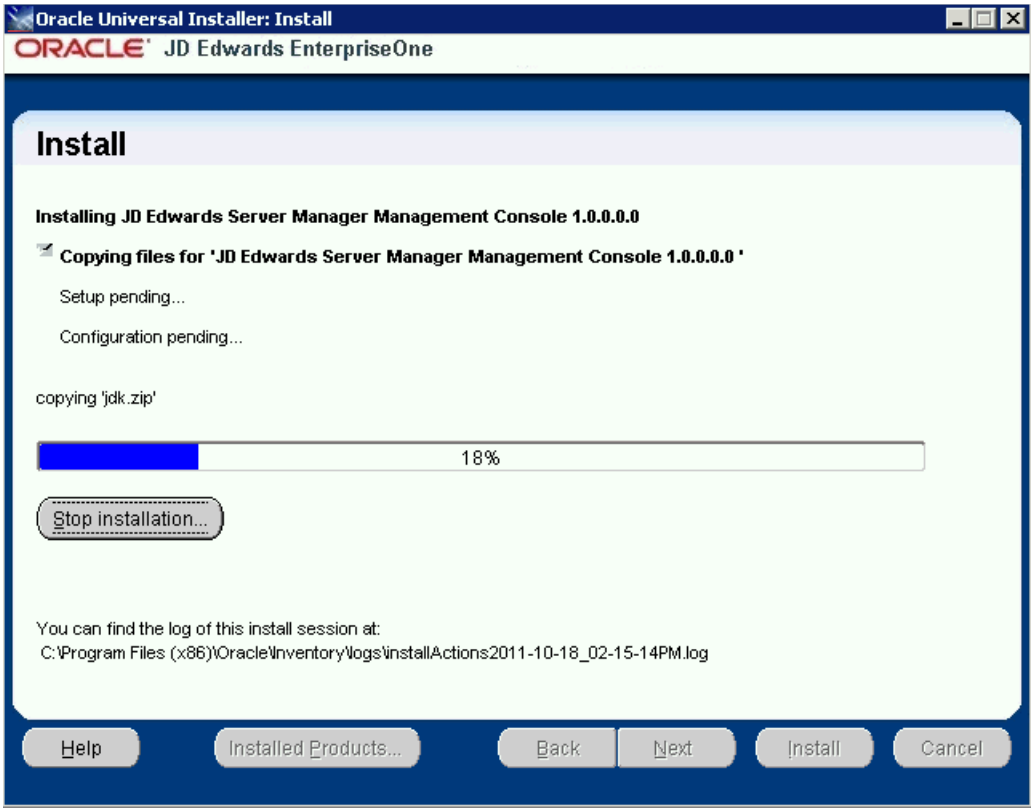
Caution: This port number must be available and cannot be in use by any other application on this machine. Since the installer cannot validate the port, you must be certain that these conditions are met or else the Management Console will not start.

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

11. Click the Next button.

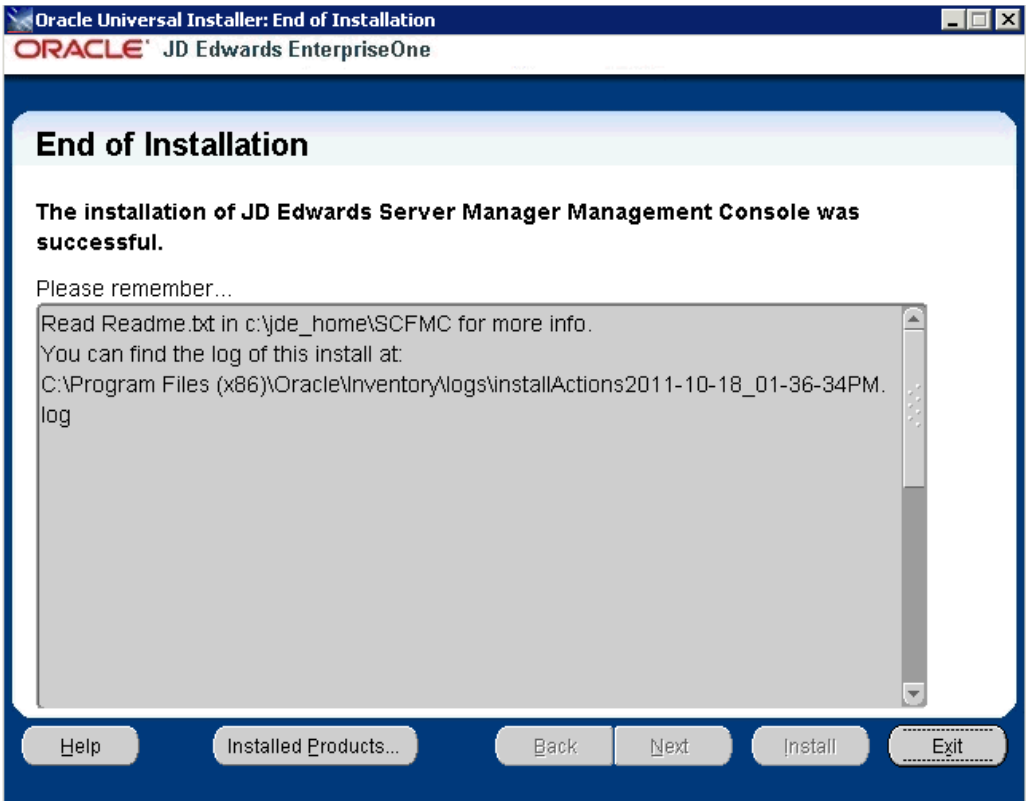


12. On Summary, verify your selections and click the Install button to begin the installation.



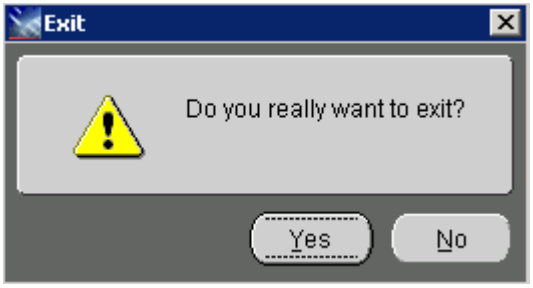
The Install progress screen is displayed. Note that this screen displays the location of the log of this installation. For example:

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



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

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



15. On the Exit dialog, click the Yes button.

3.7.1.3 Verifying the OC4J Installation

To verify the OC4J installation:

1. 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/
```

3.7.2 Installing the Management Console on WebLogic Server Tools (Release 9.1 Update 2)

Beginning with JD Edwards Tools Release 9.1 Update 2, you can install the Server Manager Console on WebLogic Server on Microsoft Windows, Linux, or Solaris platforms.

Note: Installation of the Server Manager Console on Oracle WebLogic Server 12c is supported beginning with Tools Release 9.1, Update 4.

See Also

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

- Oracle WebLogic Server 10.3.5 Documentation Home

  http://docs.oracle.com/cd/E21764_01/wls.htm

- Oracle WebLogic Server 12.1.2 Documentation Home

  http://docs.oracle.com/middleware/1212/wls

- 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:

- Section 3.7.2.1, "Prerequisites for WebLogic Server"
- Section 3.7.2.2, "Running the WebLogic Server Installer for the Server Manager Console"
- Section 3.7.2.3, "Verifying the Server Manager Console Installation on WebLogic Server"
- Section 3.7.2.4, "Enable SSL for Server Manager Console on the WebLogic Server"
- Section 3.7.2.5, "Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore"
- Section 3.7.2.6, "Troubleshooting the Server Manager Console Installation on WebLogic Server"

3.7.2.1 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.
- 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.

  Linux and Solaris

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

- 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 `nodemanger.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 `nodemanger.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\user_projects\domains\<domain_
  name>\nodemanager\nodemanager.properties
  ```

  Linux and Solaris

  WebLogic Server 11g

  ```
  /u01/Oracle/Middleware/wlserver_
  10.3/common/nodemanager/nodemanager.properties
  ```

  WebLogic Server 12c

  ```
  /u01/Oracle/Middleware/user_projects/domains/<domain_
  name>/nodemanager/nodemanager.properties
  ```

- There is no utility to stop the nodemanager process and this has to be stopped 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:

  1. Login into WebLogic Server AdminServer console.
  2. Go to the Environment > Machines tab and select the nodemanager machine to which the Domain is registered.
  3. 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\wlserver`

  Linux and Solaris

  WebLogic Server 11g

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

  WebLogic Server 12c

  `/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.lok` 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.lok`

  Linux and Solaris

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

- 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.
- 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.

3.7.2.2 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: Section 3.7.2.1, "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: Section 3.6, "Obtain and Extract

the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)".

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 Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)":

```
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.

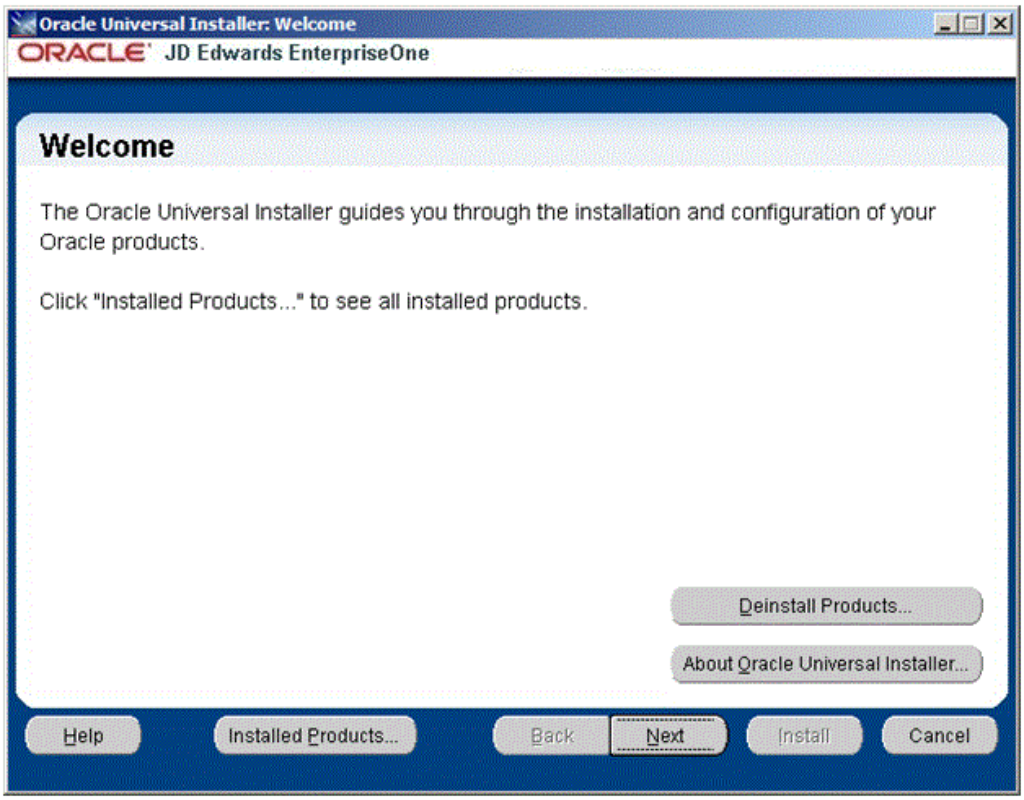
Linux or Solaris

Execute `runInstaller` from the directory in which you unzipped the installer. For example, if you followed the recommendation in Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)":

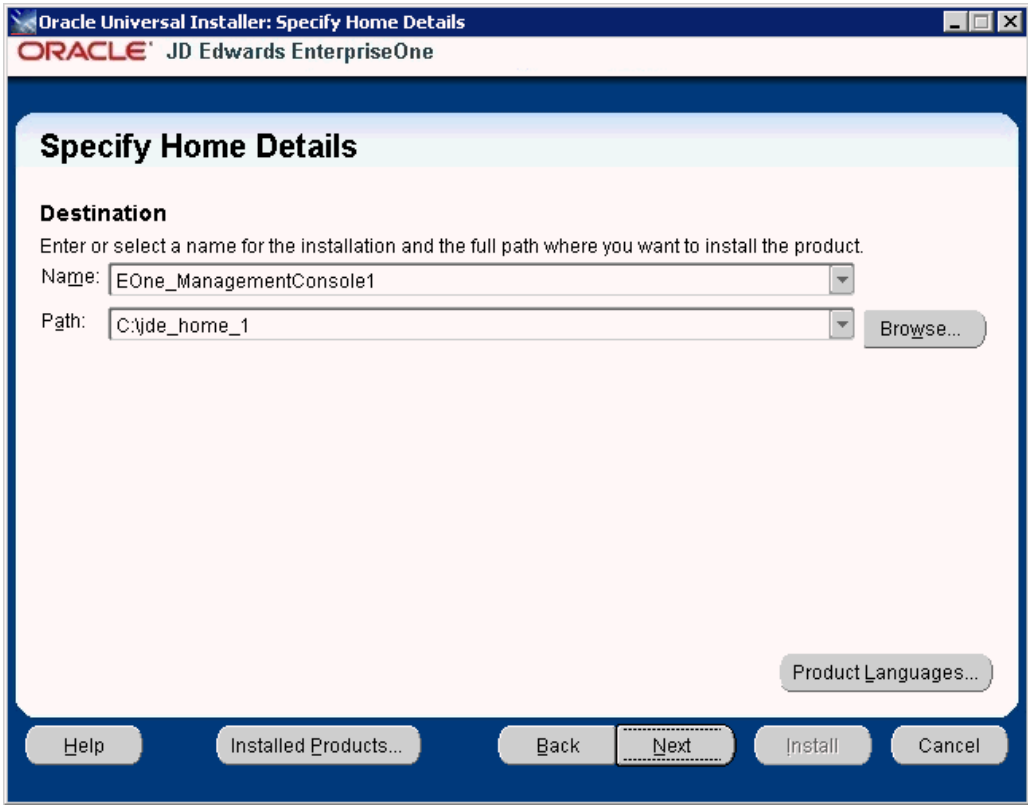
```
./SM_Console/Disk1/install/runInstaller
```

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.



4. On Welcome, click the Next button.



5. On Specify Home Details, complete these fields:

- *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.

- *Path*

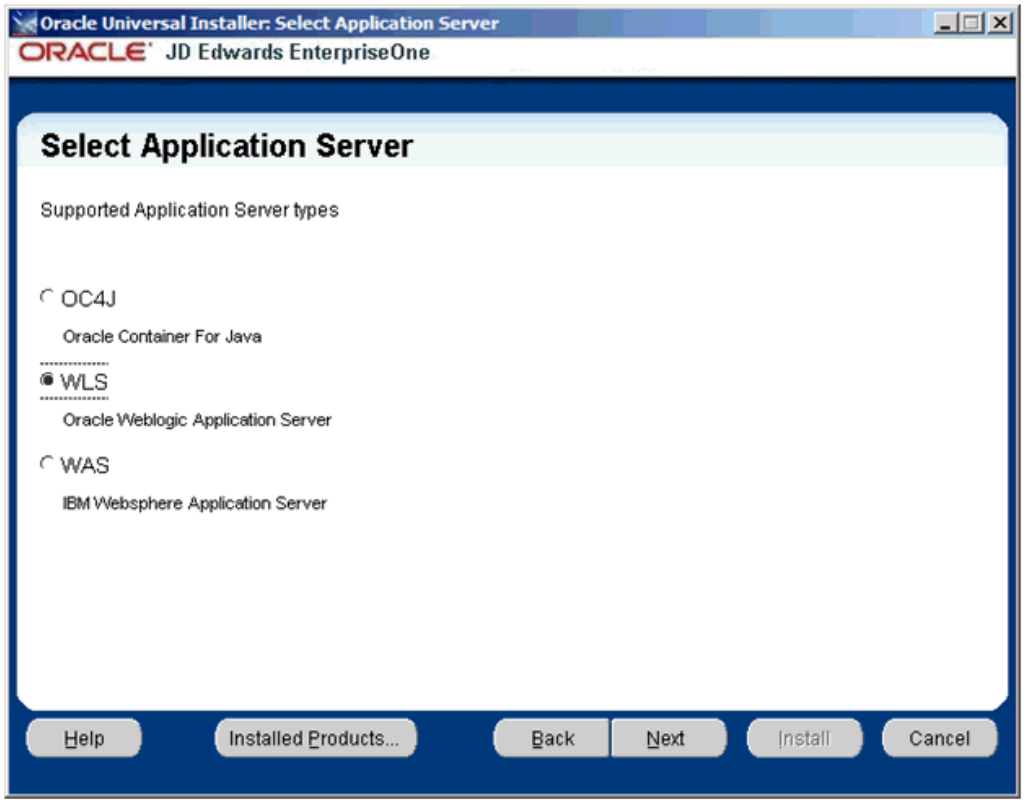
  Enter the drive and directory where you want the files installed on your Management Console. The JD Edwards EnterpriseOne Management Console installer automatically detects the root drive location on the machine and by default appends this value:

  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.



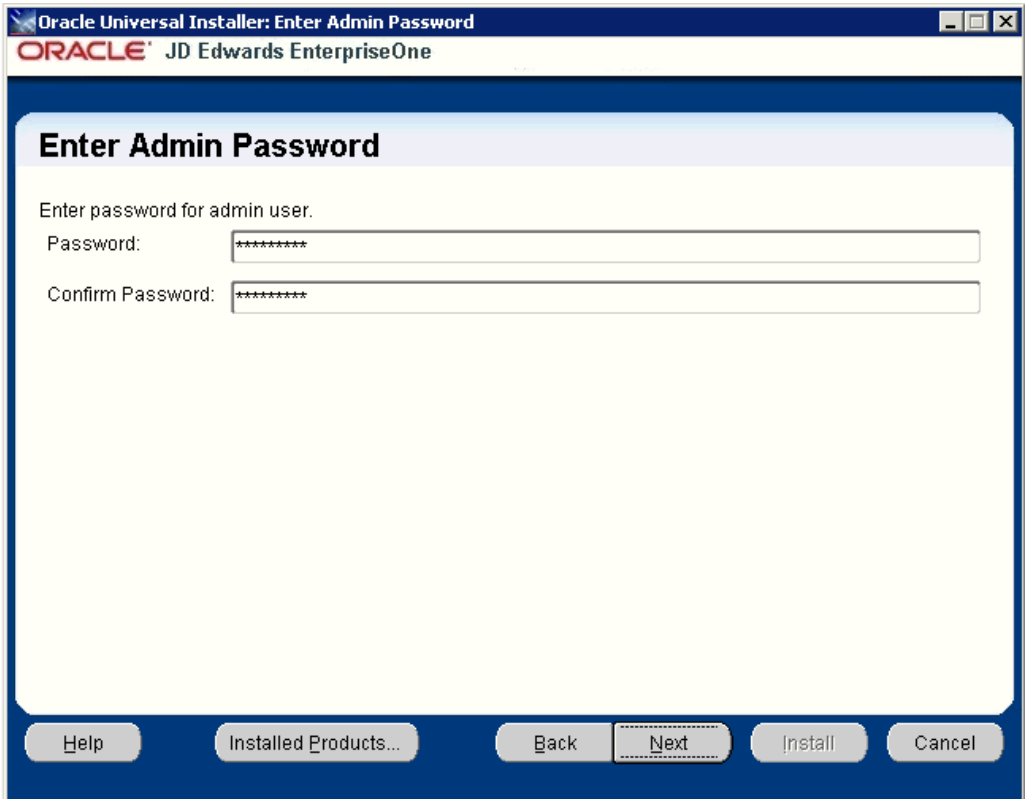
Note: If using Oracle Enterprise Linux, the above screen will not appear. The selection will default to WLS.

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

   WLS

   Oracle WebLogic Application Server

8. Click the Next button.



9. 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: ! @ # $ _

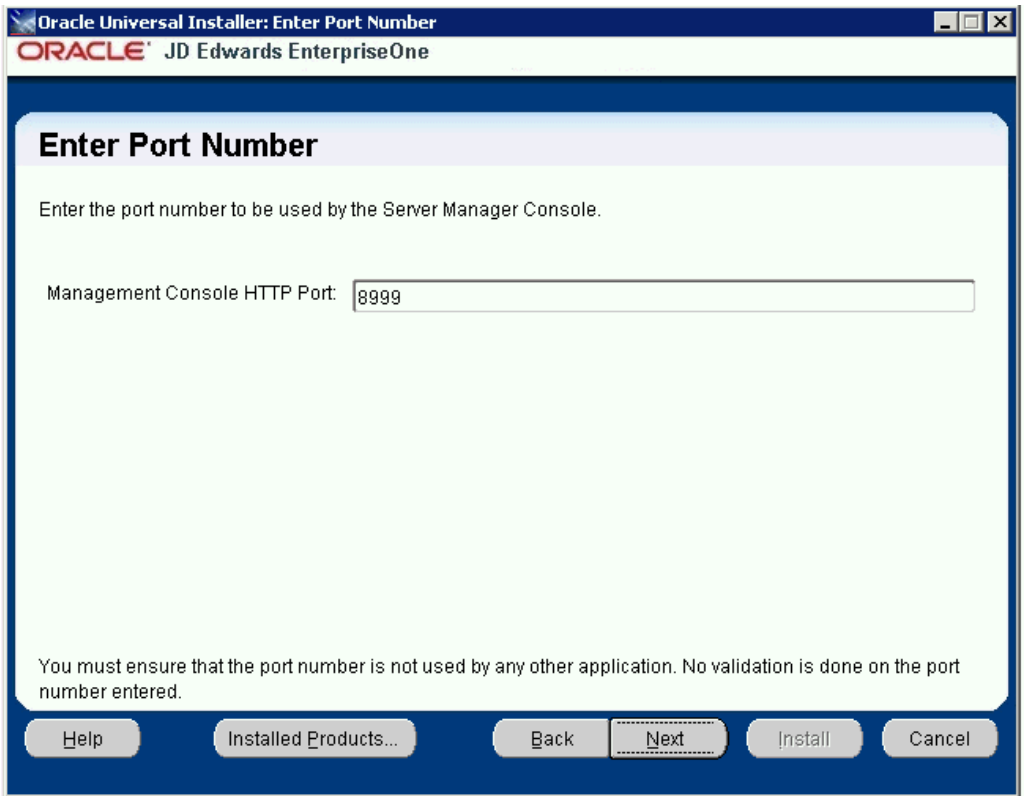
Note: The default value for the user named jde_admin is automatically populated by the Management Console installer and cannot be altered. This is the administrative user account that is associated with the Management Console.

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.

10. Click the Next button.



11. On Enter Port Number, complete this field:

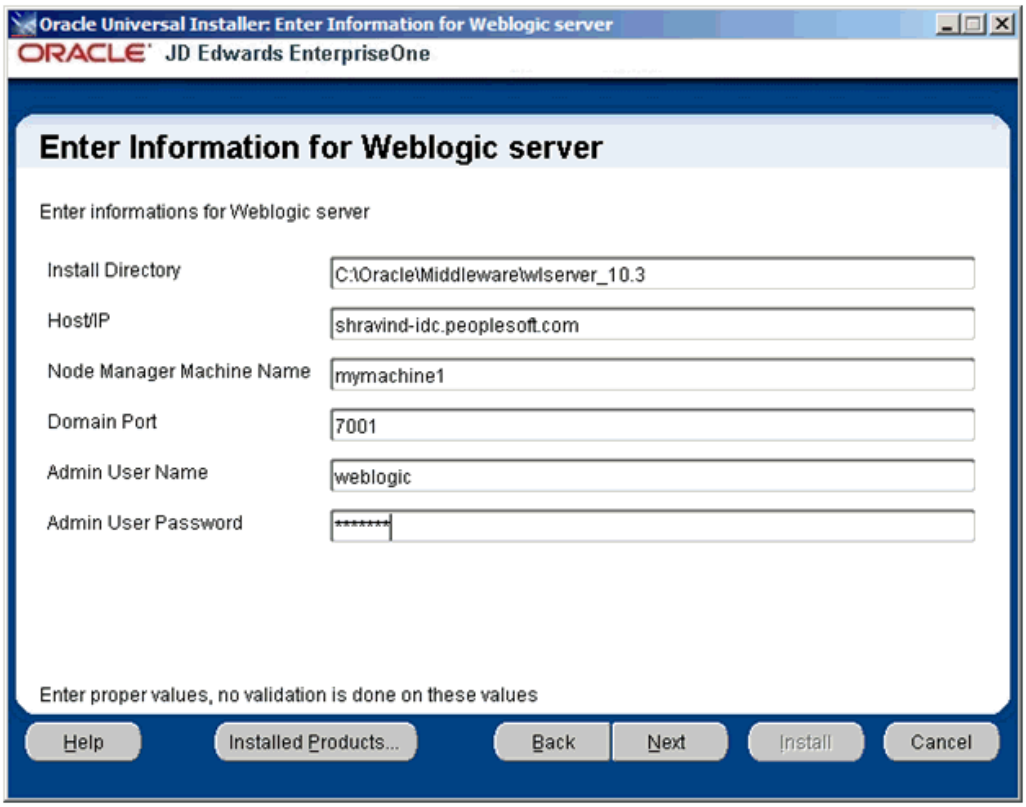
- Management Console HTTP Port

  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.



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

- *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\wlserver`

  Linux and Solaris

  WebLogic Server 11g

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

  WebLogic Server 12c

  `/u01/Oracle/Middleware/wlserver`

- *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:

  shravind-idc.peoplesoft.com

- *Node Manager Machine Name*

  The nodemanager machine name is not necessarily the physical machine name, but it can be the same.

- *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.

- *Admin User Name*

  Enter the user name of the WebLogic Server admin account.

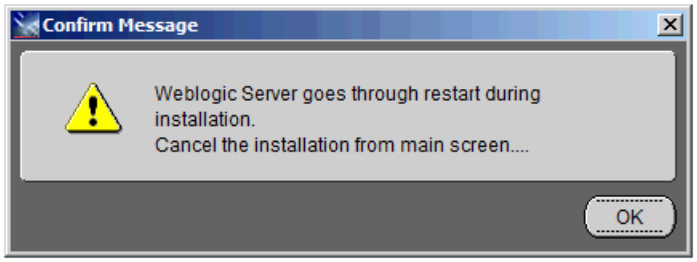
- *Admin User Password*

  Enter the password for the WebLogic Server admin account.

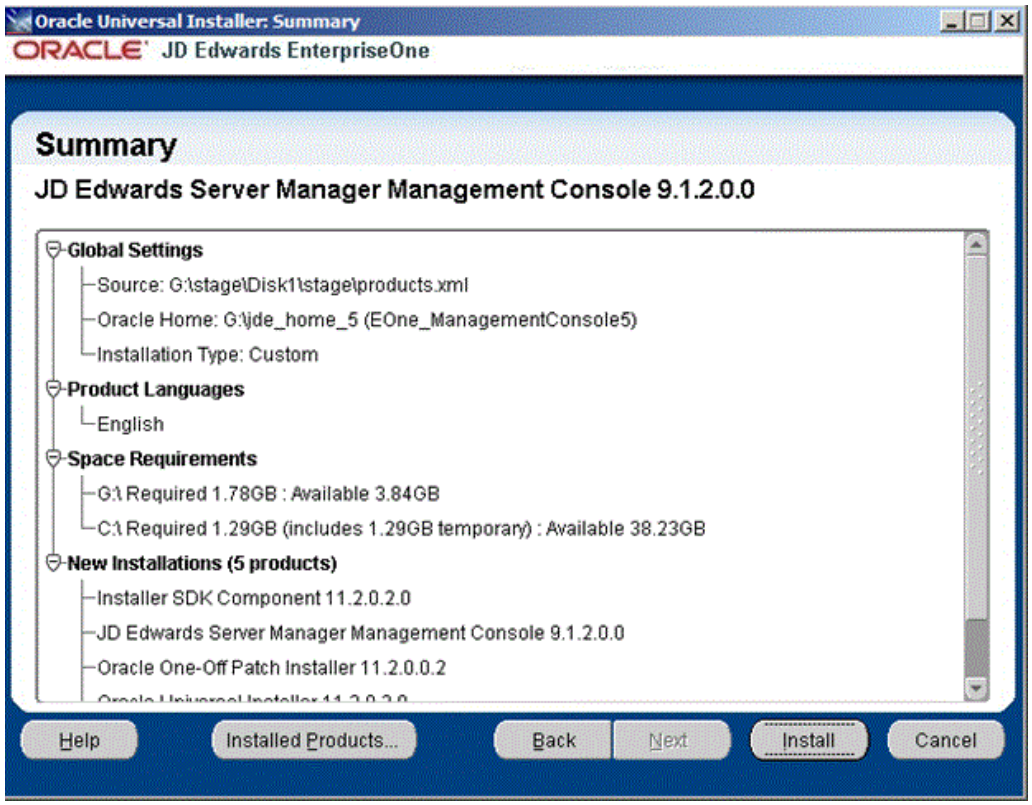
Caution: The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items. If you enter invalid values, you will have to re-run the installer with the correct values.

---

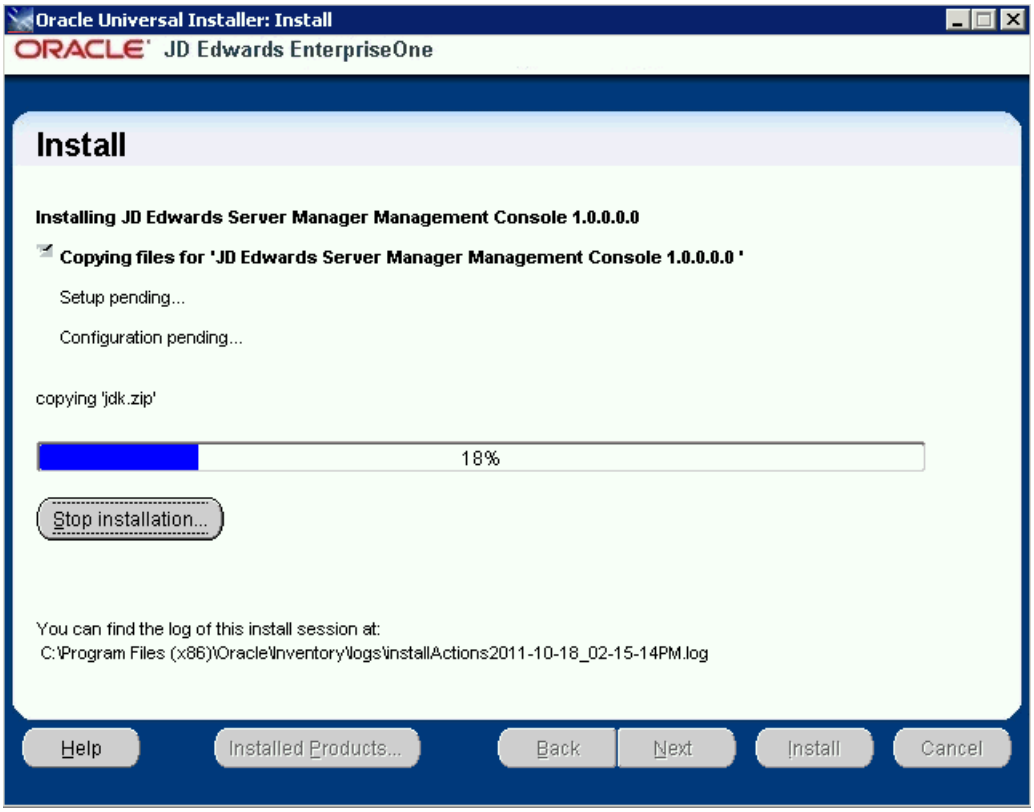
13. Click the Next button.



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.

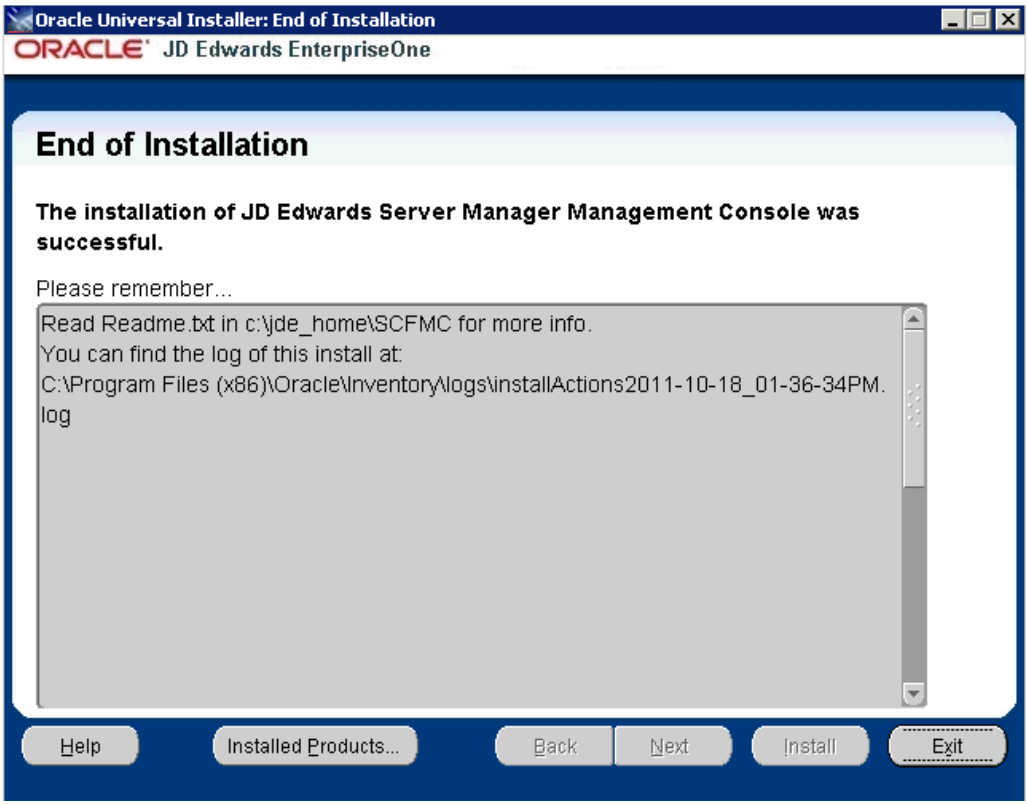


15. On Summary, verify your selections and click the Install button to begin the installation.



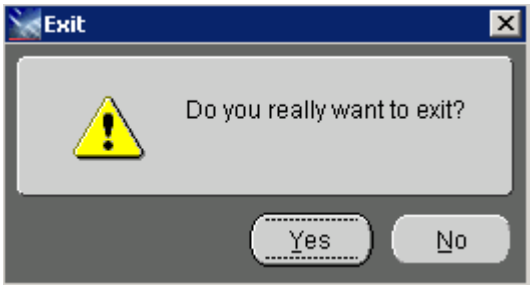
The Install progress screen is displayed. Note that this screen displays the location of the log of this installation. For example:

```
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.

3.7.2.3 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:

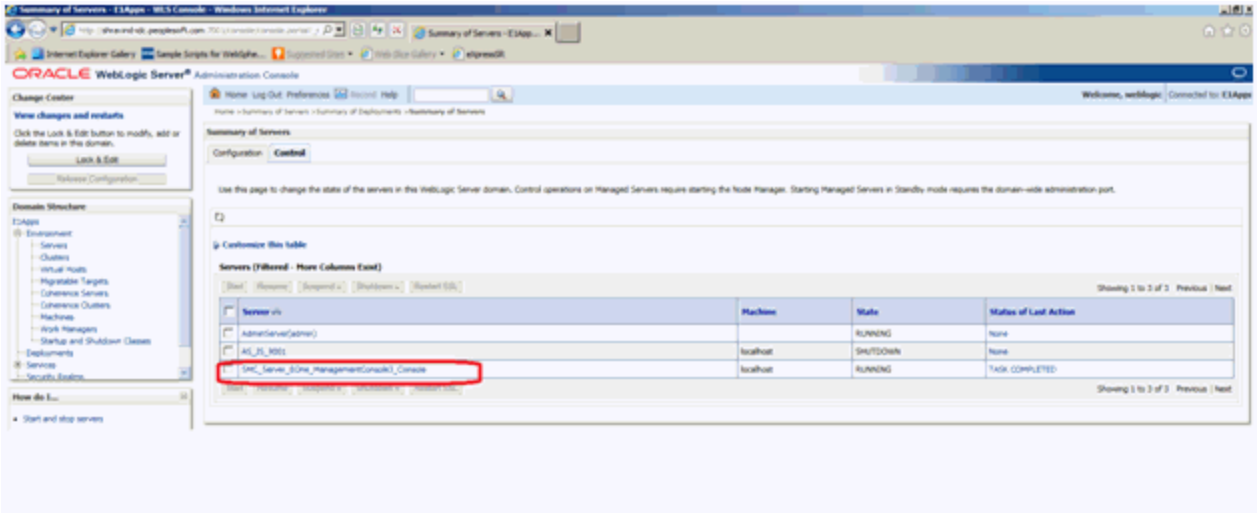
   Microsoft Windows

```
%DomainDir%\lib
```

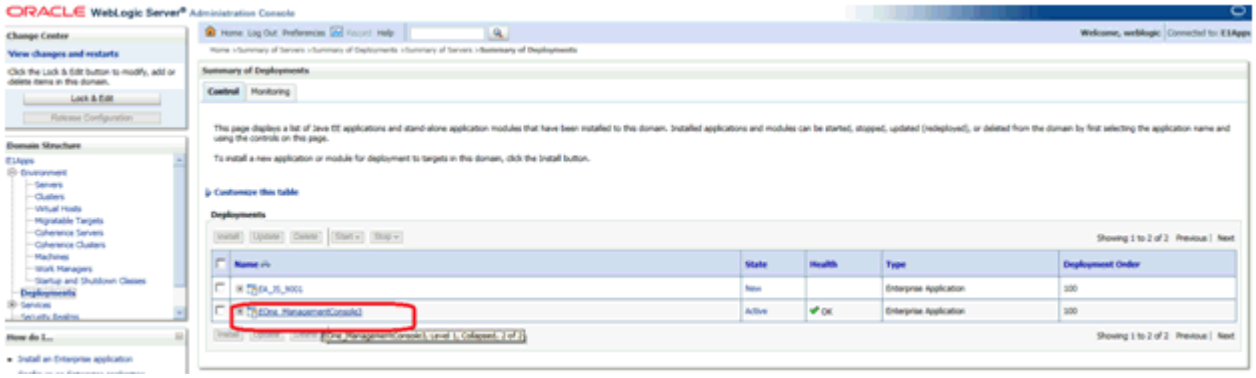
Linux or Solaris

```
$DomainDir/lib
```

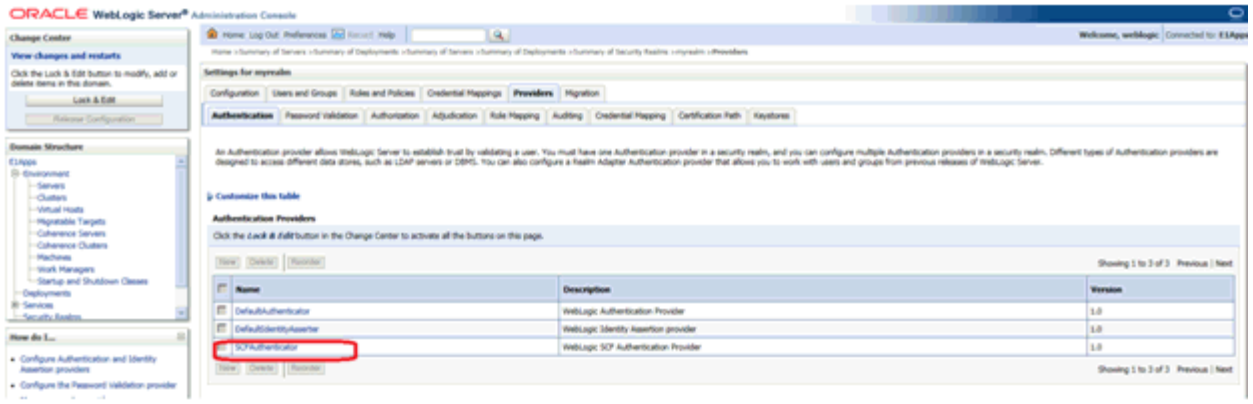
2. Go to the WebLogic Admin Server console and navigate to Environment > Servers. Verify that the Server Manager Console installer created a a new J2EE Server and that the state of that server is RUNNING. The following screen shows an example.



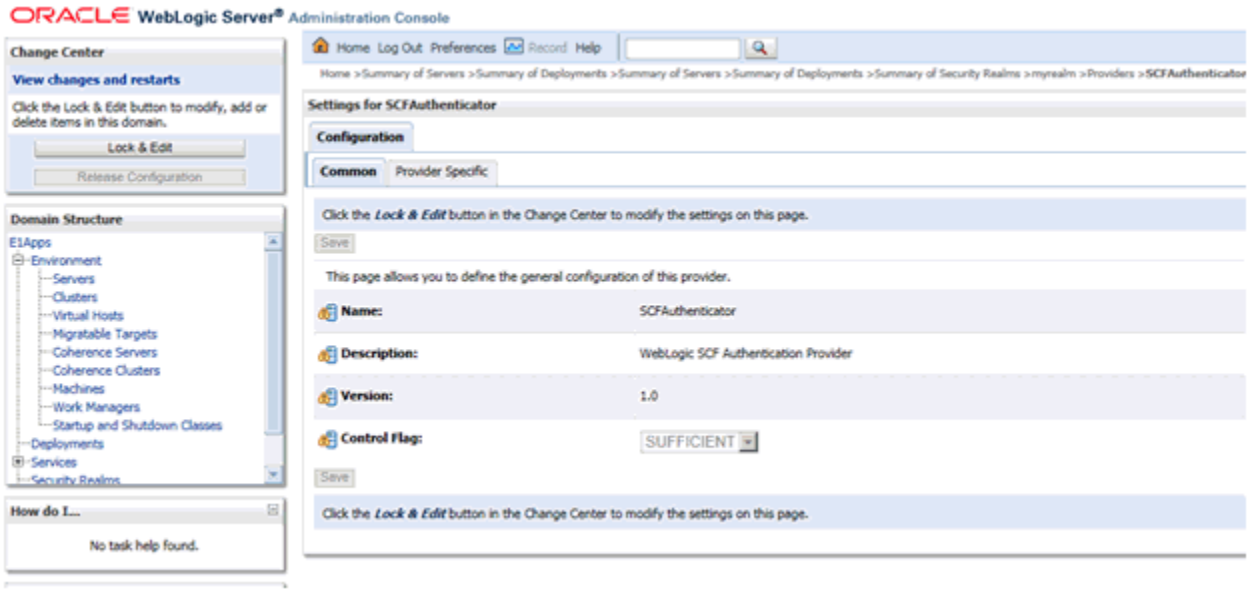
3. Go to Deployments and verify that the Server Manager Console is installed. The following screen shows an example.



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



5. 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.

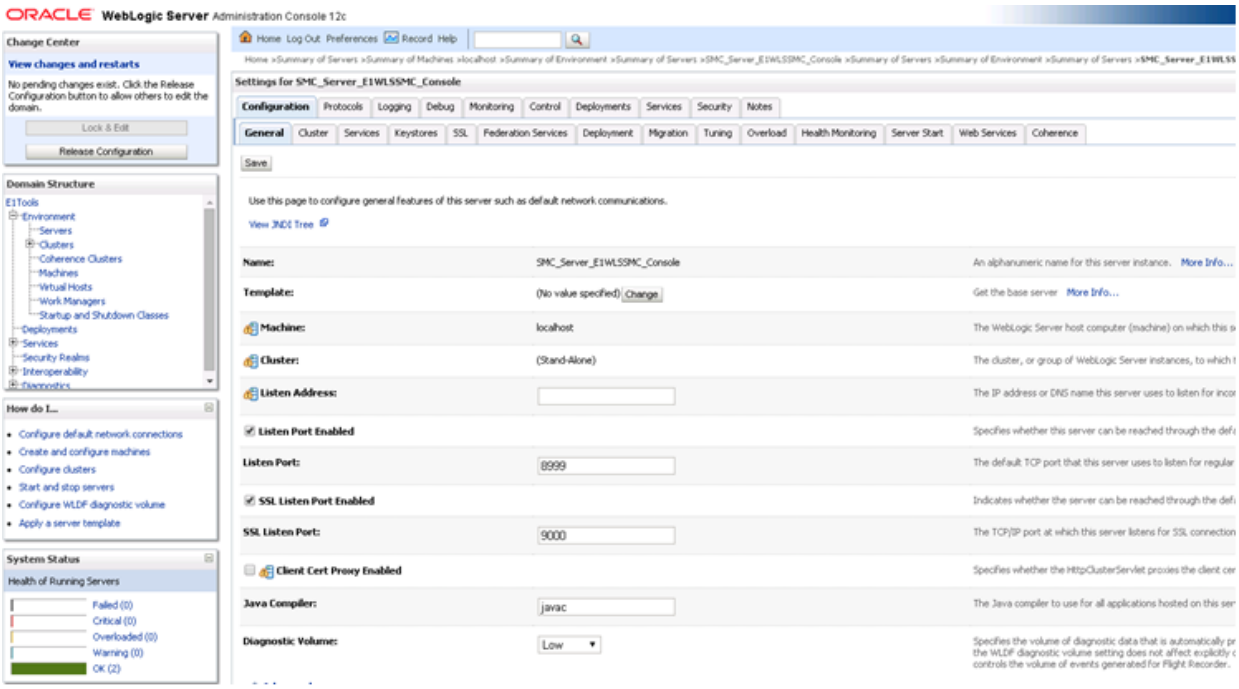
   For example:

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

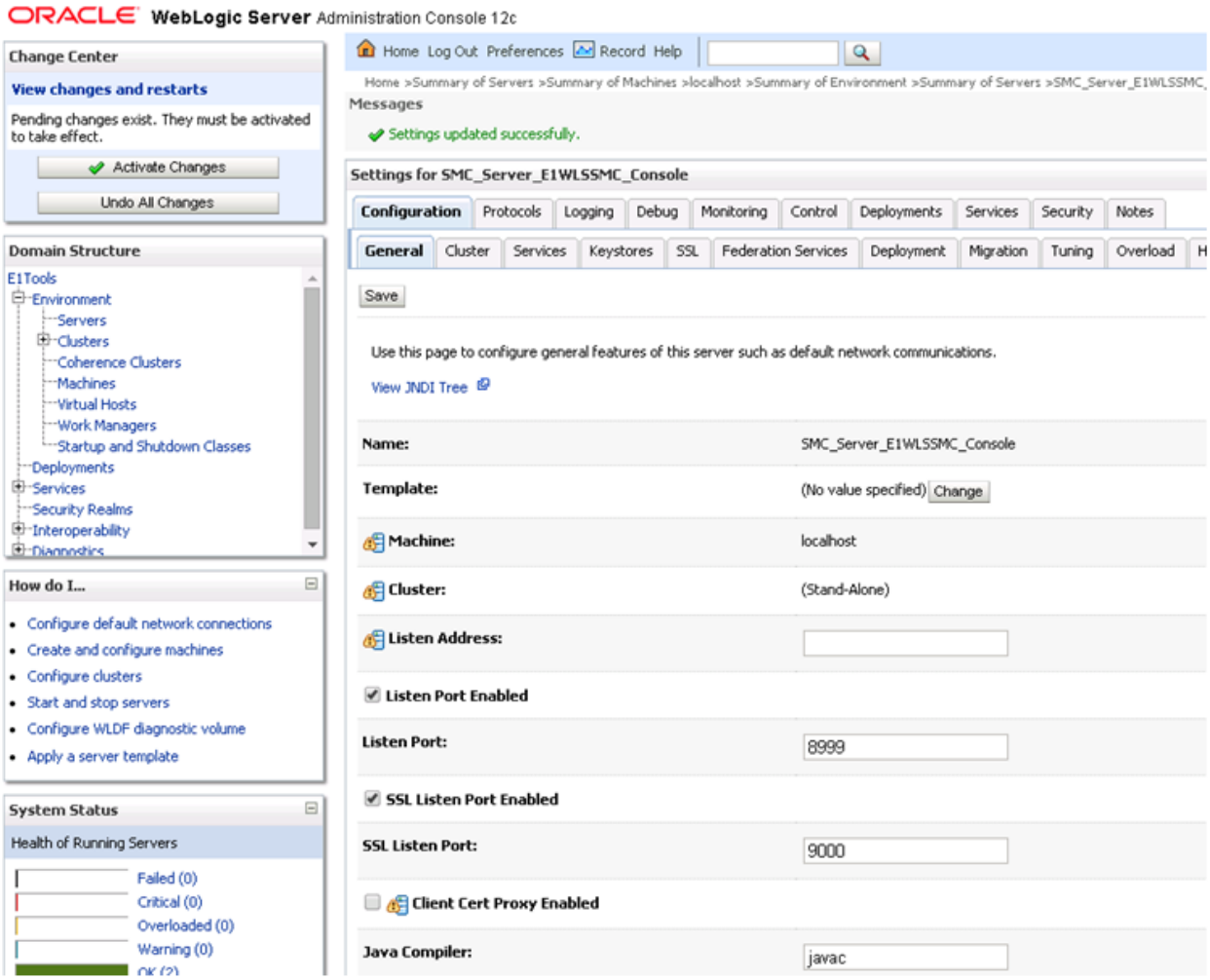
3.7.2.4 Enable SSL for Server Manager Console on the WebLogic Server

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

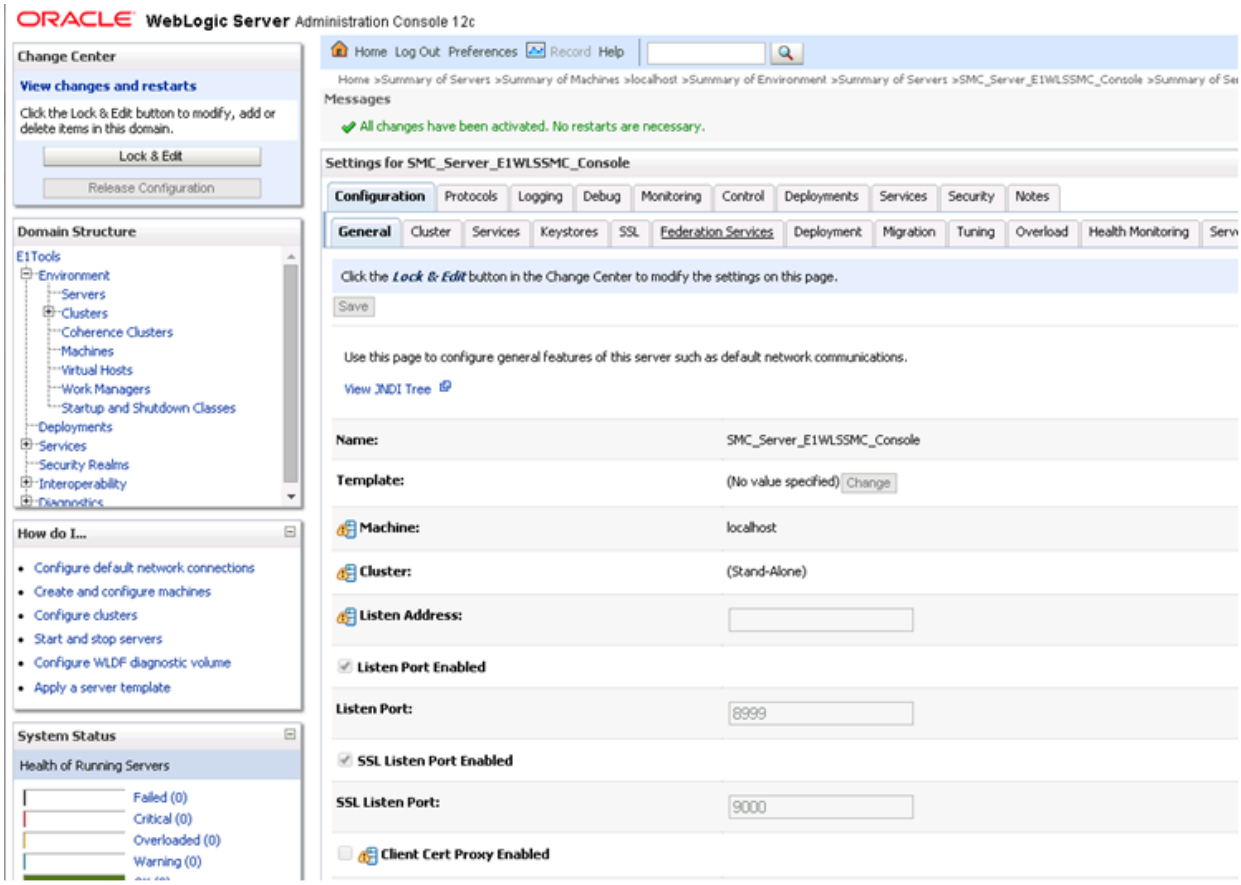
1. Access the Weblogic Admin Console in the browser for the Weblogic domain in which the Server Manager Console is installed. A sample URL would be:
   `https://denpbds11.company.com:7001/console`
2. Login to the Weblogic Admin Console using Weblogic Administrative Credentials.
3. Navigate to Environments -> 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.


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.
Lock & Edit
Release Configuration
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 (2)
Home Log Out Preferences Record Help
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 Health Monitoring Server Start Web Services Coherence
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: 8999
SSL Listen Port Enabled
SSL Listen Port: 9000
Client Cert Proxy Enabled
Java Compiler: javac
Diagnostic Volume: Low

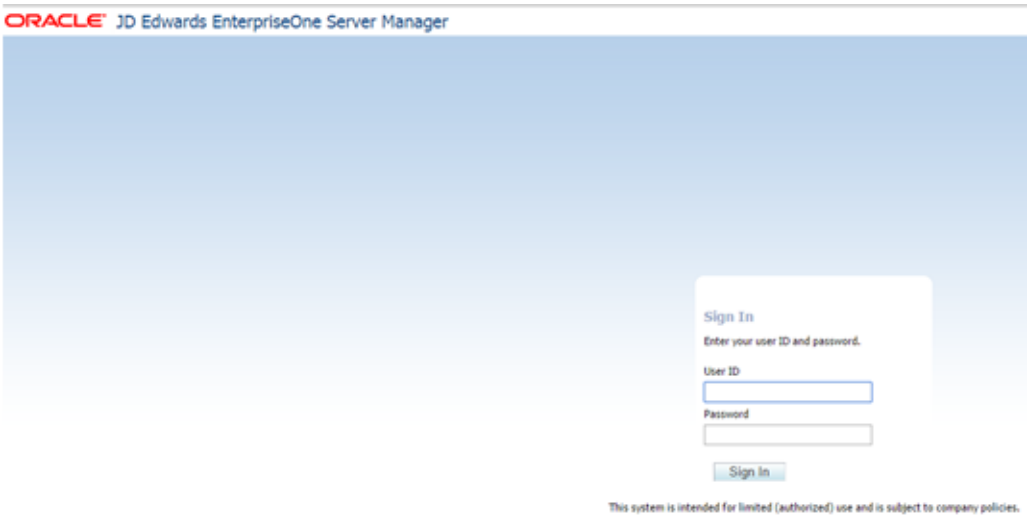
9. Click **Save**.



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.
13. 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.company.com:9000/manage/home`



14. Go to Section 3.7.2.5, "Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore" and perform the steps.

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

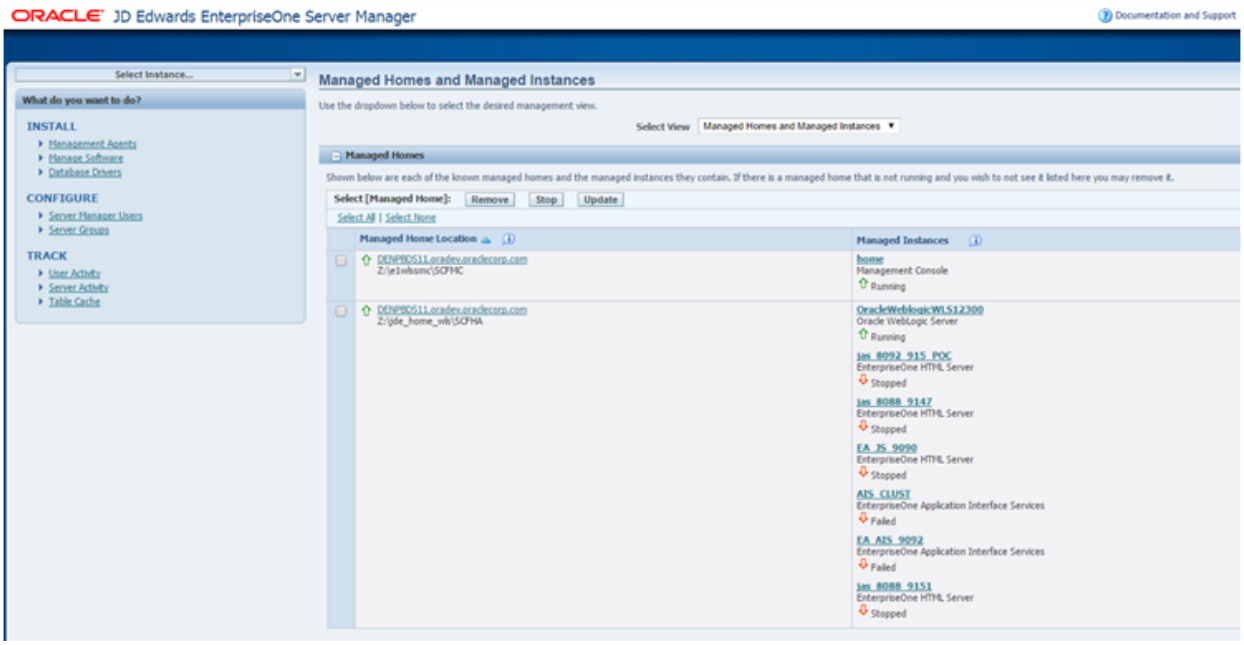
To import the Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore:

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.
4. 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**.

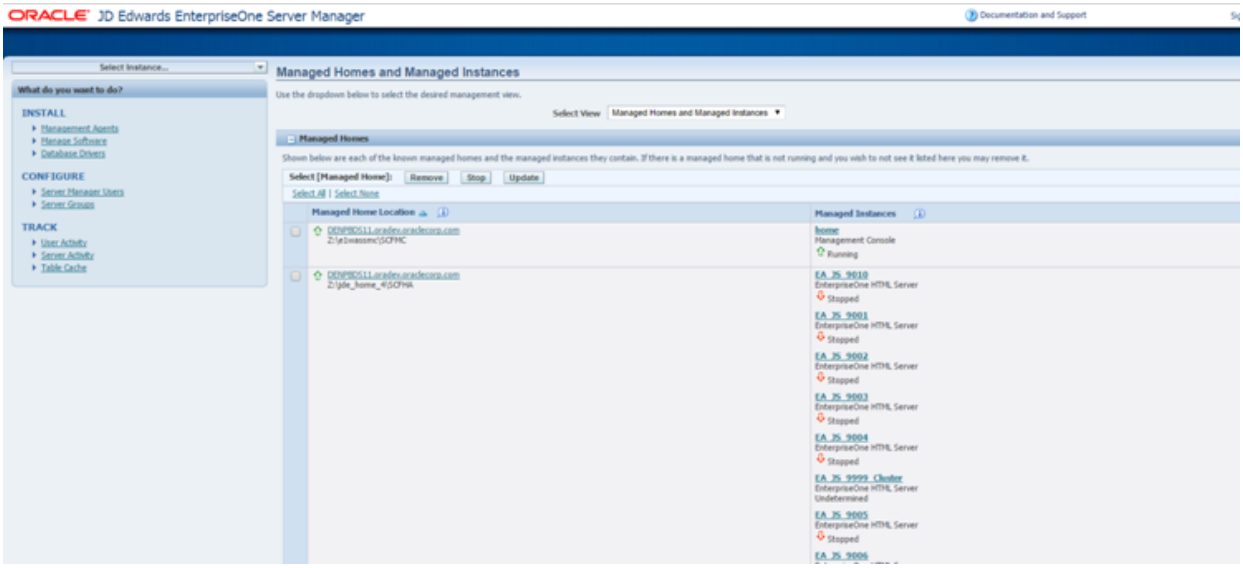
   ```
   X:\jde_home_1\SCFHA\jdk\jre\bin\keytool -import -alias smc_cert -file
   C:\SMC_Certificate.cer -keystore

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

5. 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.
6. 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> != <denpbds.company.com>

at
org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:227
)

at
org.apache.http.conn.ssl.BrowserCompatHostnameVerifier.verify(BrowserCompa
tHostnameVerifier.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.j
ava:437)

at
org.apache.http.impl.conn.DefaultClientConnectionOperator.openConnection(D
efaultClientConnectionOperator.java:180)

at
org.apache.http.impl.conn.ManagedClientConnectionImpl.open(ManagedClientCo
nnectionImpl.java:294)

at
org.apache.http.impl.client.DefaultRequestDirector.tryConnect(DefaultReque
stDirector.java:643)

at
org.apache.http.impl.client.DefaultRequestDirector.execute(DefaultRequestD
irector.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.E1Agent$ManagementServerDaemonThread.run(E1Agent.
java:2259)

at java.lang.Thread.run(Thread.java:722)
```

3.7.2.6 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: Section 3.7.2.1, "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 (x86)\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\Middlware\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.

BUG 20578571 - SERVER MANAGER CHARTS NOT UPDATING UPON PAGE LOAD

Issue / Resolution:

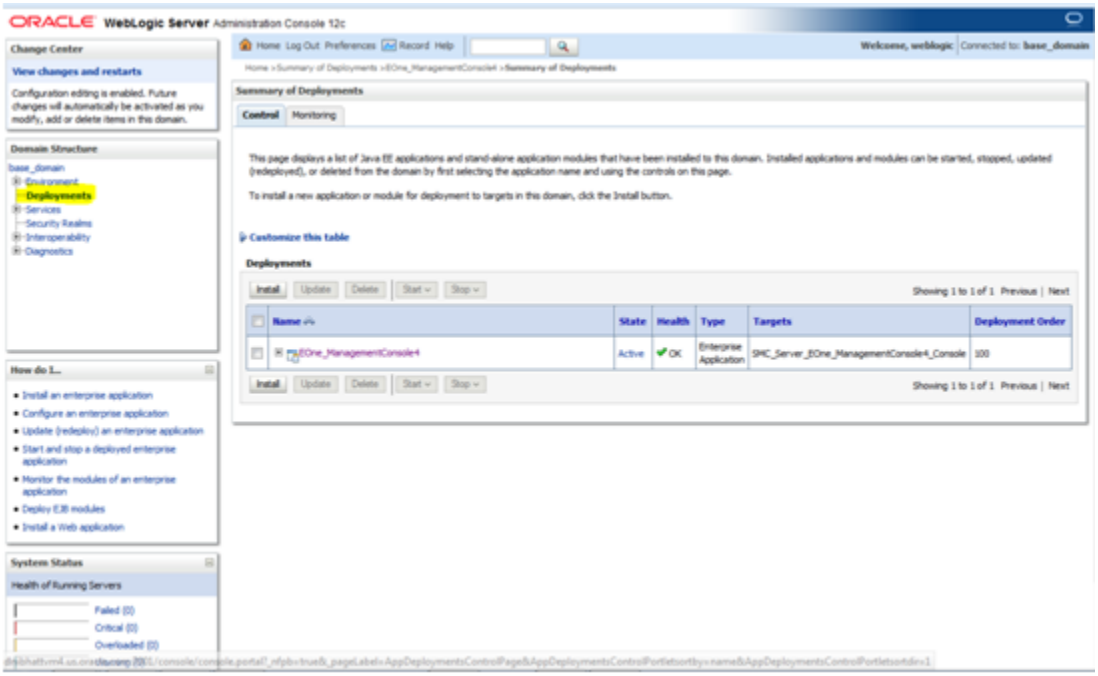
The resource charts for Enterprise Servers do not update each time you go to an Enterprise Server page. In order to get the charts to display current information, you must either do a CTRL+F5 or clear the browser cache. Otherwise, the charts will continue to display stale data.

This issue is fixed in Tools Release 9.2. The users on a Tools Release prior to 9.2. can get the Patch/POC from bug:

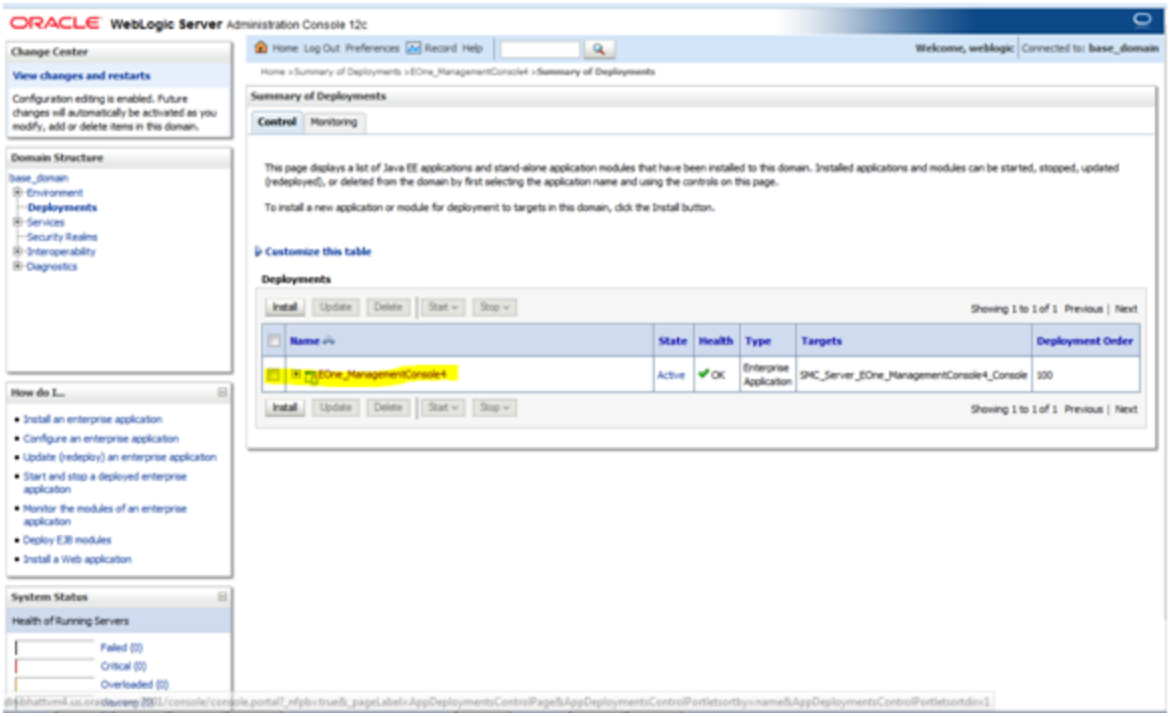
BUG 20578571 - SERVER MANAGER CHARTS NOT UPDATING UPON PAGE LOAD

For Server Manager users on WebLogic, if this patch/fix does not work, follow these steps to make it work:

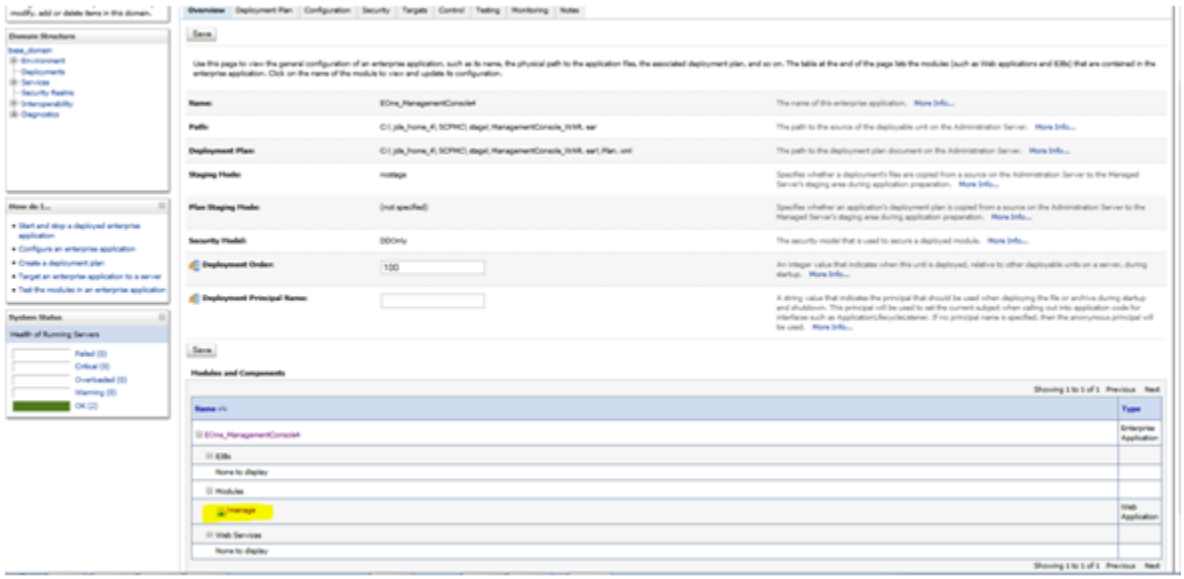
1. Login to the WebLogic Admin console.
2. On the left pane, if available, please click the **lock and edit** option.
3. Select **Deployments** on the left panel.



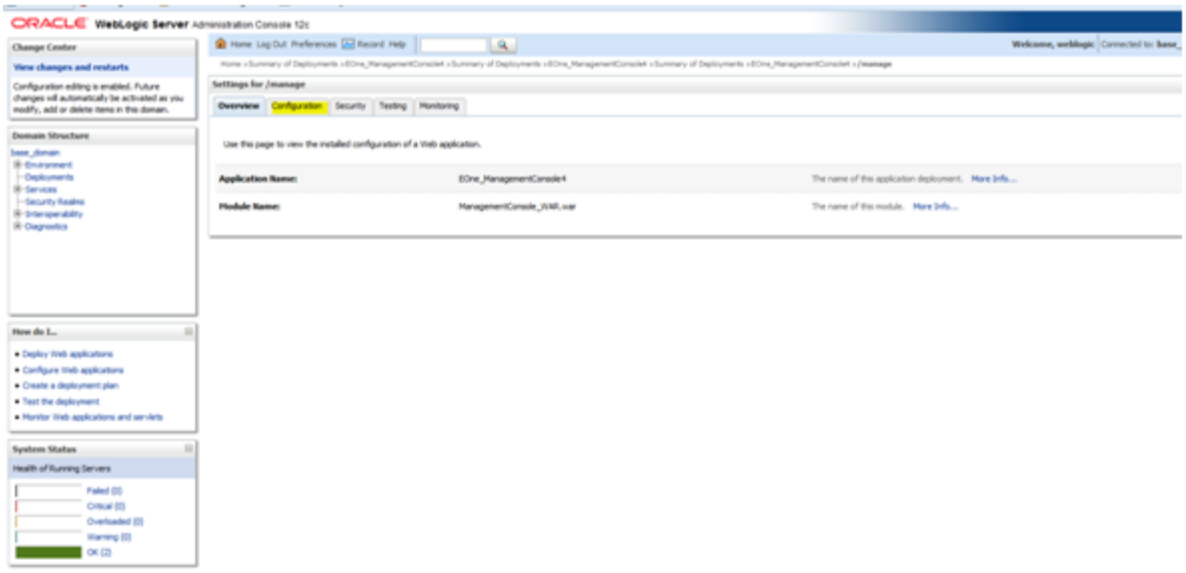
4. Select the SM console deployment in the **Deployments** section.



5. In the **Overview** tab choose the **/manage** module.



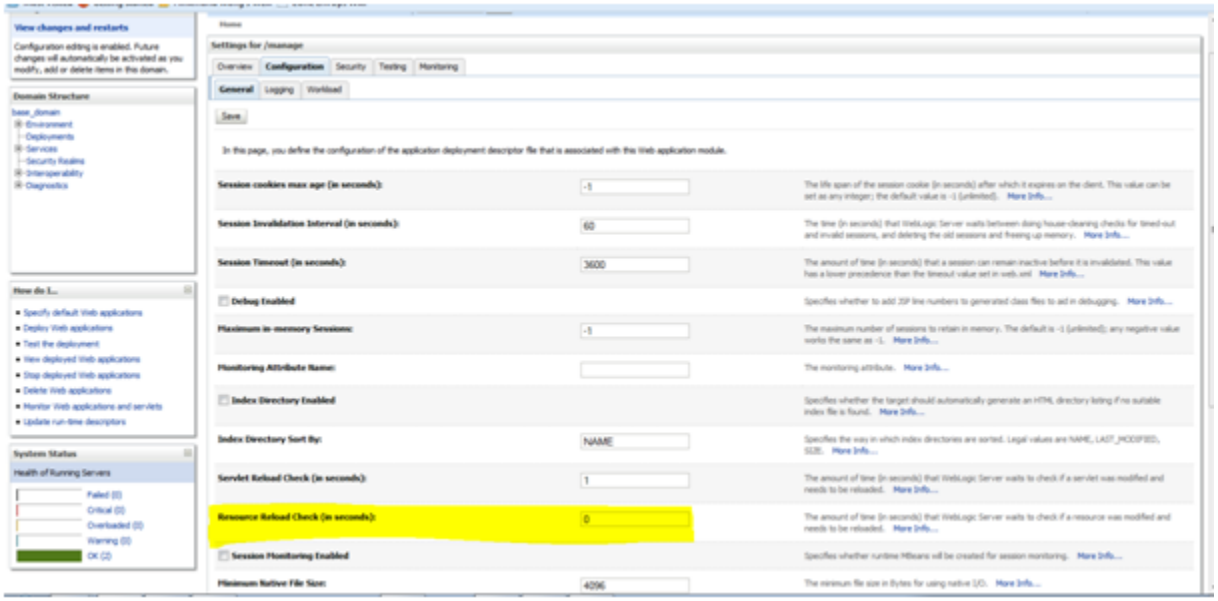
6. Click on the **Configuration** tab.



7. On the **configuration tab**, if the value of **Resource Reload Check (in seconds):** is **-1**, then change it to **0**.

   These are the available values:

   - The value **-1** means never reload. This is the default value in a production environment.
   - The value **0** means always reload.
   - The value **1** means reload every second. This is the default value in a development environment.



8. Click **Save**.
9. Click on **Release configuration** in the left pane, if it's available.

3.7.3 Installing the Management Console on WebSphere Application Server (Tools Release 9.1 Update 2 and Update 3)

Beginning with JD Edwards Tools Release 9.1 Update 2, you can install the Server Manager Console on WebSphere Application Server on Microsoft Windows platforms.

See Also

IBM WebSphere Application Server 7/8.5 Infocenter

`http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp`

`http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp`

This section discusses these topics:

- Section 3.7.3.1, "Starting and Stopping the Server Manager Console on WebSphere on the Microsoft Windows Platform"
- Section 3.7.3.2, "General Hostname/IP Address Configuration Prerequisites"
- Section 3.7.3.3, "Creating a Profile for WebSphere Application Server Release 7.0/8.5"
- Section 3.7.3.4, "Prerequisites for WebSphere Application Server"
- Section 3.7.3.5, "Running the WebSphere Application Server Installer for the Server Manager Console"
- Section 3.7.3.6, "Verifying the Server Manager Console Installation on WebSphere Application Server"
- Section 3.7.3.7, "Enable SSL for Server Manager Console on the WebSphere Application Server"
- Section 3.7.3.8, "Troubleshooting the Server Manager Console Installation on WebSphere Application Server"

3.7.3.1 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, the supported WebSphere version is 8.5.

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:
   - **Installation Directory**

     `C:\IBM\WebSphere\AppServer`
   - **Profile to which the Server Manager Console is Installed**

     AppSrv01
   - **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
   ```

3.7.3.2 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.

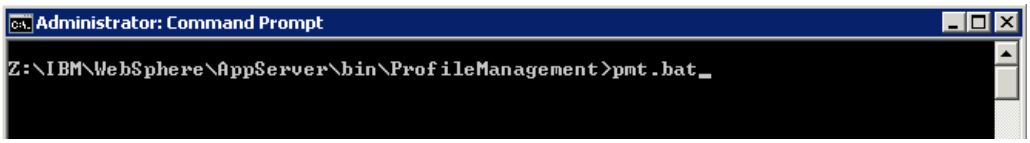
3.7.3.3 Creating a Profile for WebSphere Application Server Release 7.0/8.5

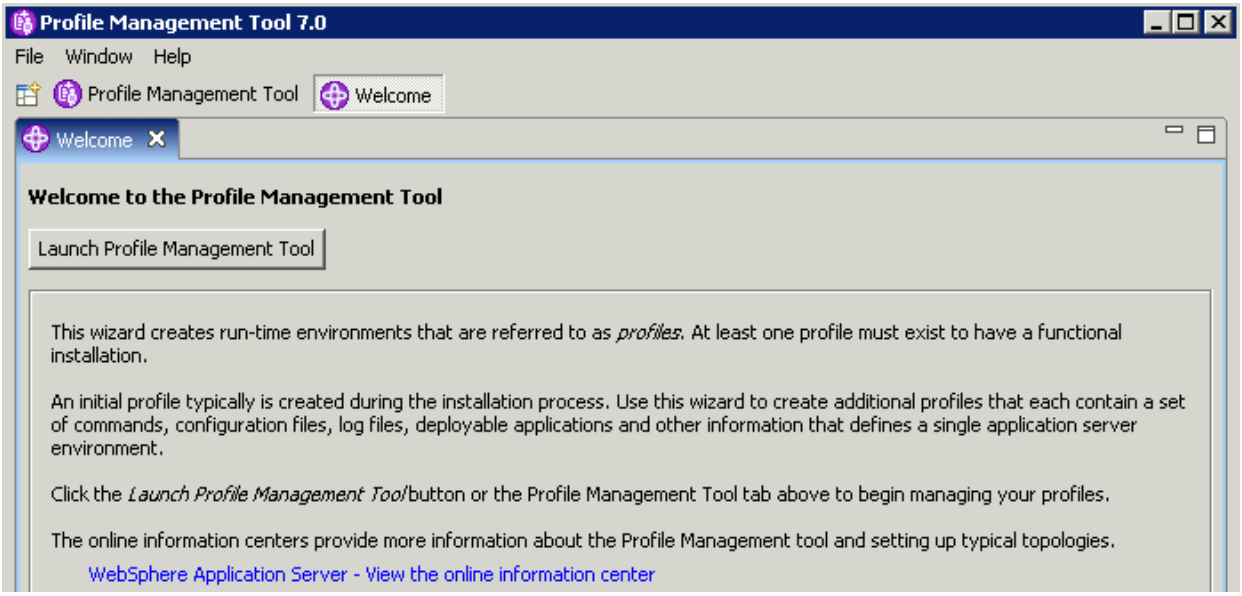
This section is provided for reference only as it relates to recommendations when used in conjunction with JD Edwards EnterpriseOne running on WebSphere Application Servers. For complete details, refer to the IBM documentation on the IBM WebSphere Application Server 7/8.5 Infocenter. The following example is based on WebSphere Application Server 7.0.

To create a profile for WebSphere Application Server Release 7.0/8.5 running on Microsoft Windows:

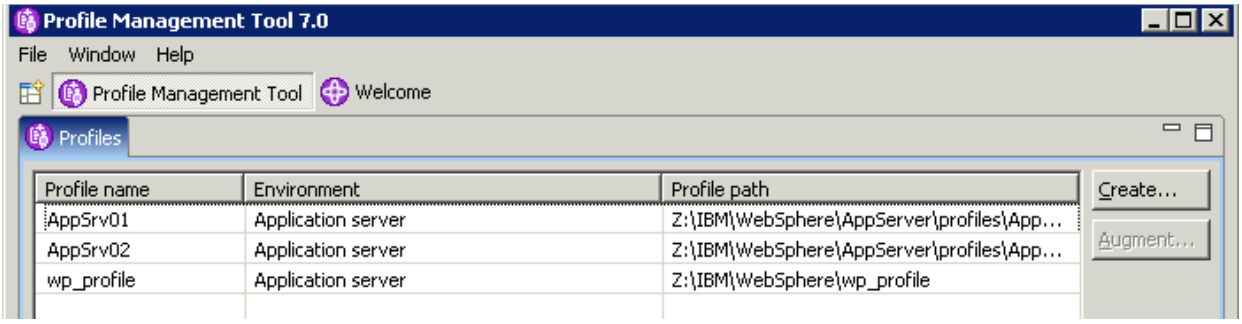
1. Open a Command Window and launch the `pmt.bat` profile management utility, which is typically located in this directory:

   ```
   c:\IBM\WebSphere\AppServer\bin\ProfileManagement
   ```

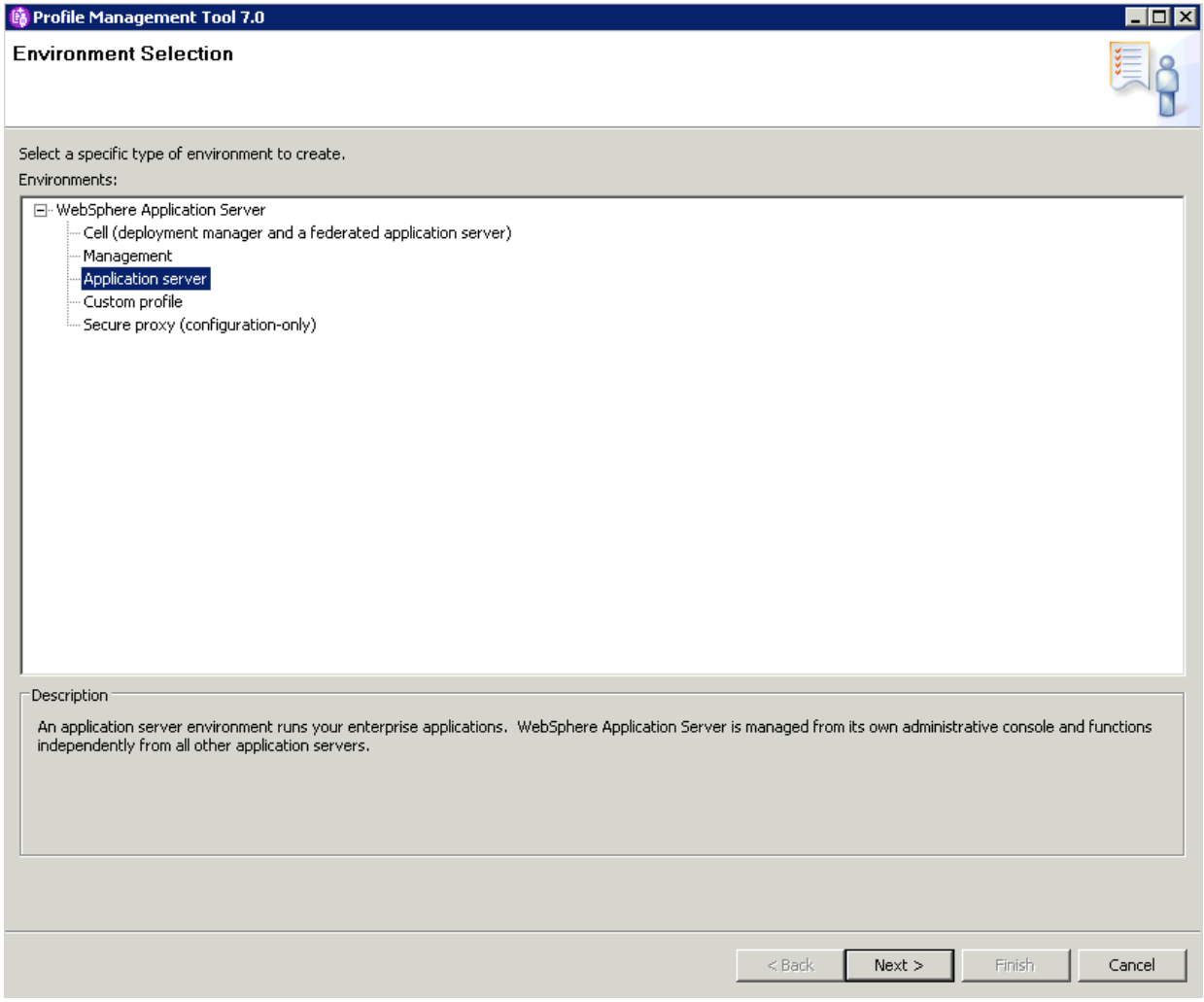




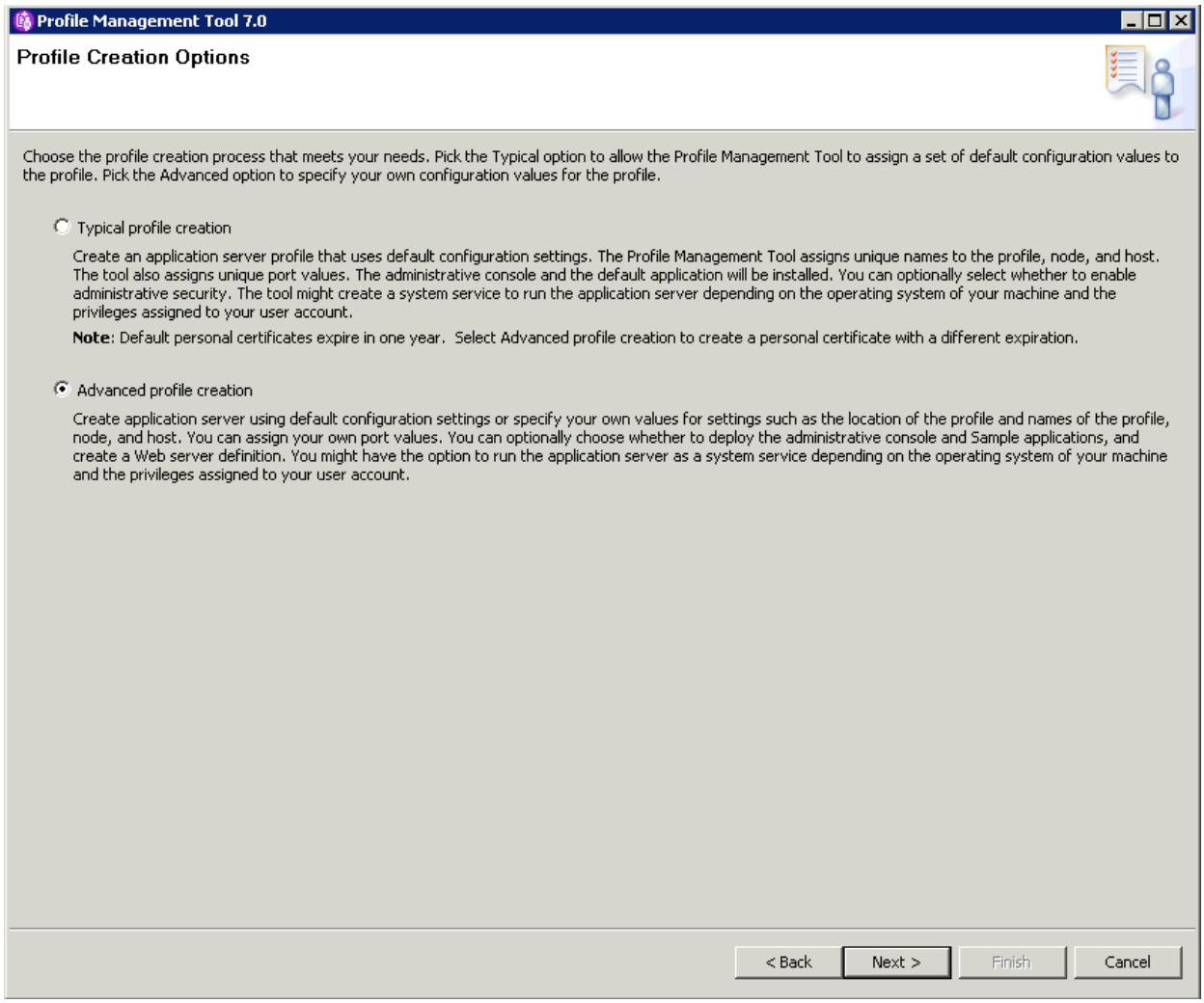
2. On Welcome to the Profile Management Tool, click the **Launch Profile Management Tool** button.



3. With the Profiles tab selected, click the **Create** button.

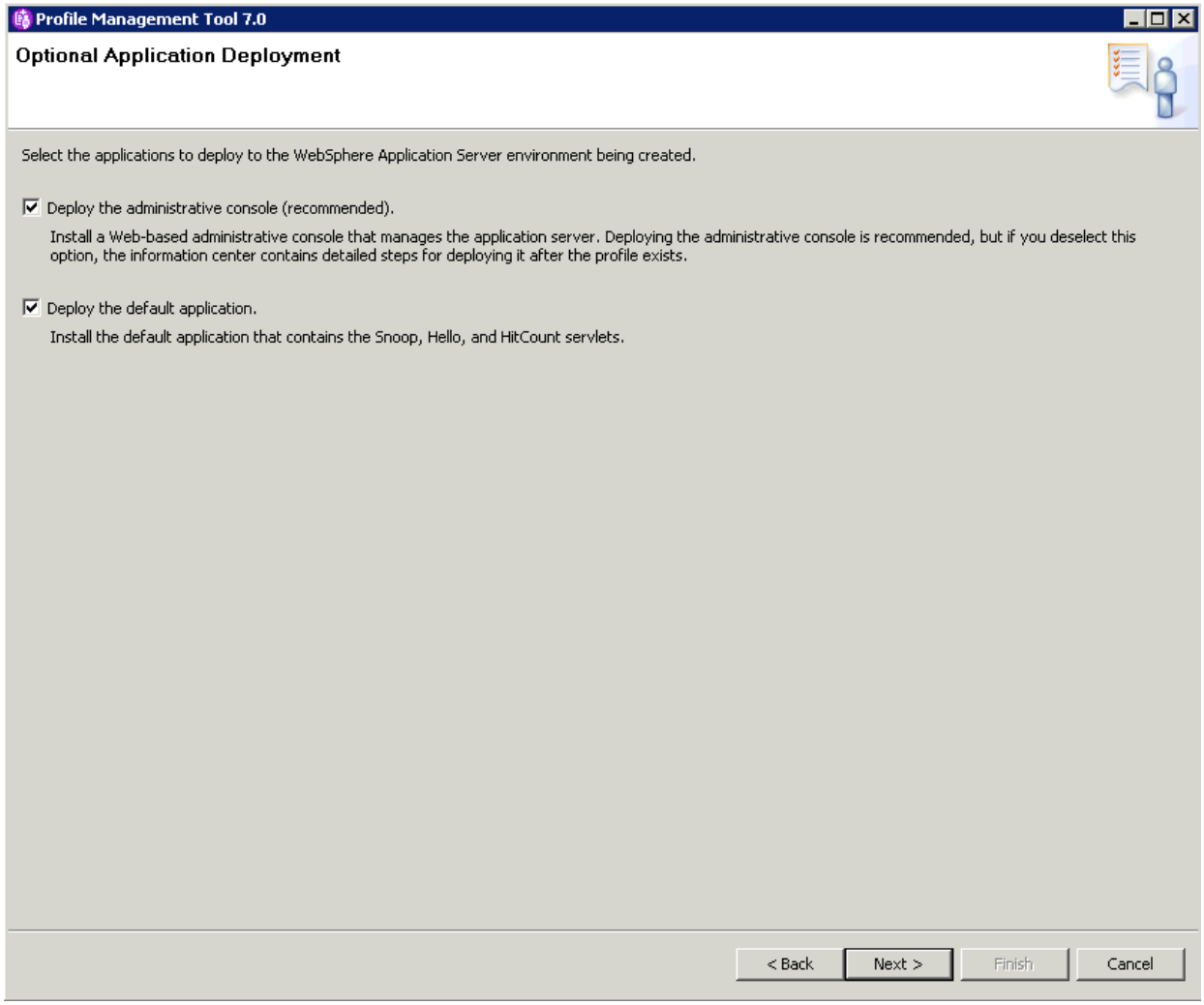


4. On Environment Selection, in the list of Environments, select this tree node:
   - **Application server**
5. Click the **Next** button.

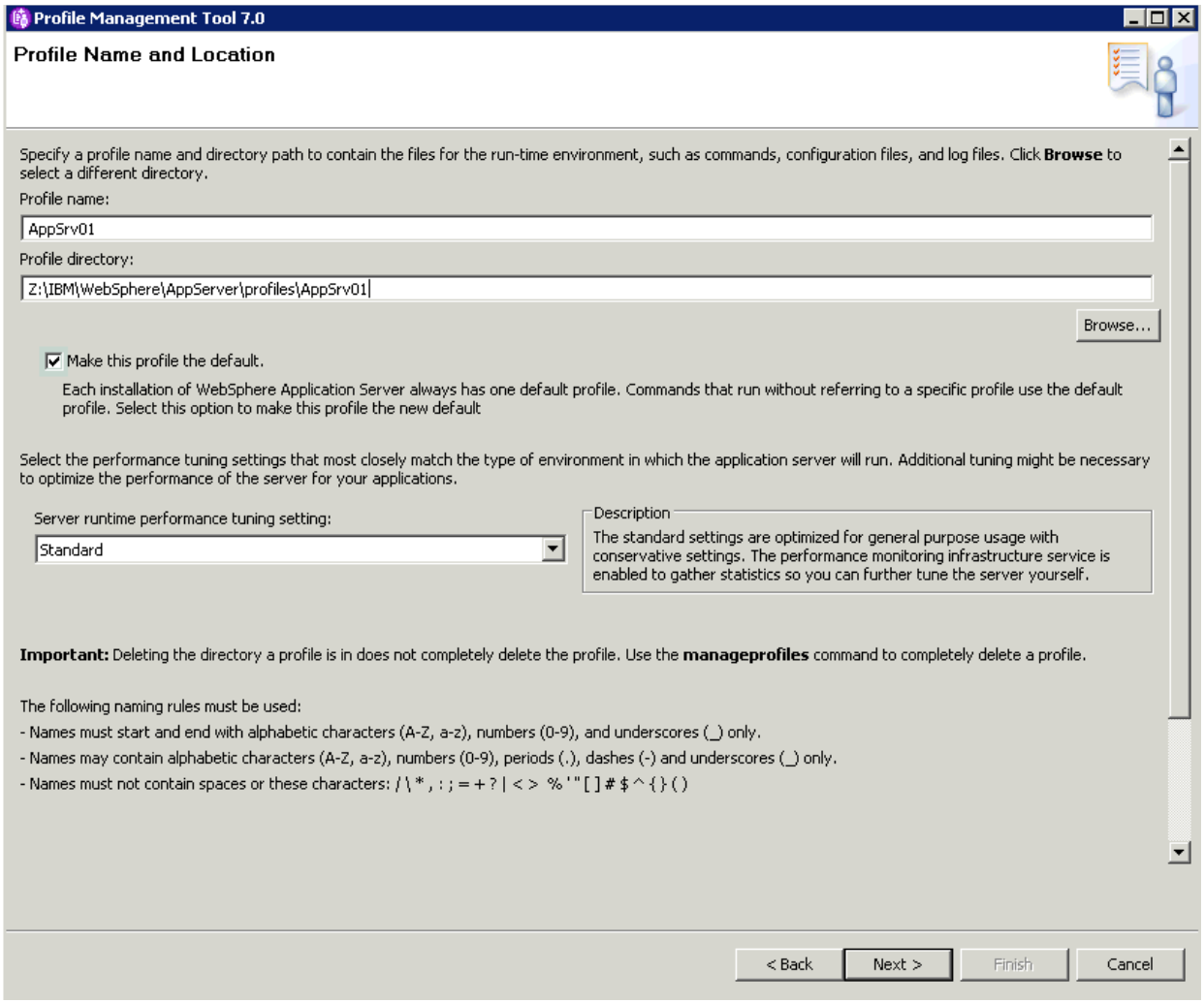


6. On Profile Creation Options, select this radio button:

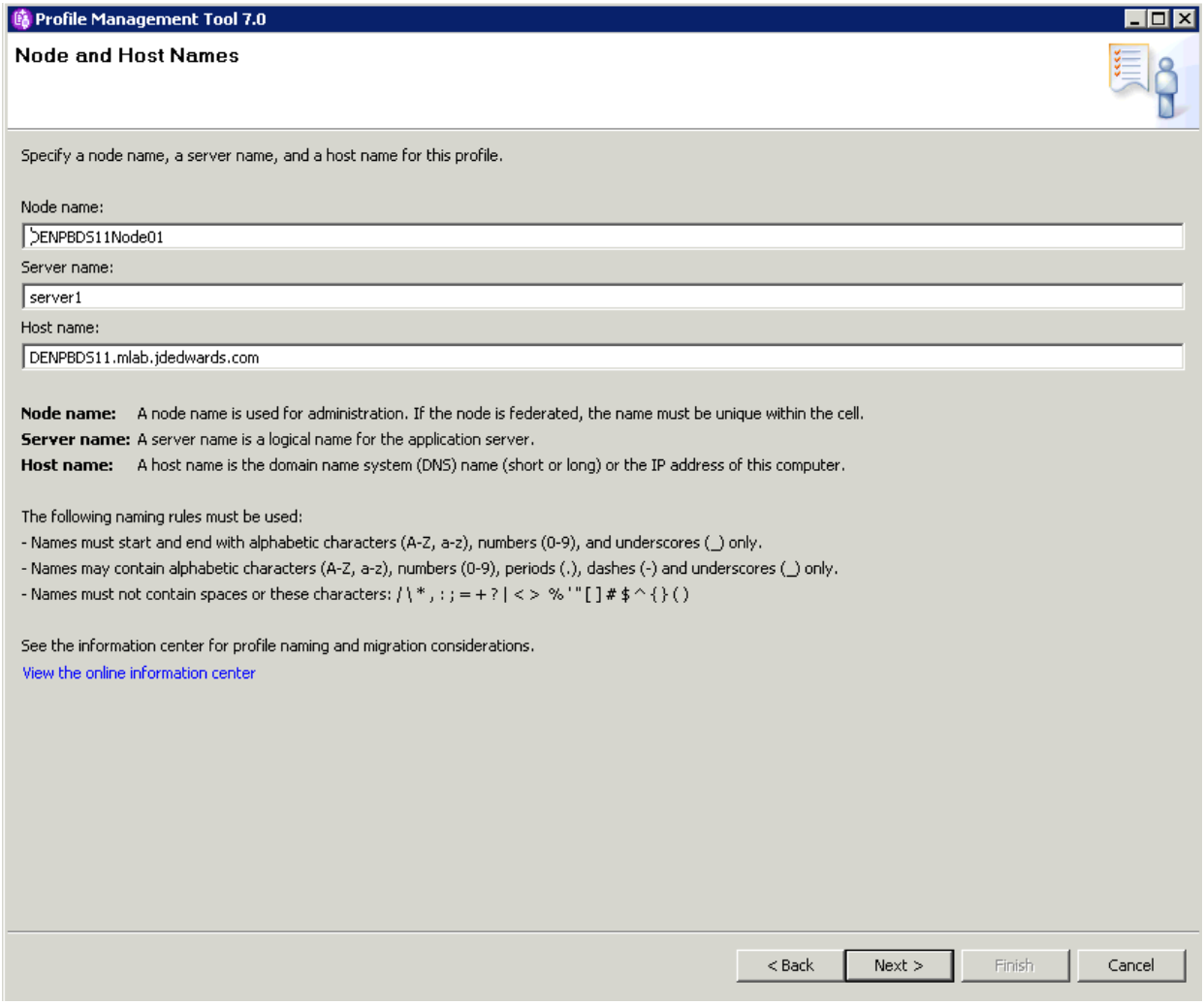
   - **Advanced profile creation**



7. On Optional Application Deployment, select these check boxes:
   - **Deploy the administrative console (recommended).**
   - **Deploy the default application.**
8. Click the **Next** button.



9. On Profile Name and Location, you can accept the default values or enter your own.
10. It is recommended that you enable this check box to make the this new profile to be the default profile:
    - **Make this profile the default**
11. Click the **Next** button.



12. On Node and Host Names, complete these fields:

- *Node name*

  Accept the default or enter your own value.

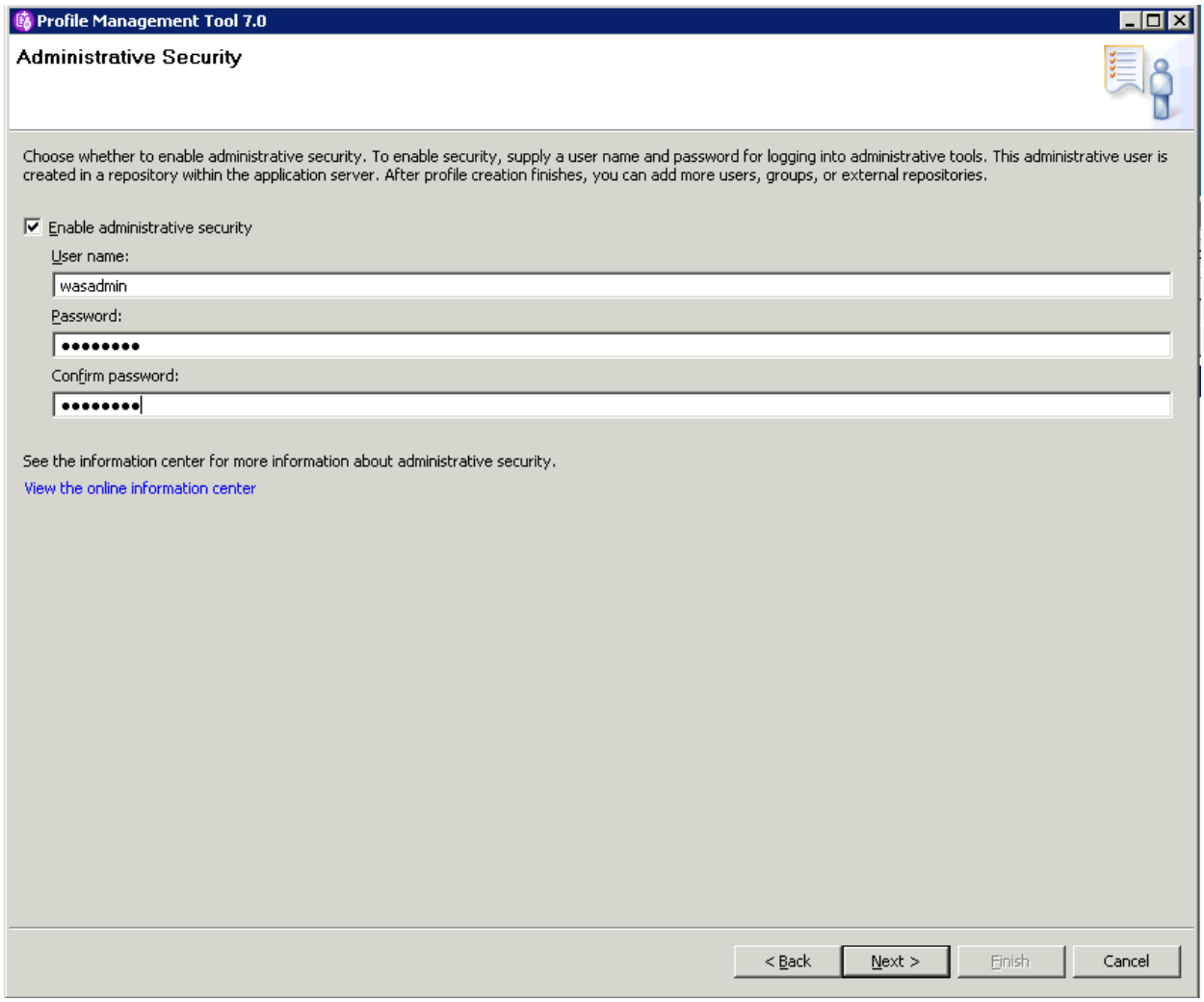
- *Server Name*

  Accept the default or enter your own value.

- *Host name*

  Ensure the correct hostname defaults into this field. This must be the fully qualified domain name of the machine. You cannot use a loopback or localhost.

13. Click the **Next** button.



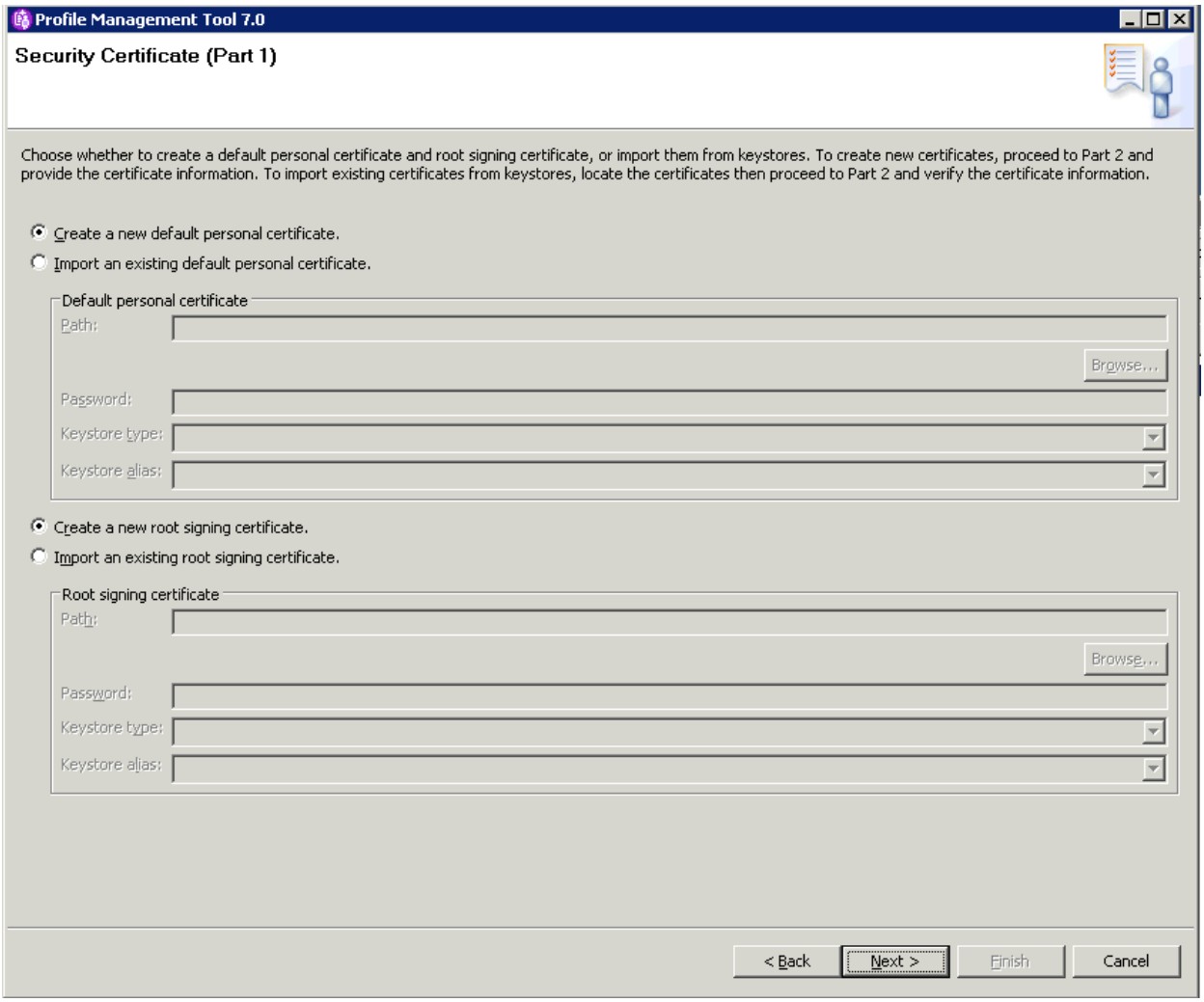
14. On Administrative Security, ensure this check box is selected:

    - **Enable administrative security**

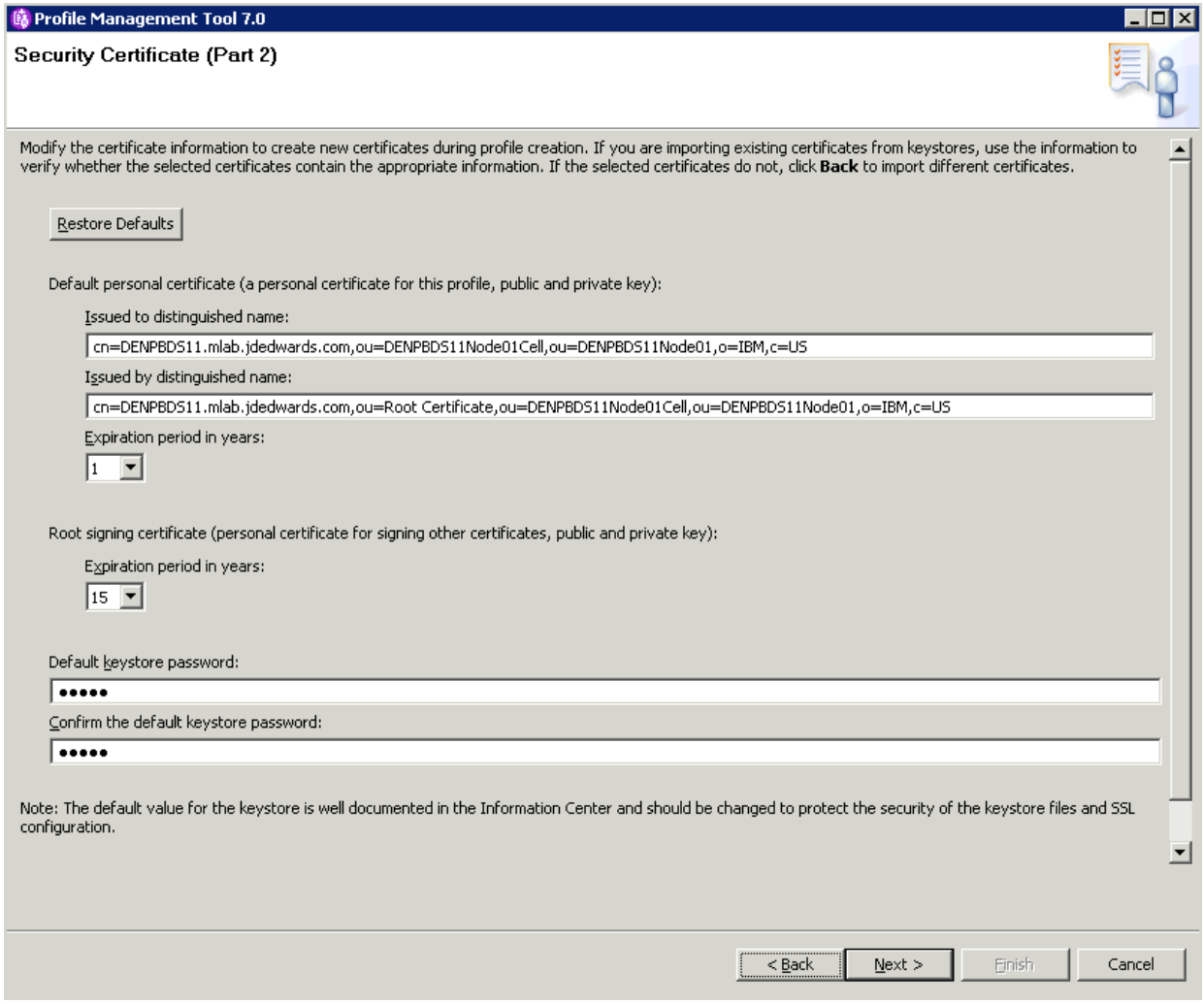
15. You should not accept the default values for these Administrative credentials. Instead you should enter unique credentials for the WebSphere Administrative user for this profile.

    Caution: Be sure and note these credentials as you will need them later in this procedure to populate settings in the `soap.client.props` file.

16. Click the **Next** button.



17. On Security Certificate (Part 1), you can accept the default values, which has these radio buttons selected:
    - **Create a new default personal certificate.**
    - **Create a new root signing certificate.**
18. Click the **Next** button.



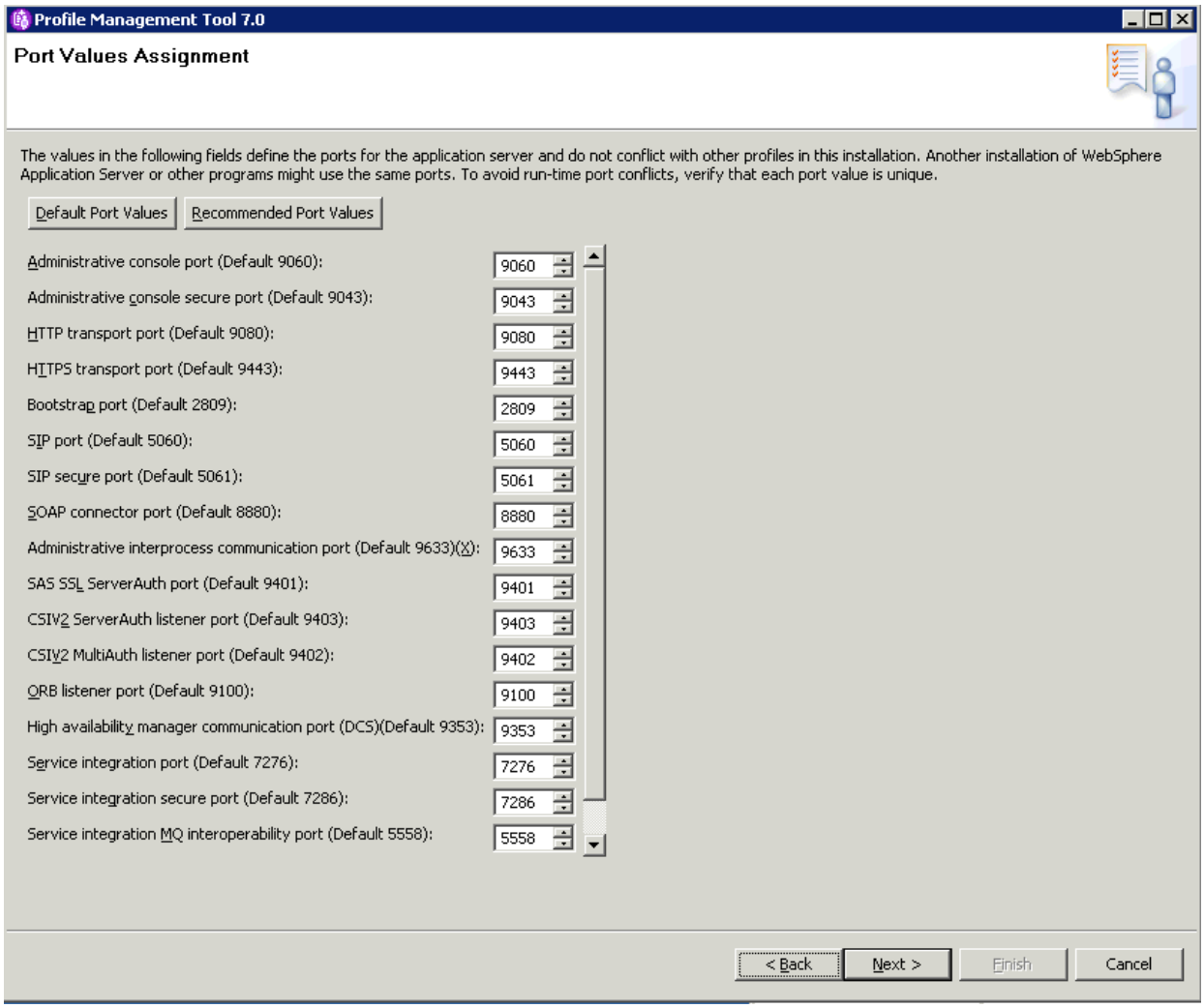
19. On Security Certificate (Part 2), you can accept the default values for these fields or configure them for your installation:

- Default personal certificate (a personal certificate for this profile, public and private key):
  - Issued by distinguished name:
  - Issued to distinguished name:
  - Expiration period in years
- Root signing certificate (personal certificate for signing other certificates, public and private key):
  - Expiration period in years:
- Default keystore password
- Confirm the default keystore password

Caution: The default value for the keystore is well documented in the Information Center and should be changed to protect the security of the keystore files and SSL configuration.

---

20. Click the **Next** button.

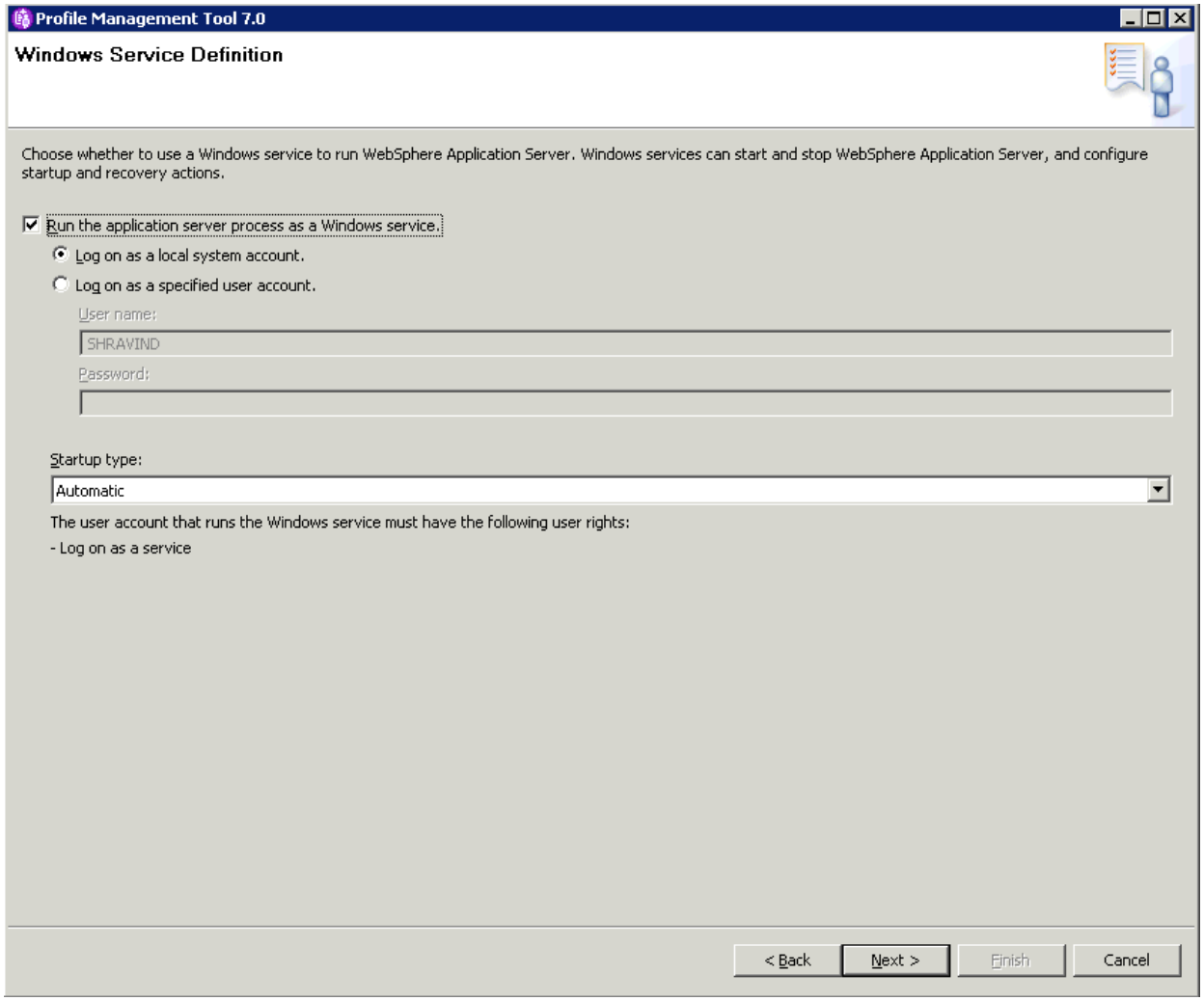


21. On Port Value Assignments, generally you should not change the system-derived port numbers. This is because the WebSphere installer assigns unique port numbers for each profile.

Note: You should note the Administrative console port and the SOAP connector port as you will need these configuration values in order to complete connectivity.

---

22. Click the **Next** button.

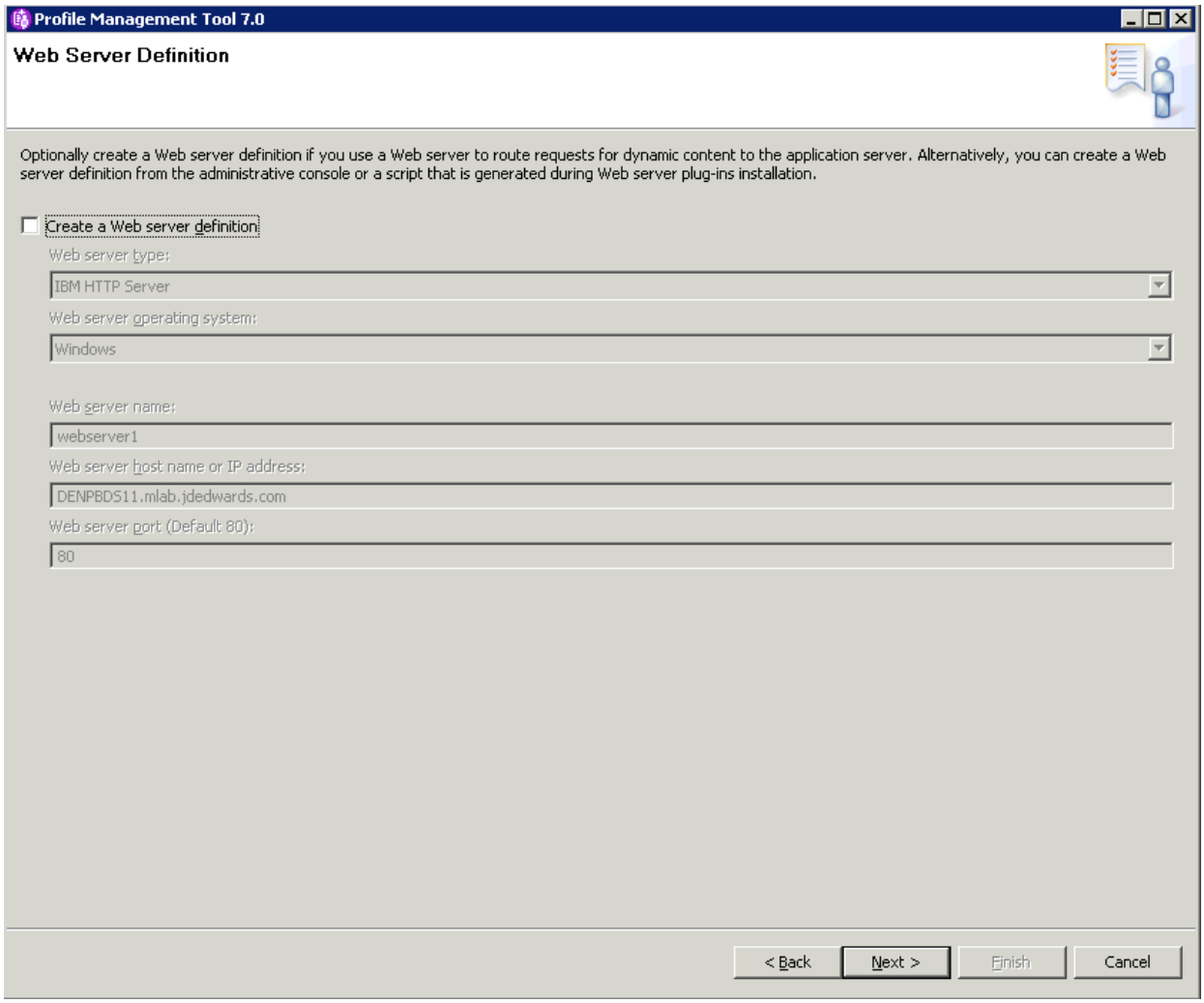


23. On Windows Service Definition, you can choose whether to use a Windows service to run WebSphere Application Server. Windows services can start and stop WebSphere Application Server, and can configure startup and recovery actions. If you want to use a Windows service to run WebSphere Application Server, click this check box:

    - **Run the application server process as a Windows service.**

      If you enable this check box, you can further define the type of account on which to log on as. You can also choose the startup type for the service.

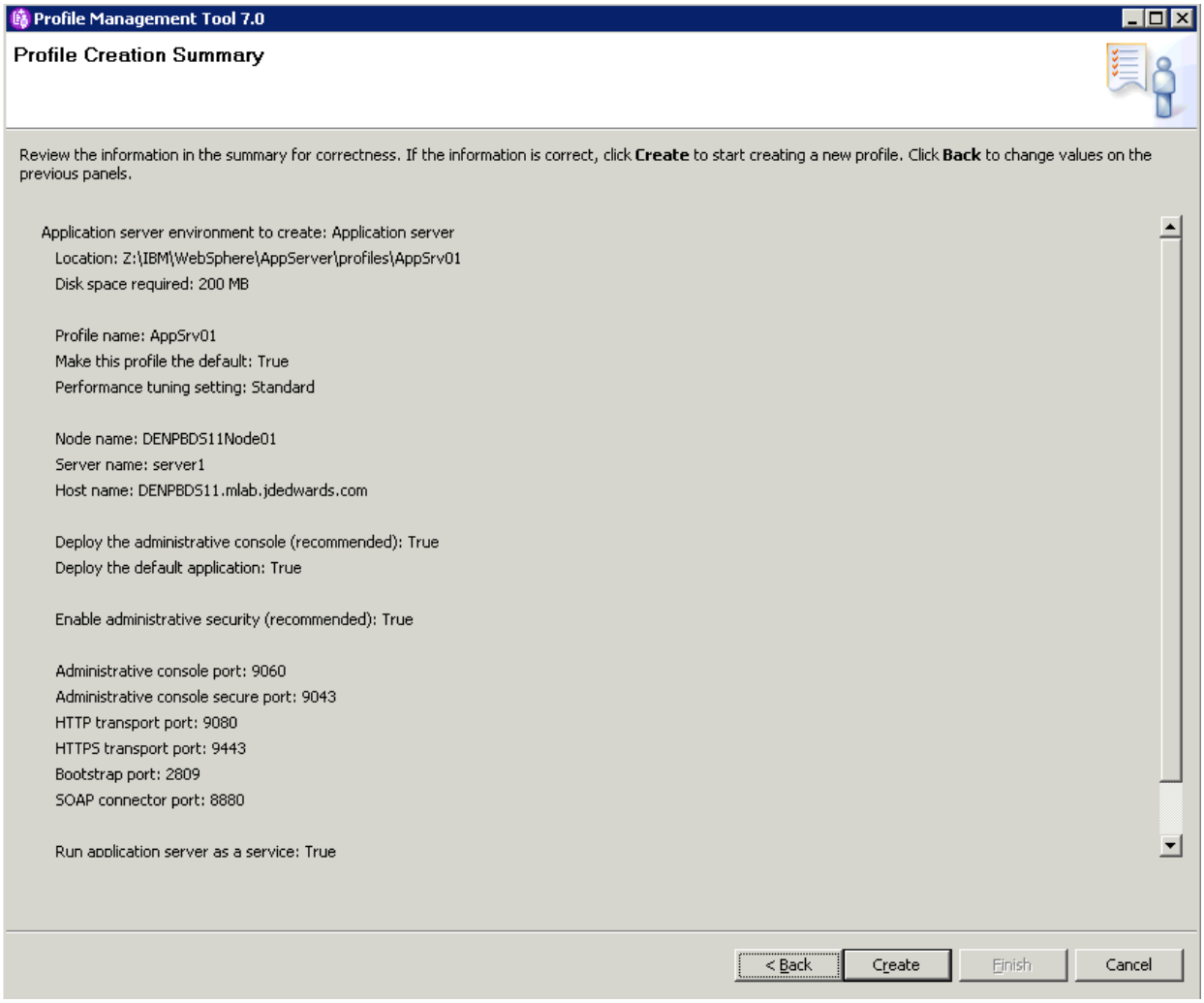
24. Click the **Next** button.



25. On Web Server Definition, optionally you can create a Web server definition if you use a Web Server to route requests for dynamic content to the application server. Alternatively, you can create a Web Server definition from the Administrative console or a script that is generated during Web Server plug-ins installation.

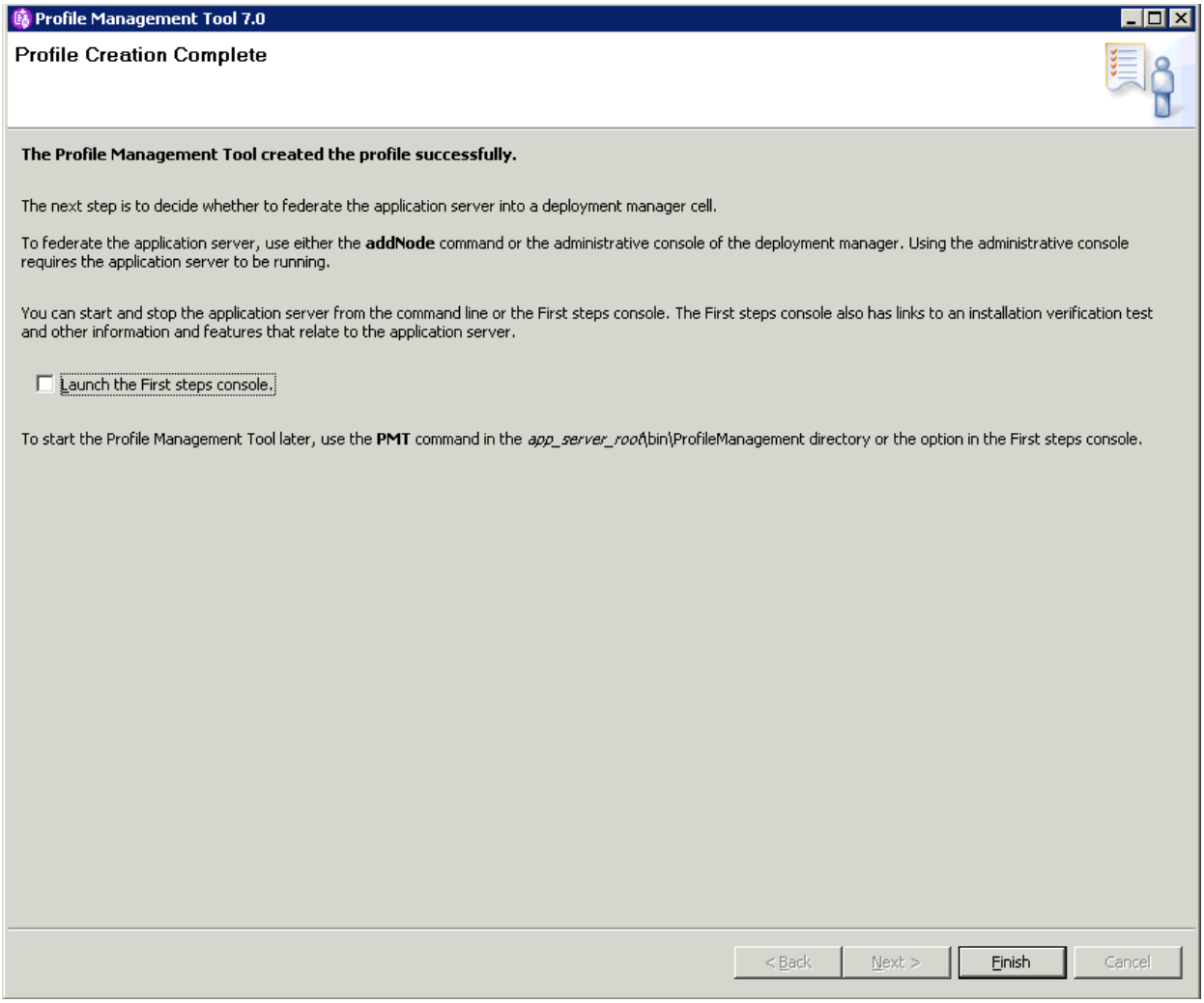
> **Tip:** For JD Edwards EnterpriseOne, it is not required to create a web server definition for the profile into which Server Manager Console will be installed. However, if you wish to the same profile to install other EnterpriseOne web components (for example, HTML Web Server, Transaction (RTE) Server, Business Services Server (BSSV)), then creating a web server definition is required. In that case, you should select this check box and configure the web server type:
>
> - **Create a Web Server definition**

26. Click the **Next** button.



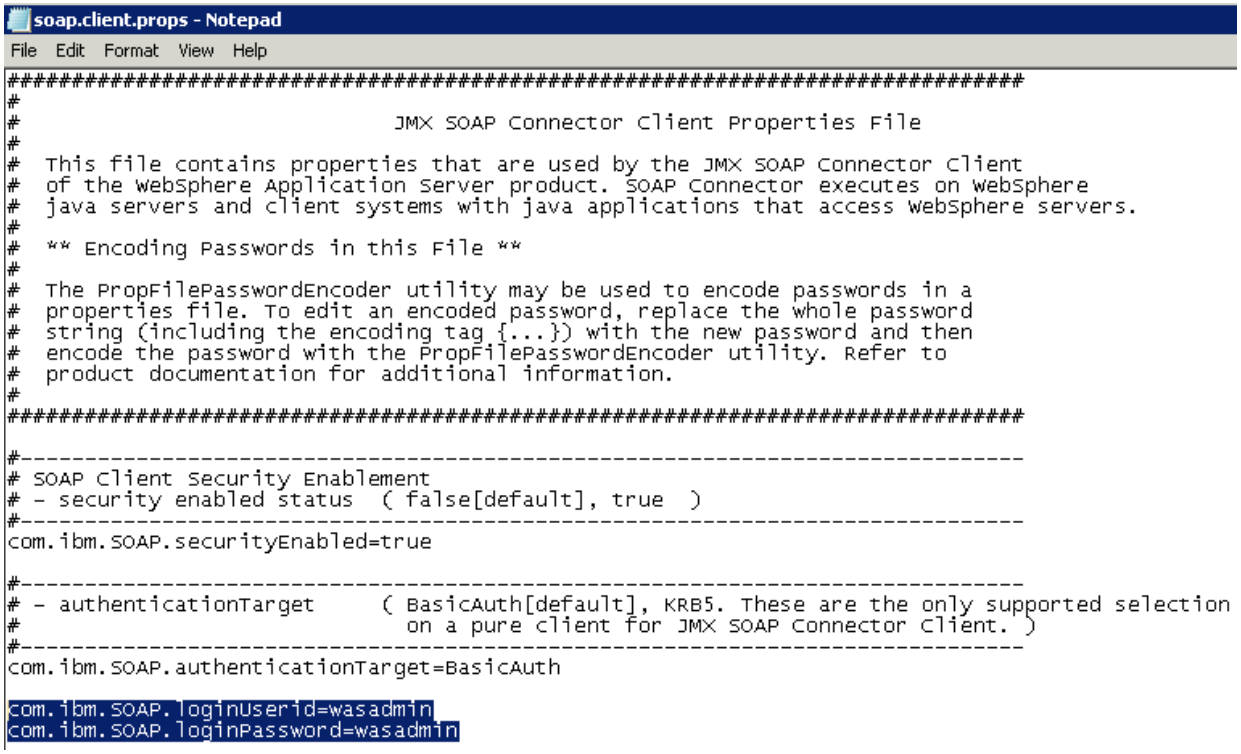
27. On Profile Creation Summary, review the information in the summary for correctness. If the information is correct, click the **Create** button to start creating a new profile. Otherwise, click the **Back** button to change values on the previous panels.

If you clicked the **Create** button, wait for the configuration to complete, which is indicated by the following screen.



28. On Profile Creation Complete, ensure this check box is **not** checked:
    - **Launch the First steps console.**
29. Click the **Finish** button.
30. Exit the Profile Creation Tool; this completes the profile creation procedure.
31. Locate the `soap.client.props` file in the `\properties` directory. For example :

    `z:\IBM\WebSphere\AppServer\profiles\AppSvr01\properties`
32. Using Notepad, open the `soap.client.props` file and update the Administrative userid and password from the default values to the Administrative userid and password with the information provided during the profile creation time. Within the `soap.client.props` file, these values are specified as shown by the highlighted segment in the example below.



33. Change the value of the `com.ibm.SOAP.securityEnabled=` setting from the default value of false to true as shown in this example:

```
#-----------------------------------------------------------------------------
# SOAP Client Security Enablement
# - security enabled status  ( false[default], true  )
#-----------------------------------------------------------------------------
com.ibm.SOAP.securityEnabled=true
```

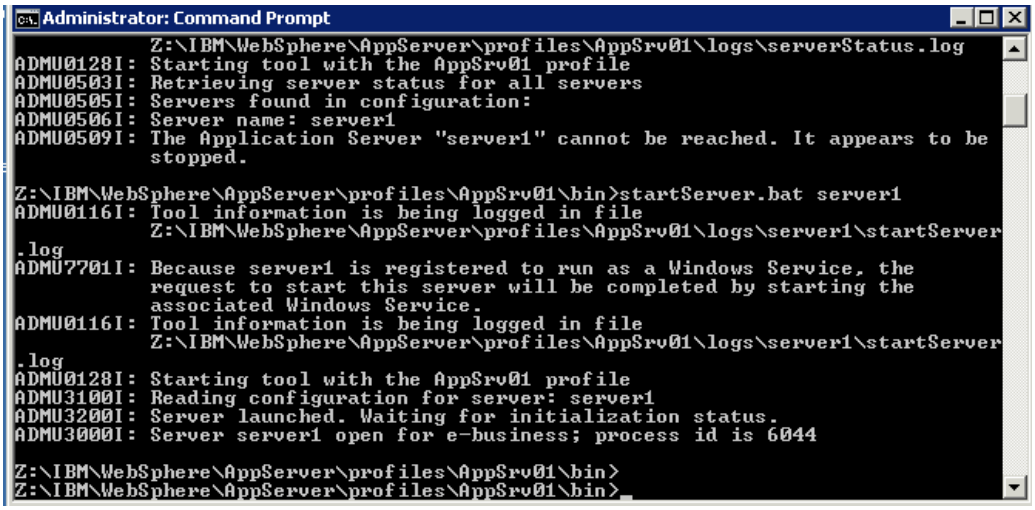
34. It is recommended that you change the value of the `com.ibm.SOAP.requestTimeout=` setting from the default value of 180 to 300.

35. Save the changes to the `soap.clien.props` file and close the Notepad utility.

36. Open an Administrative Command Prompt Window and start the Administrative server of the newly created profile using this utility:

    `startServer.bat`

    The following shows an example of a properly executed `startServer.bat` command.



37. Access Administrative Console using this URL:

`<machine_name>:<port>/ibm/console/login.jsp`

For example:

`denlab.mlab.jdedwards.com/ibm/console/login.jsp`

38. After you log in to the Administrative Console, you have completed the profile creation step.

3.7.3.4 Prerequisites for WebSphere Application Server

The prerequisites depend on your profile type:

- Section 3.7.3.4.1, "Standalone Profile"
- Section 3.7.3.4.2, "DMGR Profile"

Important: There is no special requirement to install the Server Manager Console into a separate WebSphere Server profile; an existing profile can be used.

A single WebSphere Server profile can run both the JD Edwards EnterpriseOne BSSV Instance/Server and the Server Manager Console.

The WebSphere profile onto which the Server Manager Console is installed should be the default profile for the WebSphere setup. If you are installing the Server Manager Console to a new profile, the profile should be created as the default profile prior to installation. For further information refer to Bug 14487301, which is entitled: GRAPHS ARE NOT SHOW FOR THE ENTERPRISE SERVER IN SM INSTALLED ON WAS.

3.7.3.4.1 Standalone Profile Ensure the following prerequisites are met prior to running the Server Manager Console installer into a Standalone profile.

- A Standalone WebSphere Profile with administrative security enabled must be available, where admin security is enabled during profile creation time. An unsecure WebSphere Profile (defined as a profile on which the Administrative Security is not enabled) is **not** supported.
- The admin server for the profile (for example, the **server1** server) must be running and accessible.
- The `soap.client.props` file within the `$PROFILE_DIR\properties` directory should have SOAP security enabled and the SOAP connection userid and password to be configured.
- The profile onto which the Server Manager Console is being installation should be the default profile in the WebSphere installation.
- The Administrator performing installation must know the WebSphere admin userid and password because these values are required as input to the installer.
- The user performing installation must know the AppServer installation directory because this value is required as input to the installer. For example:

  `C:\IBM\WebSphere\AppServer`
- The user performing the installation must know the Hostname as configured during WebSphere Profile creation time because this value is required as input to the installer. You can obtain value by checking the Hostname entry in this file:

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

  For example, a valid value might be:

  `Host Name: shravind-idc.peoplesoft.com`
- The user performing installation must know the SOAP connector port for the WebSphere profile into which the Server Manager Console will be installed because this value is required as input to the installer. This value can be located in the `AboutThisProfile.txt` file. For example:

  `SOAP connector port: 8880`
- In the `soap.client.props` file for the WebSphere profile, which is typically located at this location:

  `C:\IBM\WebSphere\AppServer\profiles\<Profile_Name>\properties\soap.client.props`

  verify the following entries are present and set correctly:

  `com.ibm.SOAP.securityEnabled=true` (the default value is false)

  `com.ibm.SOAP.loginUserid=<admin userid>`

  `com.ibm.SOAP.loginPassword=<admin password>`

Note: Prior to running the installer for the Server Manager Console, you must restart the Admin Server (for example, **server1**) after you have made any changes to the `soap.client.props` file.

3.7.3.4.2 DMGR Profile Ensure the following prerequisites are met prior to running the Server Manager Console installer into a DMGR profile.

- The user performing installation must know the AppServer installation directory because this value is required as input to the installer. For example:

  `C:\IBM\WebSphere\AppServer`

- The DMGR + Cell Profile must have administrative security enabled.

- In the `soap.client.props` file for the WebSphere profile, which is typically located at this location:

  `C:\IBM\WebSphere\AppServer\profiles\Dmgr01\properties\soap.client.props`

  verify the following entries are present and set correctly:

  `com.ibm.SOAP.securityEnabled=true` (the default value is false)

  `com.ibm.SOAP.loginUserid=<admin userid>`

  `com.ibm.SOAP.loginPassword=<admin password>`

  Note: Prior to running the installer for the Server Manager Console, you must restart the Admin Server (for example, the deployment manager server and the node agents) after you have made any changes to the `soap.client.props` file.

  Similarly the `soap.client.props` file of the Federated Profile must have the above entries present and set correctly.

- The DMGR Server must be running. You can start the server using this command:

  `C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\startManager.bat`

- The nodeAgent associated with the Federated Profile (for example, **AppSrv02**) must be running. You can start the agent using this command:

  `C:\IBM\WebSphere\AppServer\profiles\AppSrv02\bin\startNode.bat`

- The Hostname and the SOAP connector port for the DMGR must be known to the administrator performing the installation because this value is required as input to the installer. This information is available by checking the entries for Hostname and SOAP connector port in this file:

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

- The username and password to login into the DMGR must be known to the administrator performing the installation because this value is required as input to the installer.

3.7.3.5 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 as a user with privileges as described in the preceding section of this guide entitled: Section 3.7.3.4, "Prerequisites for WebSphere Application 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: Section 3.6, "Obtain and Extract

the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)".

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 Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)":

```
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.

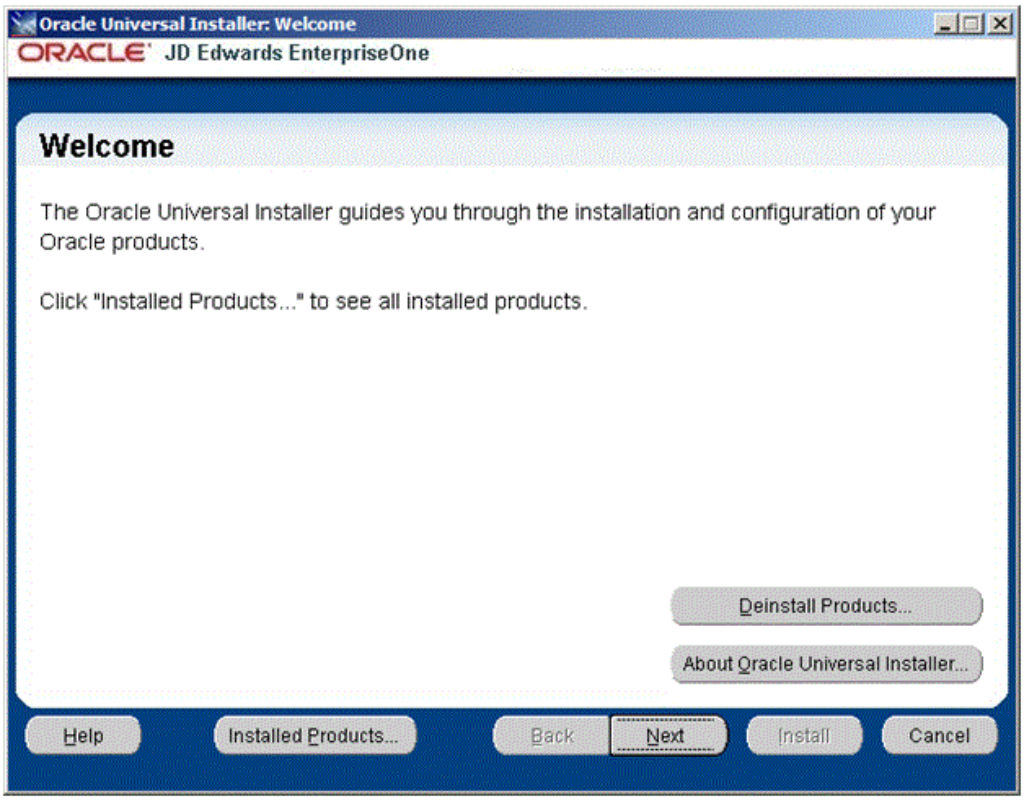
Linux or Solaris

Execute `runInstaller` from the directory in which you unzipped the installer. For example, if you followed the recommendation in Section 3.6, "Obtain and Extract the Server Manager Management Console for JD Edwards EnterpriseOne Tools (Release 9.1 Update 2)":

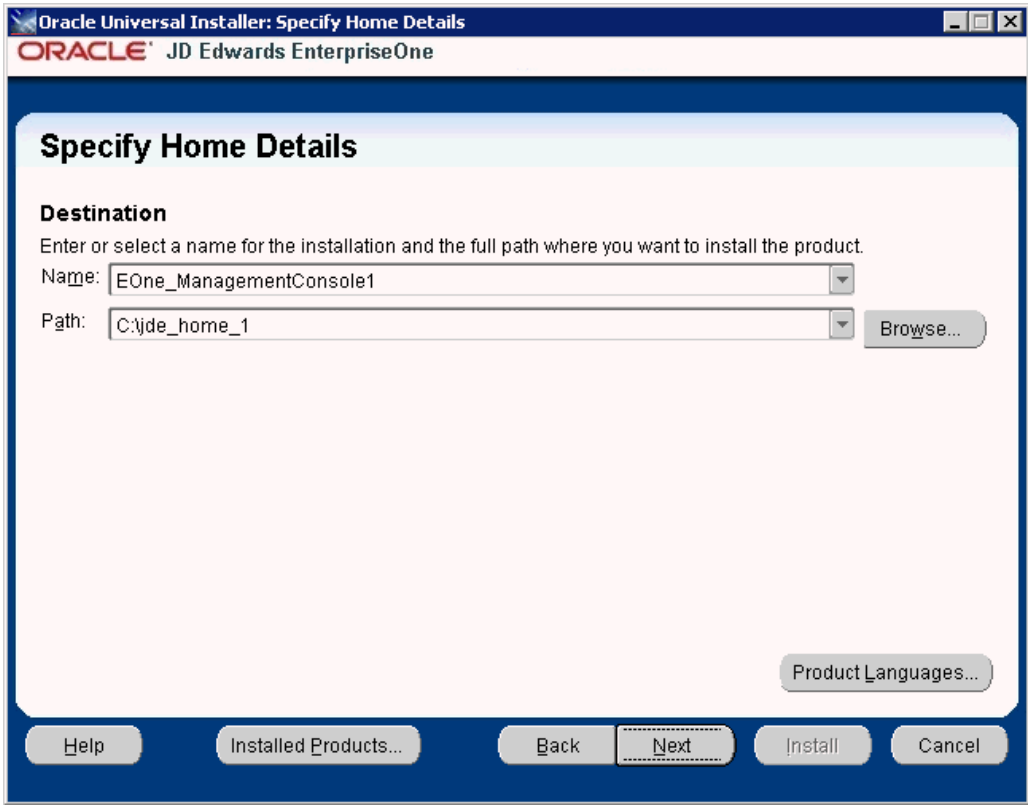
```
./SM_Console/Disk1/install/runInstaller
```

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.



4. On Welcome, click the Next button.



5. On Specify Home Details, complete these fields:

   - *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.

   - *Path*

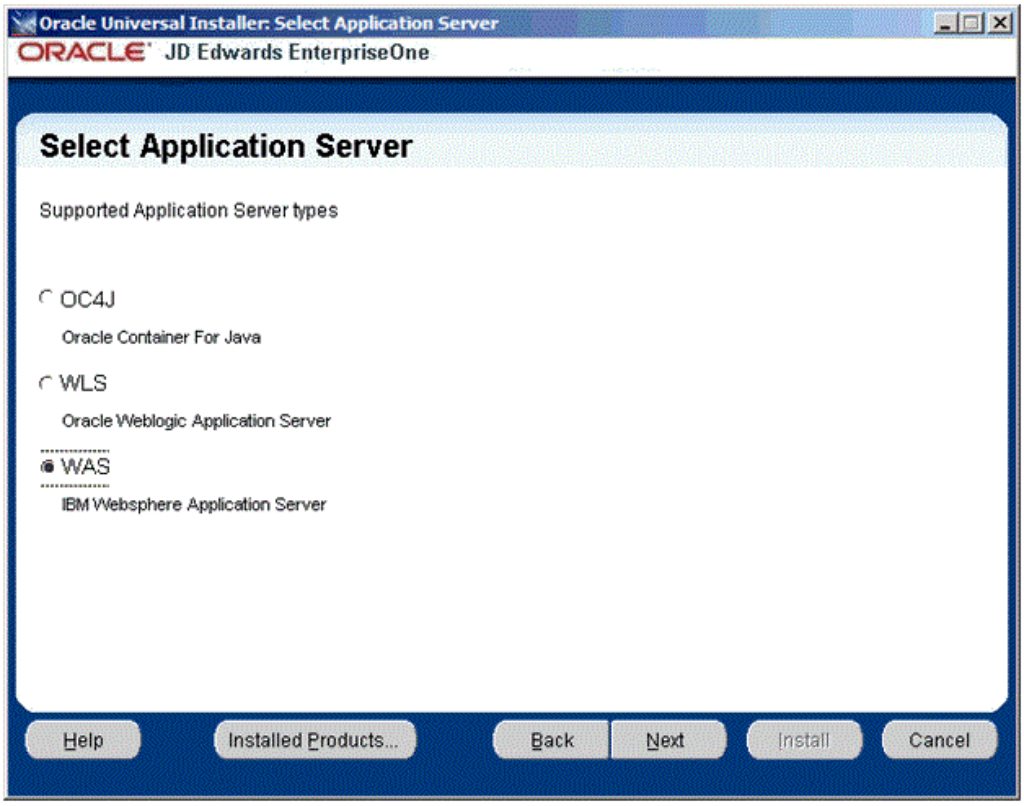
     Enter the drive and directory where you want the files installed on your Management Console. The JD Edwards EnterpriseOne Management Console installer automatically detects the root drive location on the machine and by default appends this value:

     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.

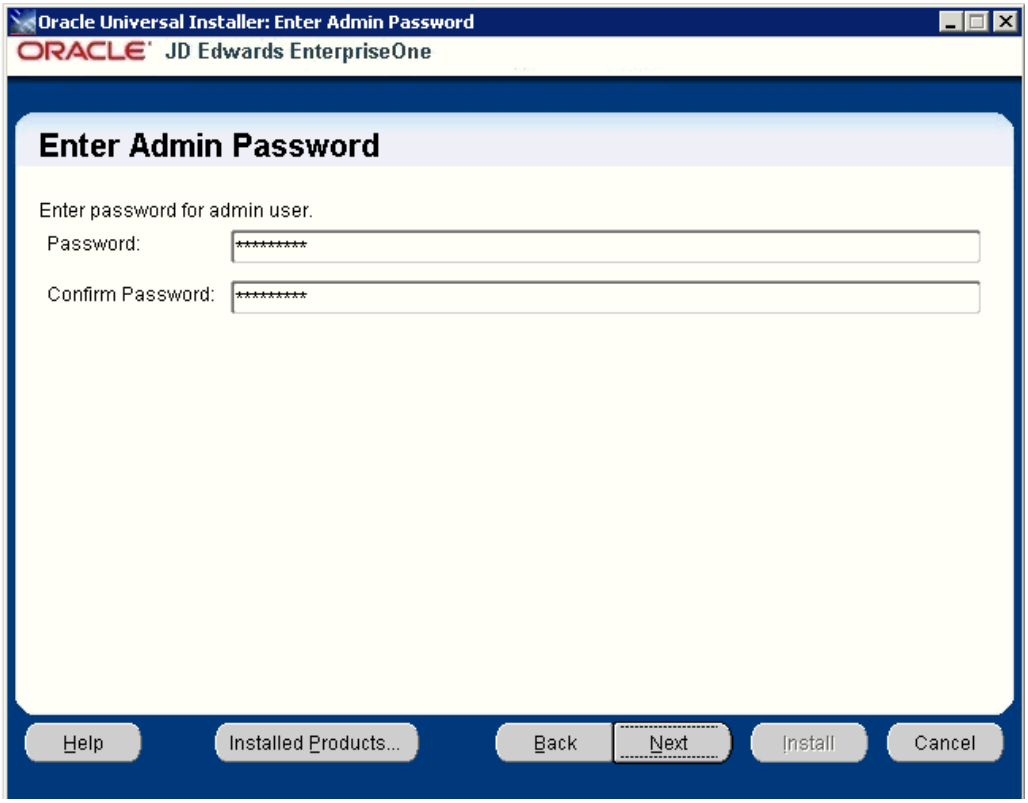


7. On Select Application Server, select this radio button:

   WAS

   WebSphere Application Server

8. Click the Next button.



9. 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: ! @ # $ _

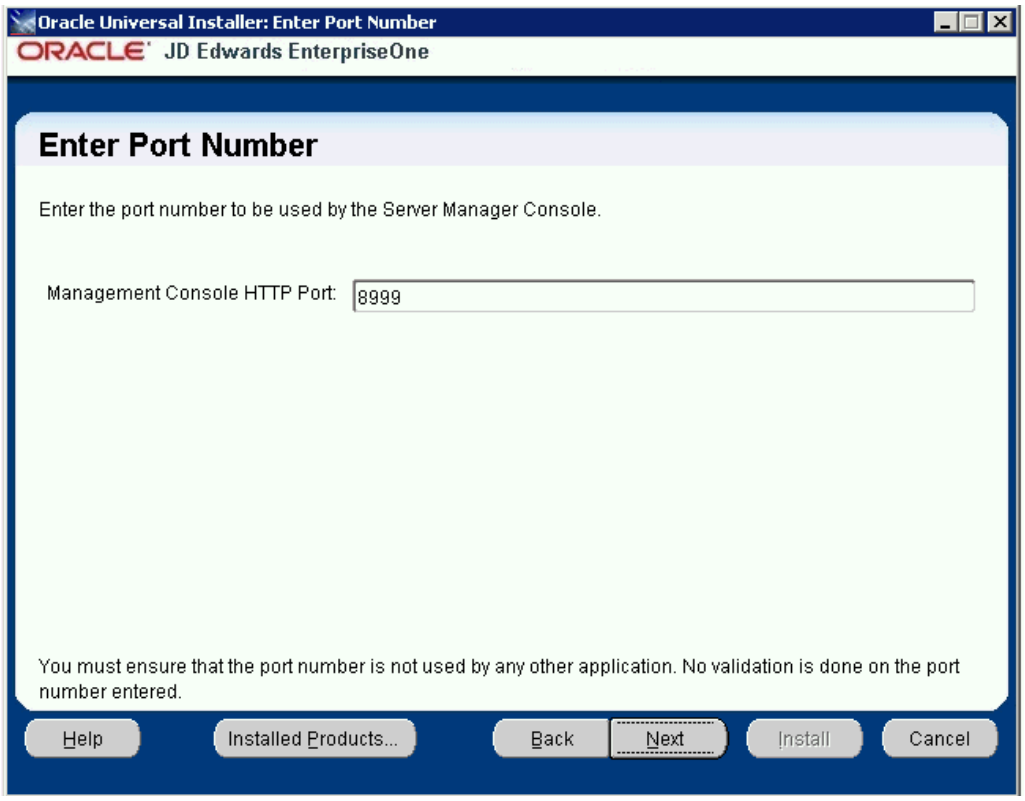
Note: The default value for the user named jde_admin is automatically populated by the Management Console installer and cannot be altered. This is the administrative user account that is associated with the Management Console.

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.

10. Click the Next button.



11. On Enter Port Number, complete this field:

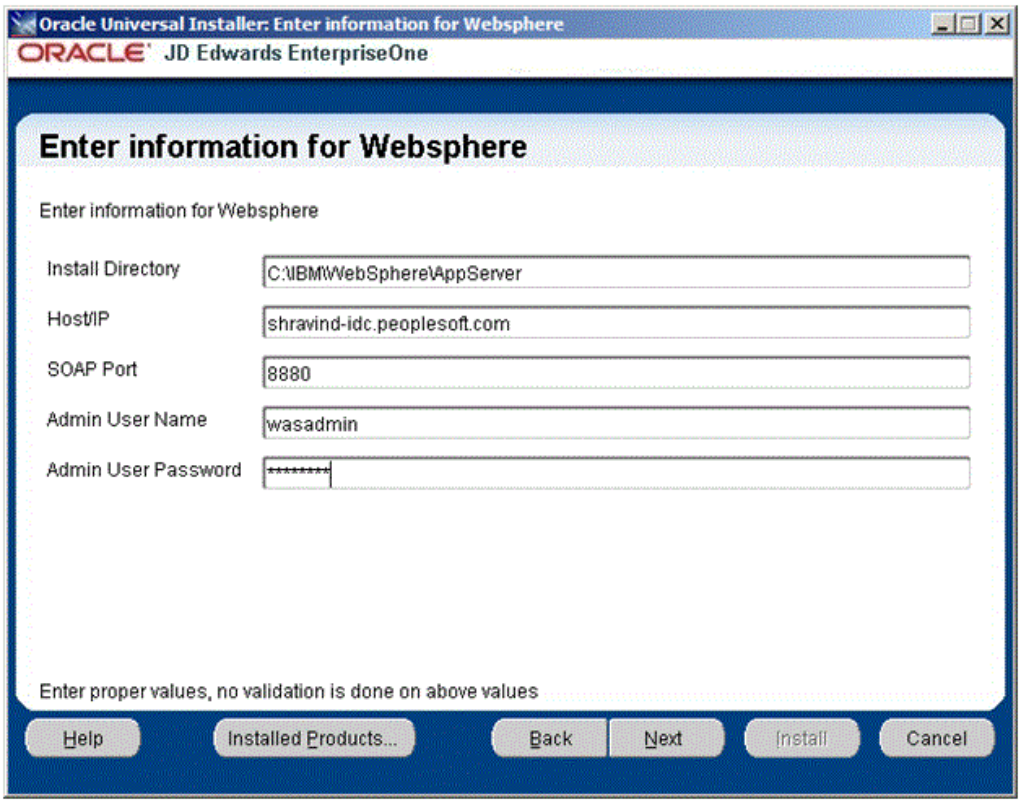
- Management Console HTTP Port

  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.



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

- *Install Directory*

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

  `C:\IBM\WebSphere\AppServer`

- *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:

  shravind-idc.peoplesoft.com

- *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`

- *Admin User Name*

  Enter the user name of the WebSphere admin account.

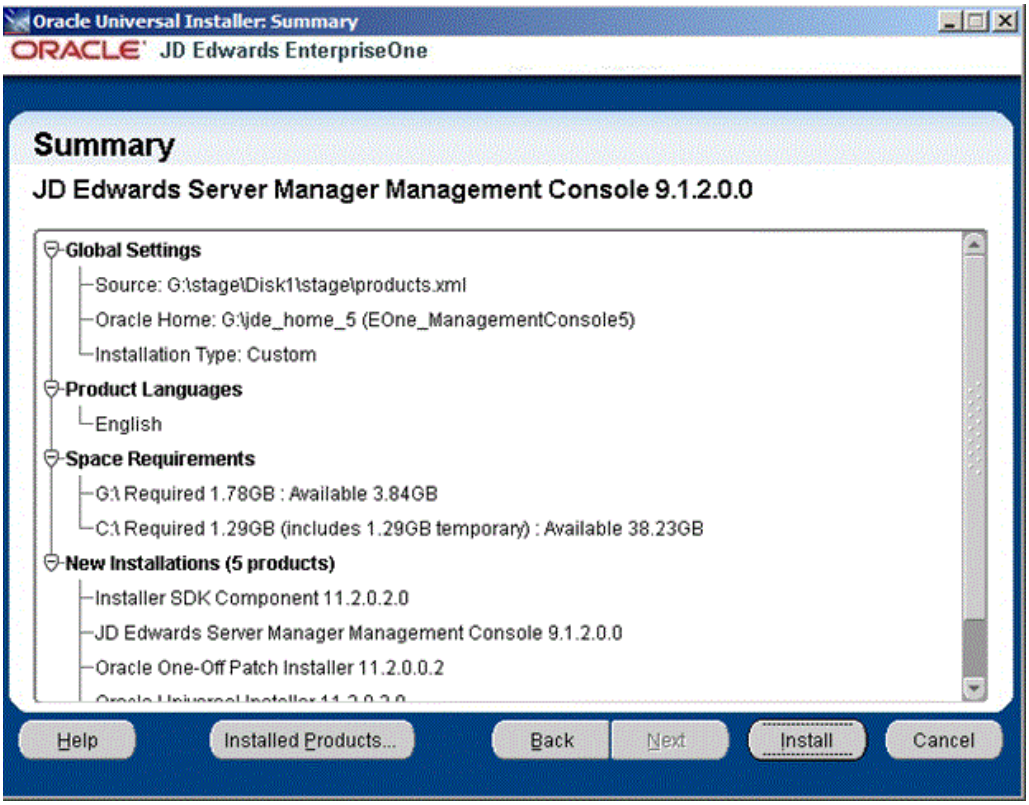
- *Admin User Password*

  Enter the password for the WebSphere admin account.

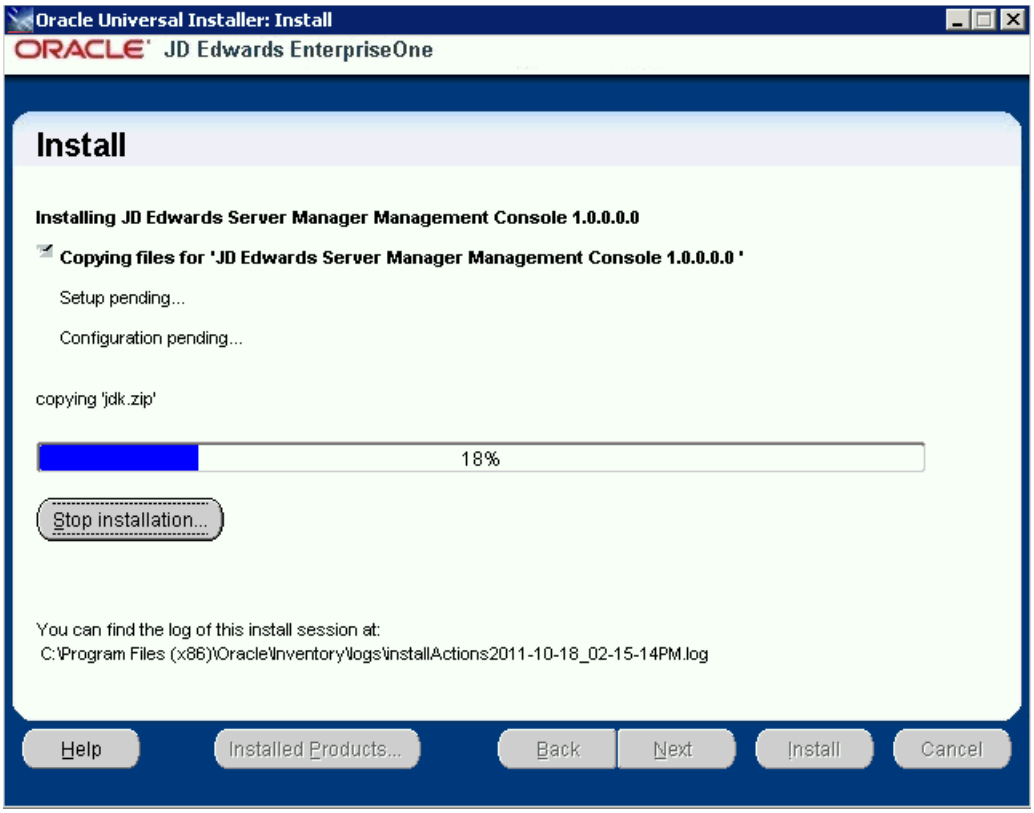
Caution: The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items. If you enter invalid values, you will have to re-run the installer with the correct values.

---

13. Click the Next button.



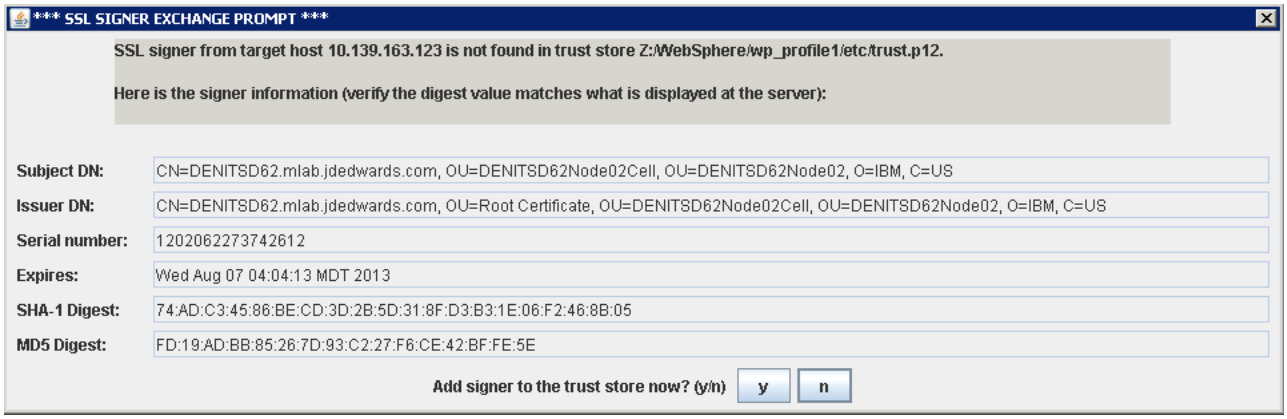
14. On Summary, verify your selections and click the Install button to begin the installation.



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
```

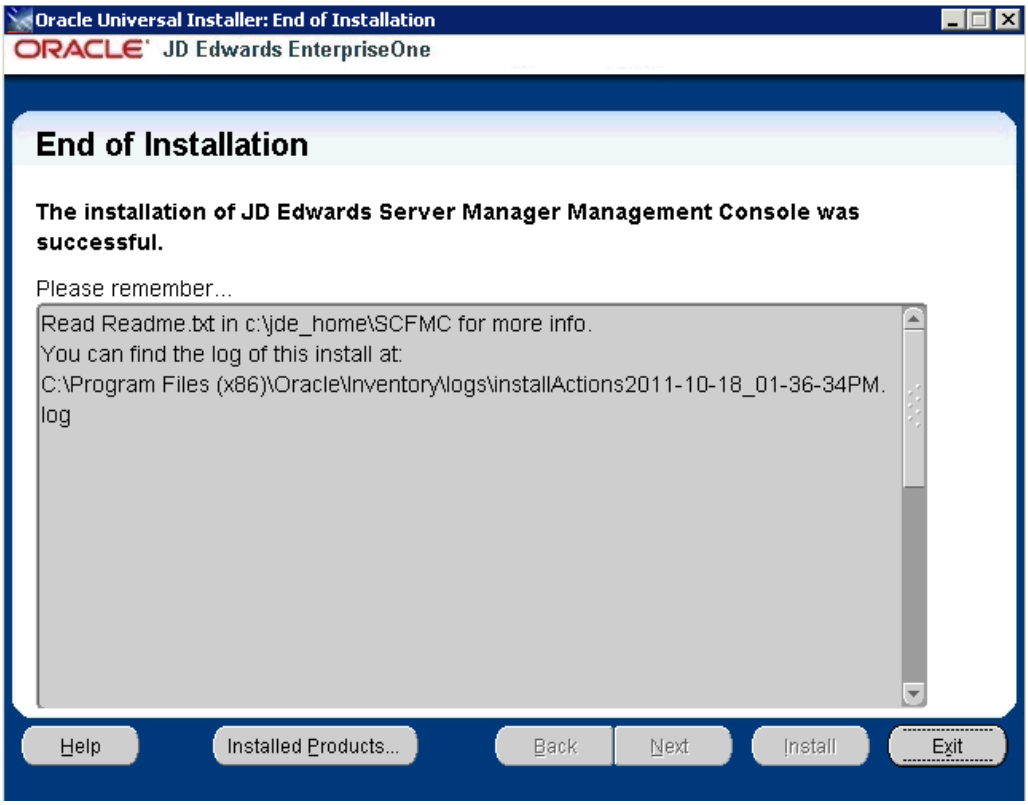
Important for Installations for WebSphere running on Microsoft Windows using the Tools Release 9.1 Update 2 or Update 3 version of the Server Manager Console Installer. When installing the Server Manager Console on WebSphere on a non default profile (that is a profile which is not configured as a default 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:



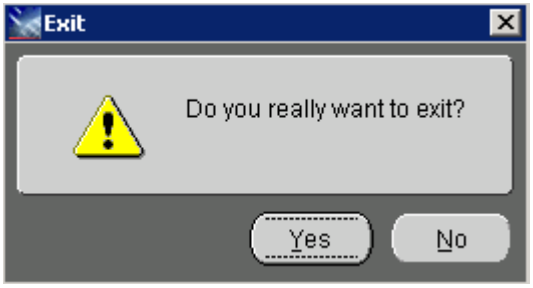
Troubleshooting Installations for WebSphere running on Microsoft Windows using the Tools Release 9.1 Update 2 and Update 3 version of the Server Manager Console Installer. If you do not select “y” on the above applet prompt entitled: “SSL Signer Exchange Prompt”, the Server Manager Console installation 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.



15. On End of Installation, verify the installation was successful. The “Please remember …” section also provides the installation log location.
16. Click Exit to exit the Oracle Universal Installer for the Server Manager Management Console.



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

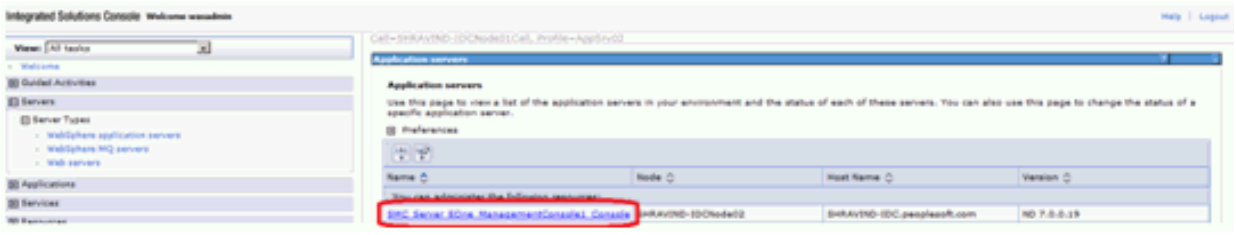
    `$ORACLE_HOME\SCFMC\`

3.7.3.6 Verifying the Server Manager Console Installation on WebSphere Application Server

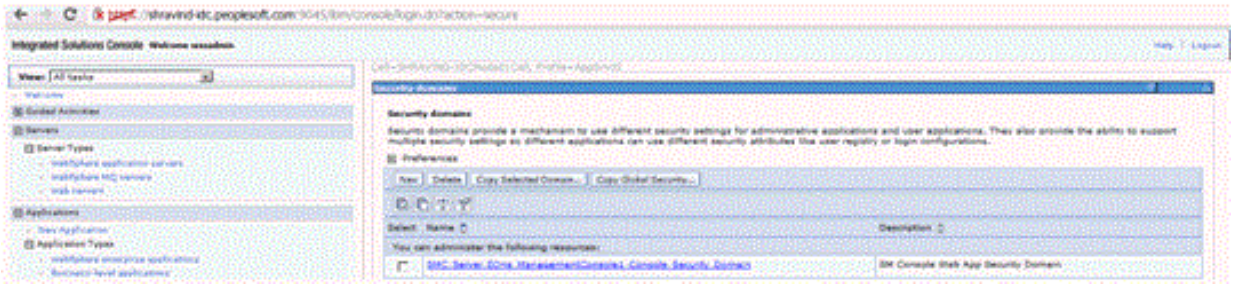
To verify the Server Manager Console installation on WebSphere Application Server:

1. Login into the WebSphere Server Admin Console.
2. Go to Servers > Server Types > WebSphere Application Servers.

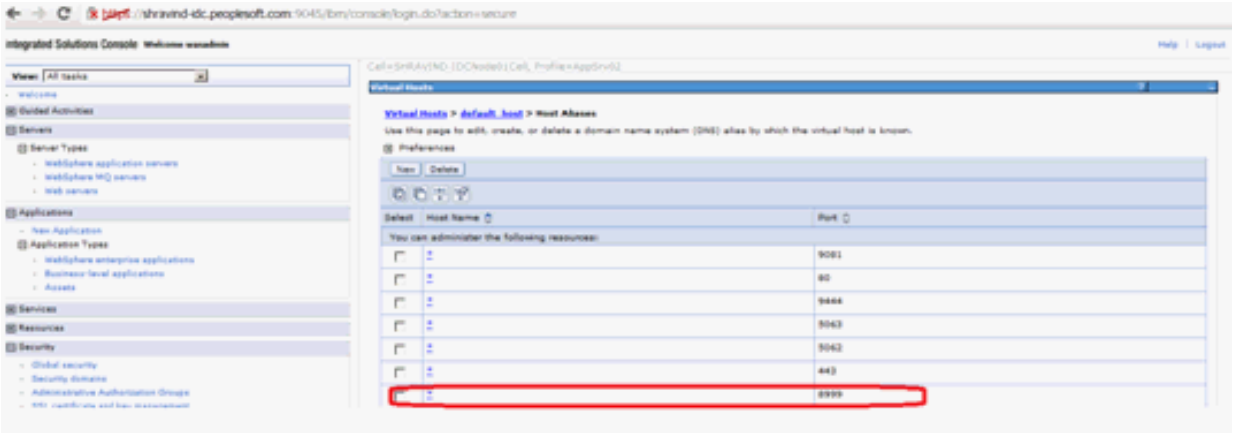
3. Verify a new J2EE Server is created for the Server Manager Console. The following screen shows an example.



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



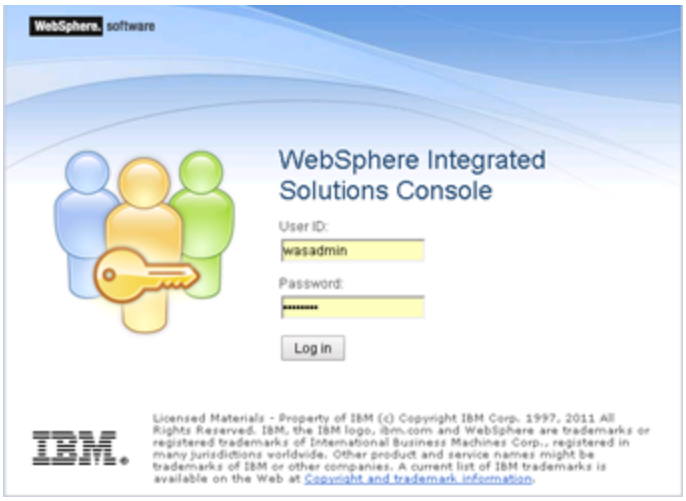
5. Go to Virtual Hosts > default_host > Host Aliases and verify that there is a host alias entry created with the HTTP Port number that you specified during the installation of the Server Manager Console. The following screen shows an example.



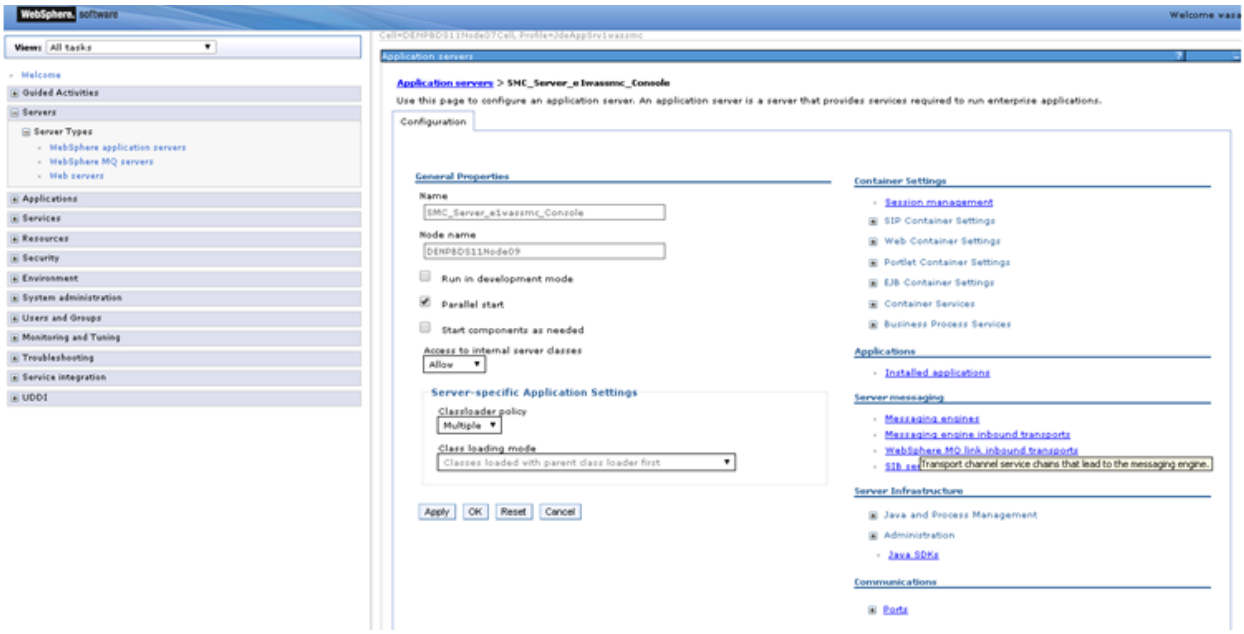
6. Verify that the successful installation has automatically started the Server Manager Console.

3.7.3.7 Enable SSL for Server Manager Console on the WebSphere Application Server

1. 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.company.com:9146/ibm/console`



2. Login to the WebSphere Admin Console using the WebSphere Administrative credentials.
3. Navigate to Servers -> Server Types -> WebSphere Application Servers.
4. Click on the Server Manager Console J2ee server (in the example below it is the SMC_ Server_e1wassmc_Console).



5. 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.
6. 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	

7. Next, navigate to Environment -> Virtual hosts -> default_host -> Host Aliases.
8. 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.company.com:9519/manage/home`

13. Go to Section 3.7.2.5, "Import Server Manager Console Certificate into the Server Manager Agent Truststore/Keystore" and perform the steps.

3.7.3.8 Troubleshooting the Server Manager Console Installation on WebSphere Application Server

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

1. Verify that all the prerequisites are met as listed in the section of this guide entitled: Section 3.7.3.4, "Prerequisites for WebSphere Application Server".
2. 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`
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.

   Microsoft Windows

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

   Linux or Solaris

   `/u01/app/oracle/oraInventory/logs`
4. 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_xxxx\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.

3.7.4 Troubleshoot the Management Console Installation

This section discusses:

- Section 3.7.4.1, "Installer Fails to Complete"
- Section 3.7.4.2, "Management Console Will Not Start"
- Section 3.7.4.3, "Management Console Will Not Save Configuration Settings"

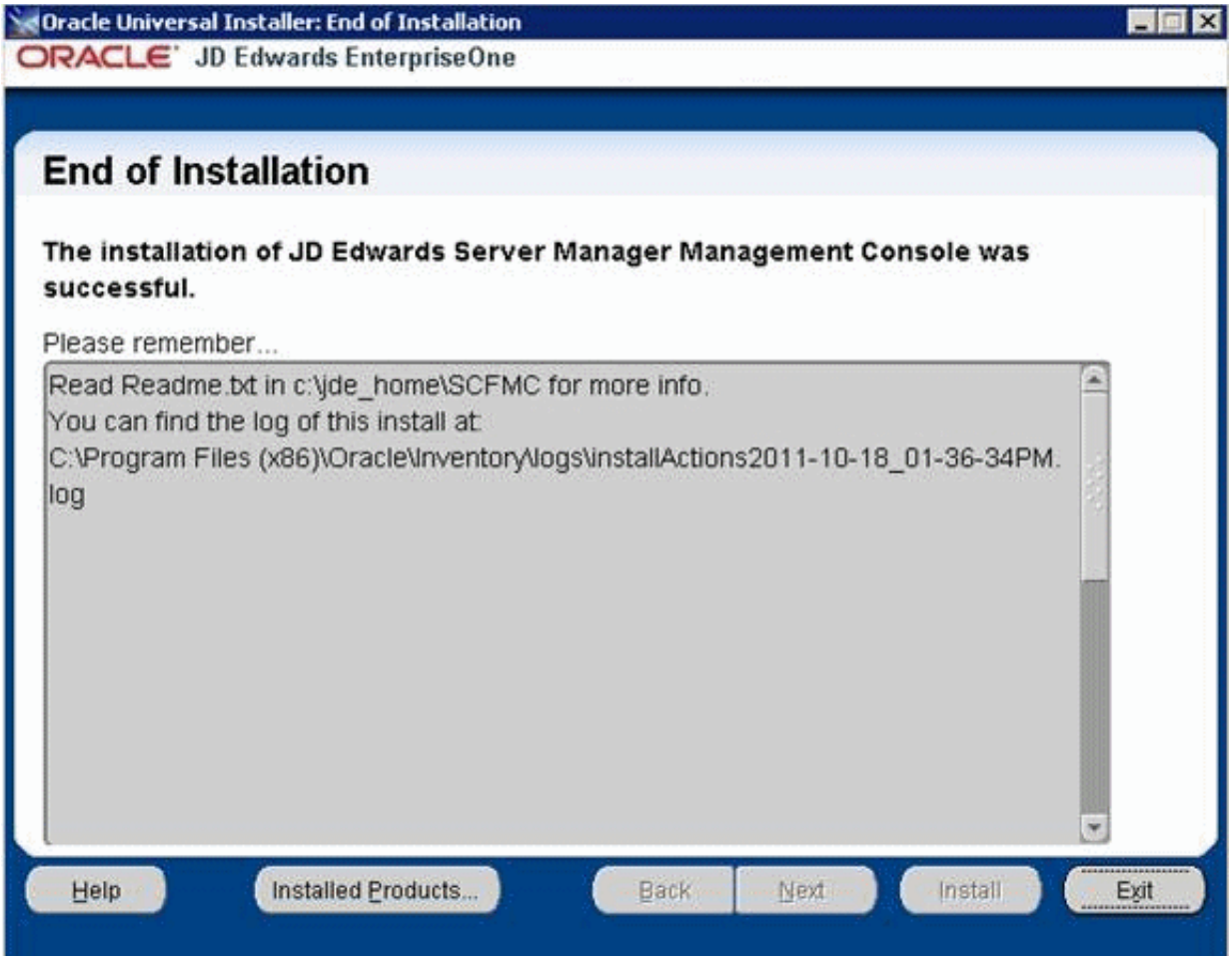
3.7.4.1 Installer Fails to Complete

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 (Release 9.1 Update 2).

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

```
C:\Program Files
(x86)\Oracle\Inventory\logs\installActions2011-10-18-02-15-1
4PM.log
```



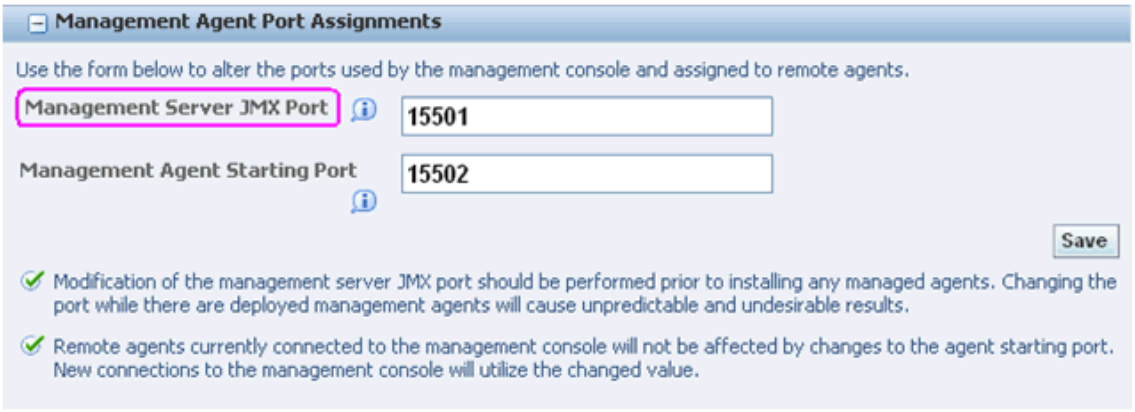
3.7.4.2 Management Console Will Not Start

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.

3.7.4.3 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:



3.8 Upgrade the Server Manager Management Console from a Previous Release to Tools Release 9.1

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 to Release 9.1.2. An Update is performed from within the Server Manager Console itself.

For Tools Release 9.1, you have the option to Upgrade an existing Server Manager Management Console that was installed with a previous release. It is important to note that this Upgrade is new functionality that is independent of the existing Server Manager self-updating functionality, which is obtained through the Update Center. You cannot use the Server Manager internal Update functionality to Upgrade to Tools Release 9.1.

Caution: If you decide to Upgrade your Management Console, there is no automated rollback path.

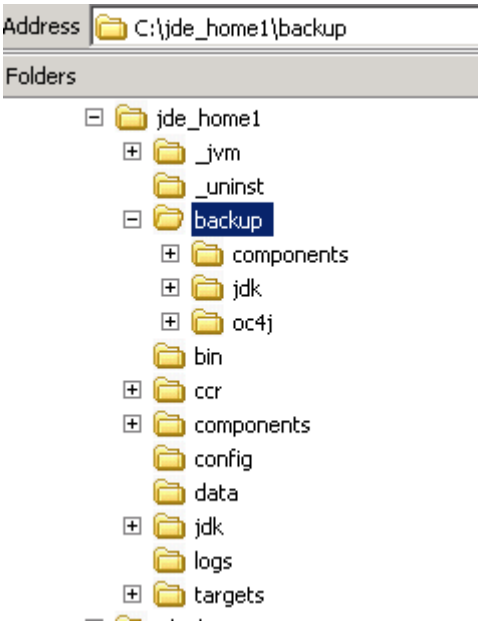
Caution: During the upgrade process the following folders from previous release will be backed up under `\backup` folder in the same Management Console home:

- `\backup\components`

  `\backup\jdk`

  `\backup\oc4j`

This is illustrated in the screen segment below.



Functionally an Upgrade of your Management Console preserves your existing Management Console configuration including the JMX port number and existing connections to the target machines of the Management Console.

Note: After you have upgraded your Server Manager Console using the OUI installer for Tools Release 9.1 (or above), you must use OUI to deinstall it as described in the section of this chapter entitled: Section 3.11, "Deinstall the Server Manager Management Console for Tools Release 9.1".

This section discusses these topics:

- Upgrade Sequence
- Running the Management Console Installer in Upgrade Mode

3.8.1 Upgrade Sequence

It is very important that you follow this sequence for upgrading:

1. Obtain the Tools Release 9.1 version of the Server Manager Management Console from the Oracle Software Delivery Cloud.
2. Run the Tools Release 9.1 installer on the machine with the existing Management Console installation.

3. The installer detects the existing Management Console installation(s) and gives you the option of upgrading.
4. If you choose to upgrade your existing Management Console, the installer creates a new JDE_HOME in which to install the Tools Release 9.1 Management Console, but uses the existing installation to obtain configuration information.

   Caution: The existing pre-9.1 installation of the Management Console must not be corrupted and must contain valid .xml files that can be read by the 9.1 Installer. If you have attempted to run the Server Manager Console Update for 9.1 prior to running the 9.1 Installer to Upgrade, you will corrupt the installation. The only recovery will be a new installation of the 9.1 which you will have to manually configure.

5. For installations beyond the initial general availability of Tools Release 9.1, you can use the standard functionality to obtain and run the update the Server Manager Console.
6. Use the standard functionality to obtain and run the updates for the Server Manager Agents on the target machines. This step is very important because for Tools Release 9.1 the Management Console and the agents must be running at least the base Tools Release 9.1.

   Caution: An exception to the Server Manager Management Console automated agent update is the AIX operating system. Prior to running the agent update, on AIX you must manually ensure that the requisite JDK or JRE for the agent is installed on the machine. For instructions on manually installing a JDK or JRE on AIX, refer to the section of this guide entitled: Manually Installing a JDK or JRE on AIX.

3.8.2 Running the Management Console Installer in Upgrade Mode

Caution: Before running the installer to Upgrade your Server Manager Management Console, you must ensure the Management Console is stopped as described in the section of this guide entitled: Start, Stop, and Restart the Management Console.

You should verify the Management Console is stopped by attempting to access the URL to the console. Refer to the section of this guide entitled: Access the Management Console.

To Upgrade the Server Manager Management Console from a previous release to Tools Release 9.1:

1. 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.
2. Obtain the Tools Release 9.1 Server Manager Console installer images from the Oracle Software Delivery Cloud.
3. Copy the installer images to the machine on which you intend to install the Server Manager Console.
4. Unzip the images into this structure:

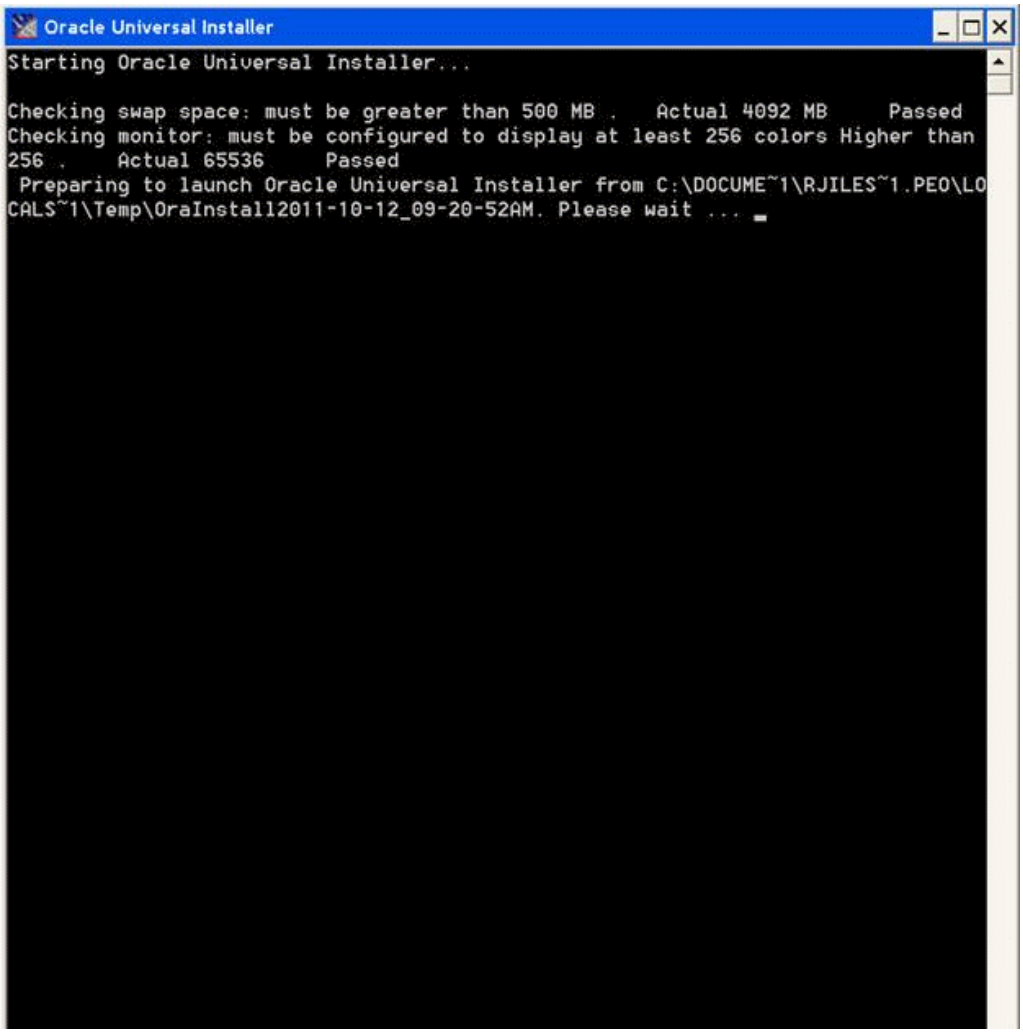
   \Disk1

\Disk2

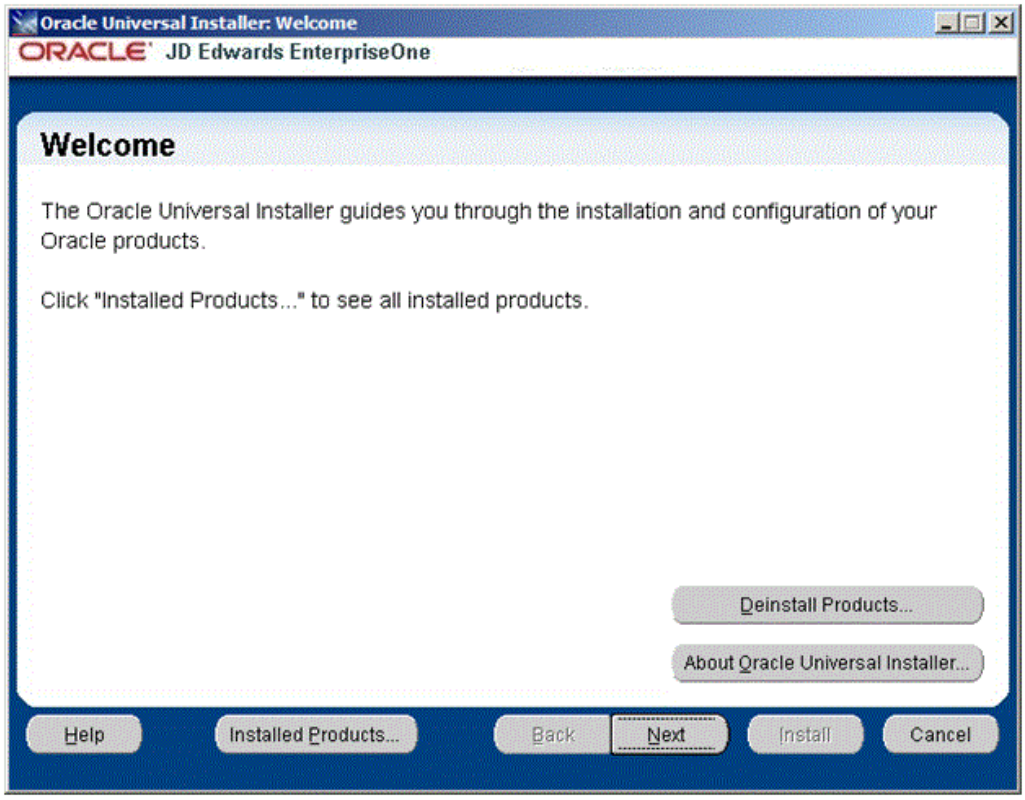
5. Run setup.exe from:

   \Disk1\Install

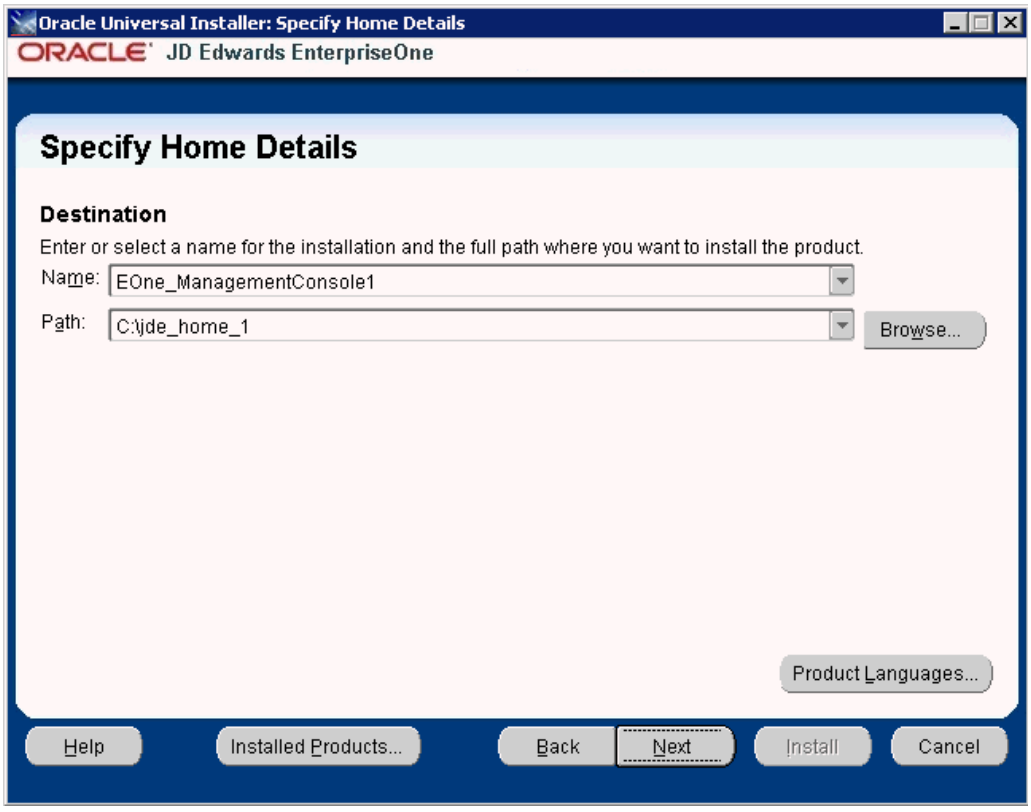
   The Windows Command window starts indicating Windows is preparing to launch the Oracle Universal Installer for the Server Manager Management Console.



   It will take a minute or so for the initialization to complete. Upon completion the OUI Welcome panel displays:



6. On Welcome, click the Next button.



1. On Specify Home Details, complete these fields:

- 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.

  Note: For upgrades you cannot specify an existing name. You must specify a new name for the upgraded Management Console.

- Path

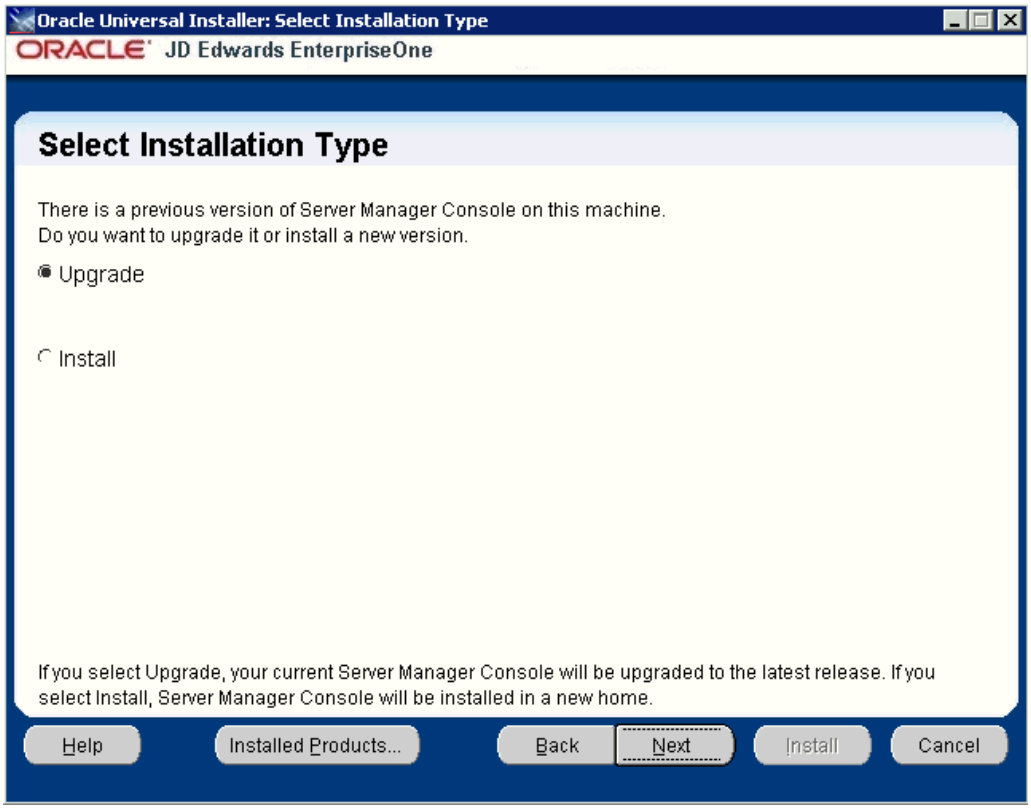
  Enter the drive and directory where you want the files installed on your Management Console. The JD Edwards EnterpriseOne Management Console installer automatically detects the root drive location on the Microsoft Windows machine and by default appends this value:

  JDE_HOME

  Note: Although JDE_HOME is the default and recommended setting, you can specify any value to replace the default value. 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_2.

  Caution: For Upgrades, you cannot re-use an existing Name or Path. You must enter unique values.

2. Click the Next button.



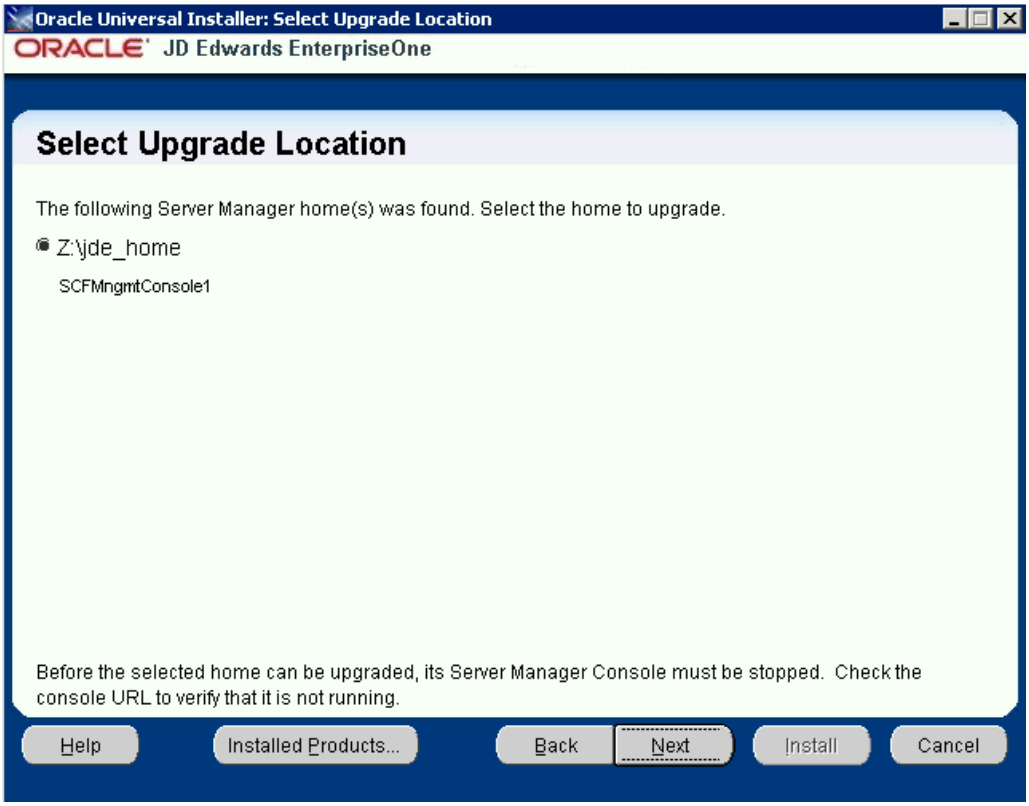
3. This Select Installation Type screen is displayed if an existing pre-Tools Release 9.1 installation of the Server Manager Console is detected.

   If you select **Upgrade**, your current Server Manager Console will be upgraded to the latest release. If you select **Install**, the Server Manager Console will be installed in a new home.

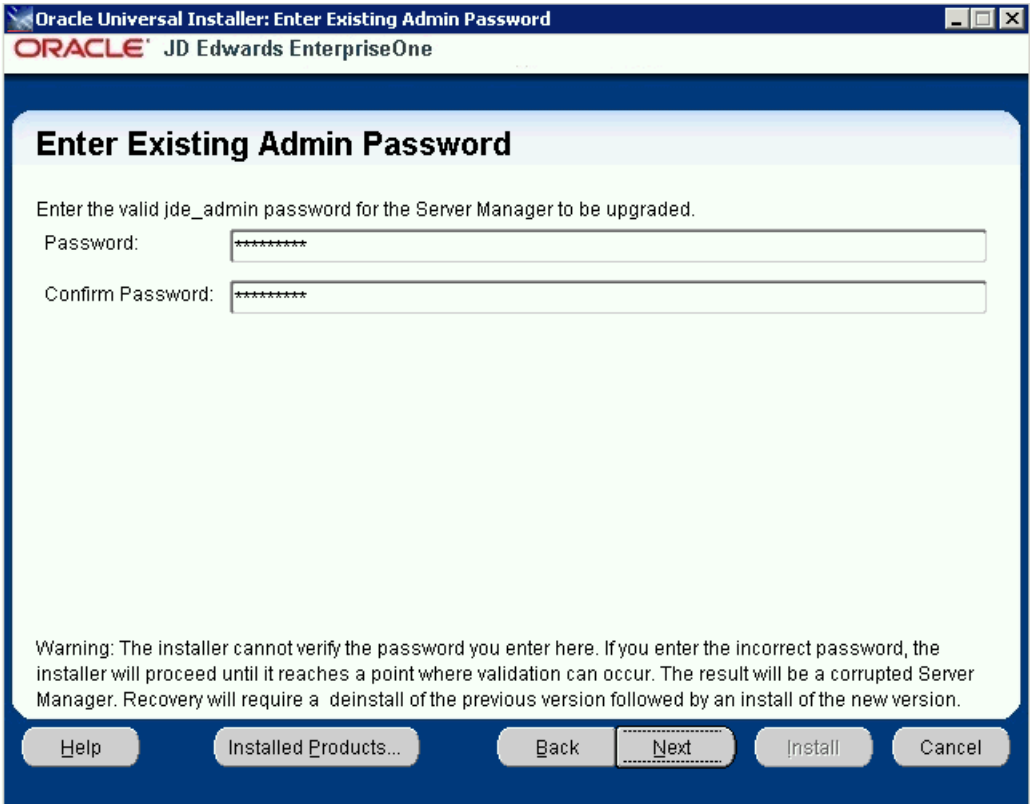
   By default, the **Upgrade** radio button is selected.

4. To Upgrade, with the Upgrade radio button selected, click the **Next** button.

5. With **Yes** button selected, click the **Next** button.



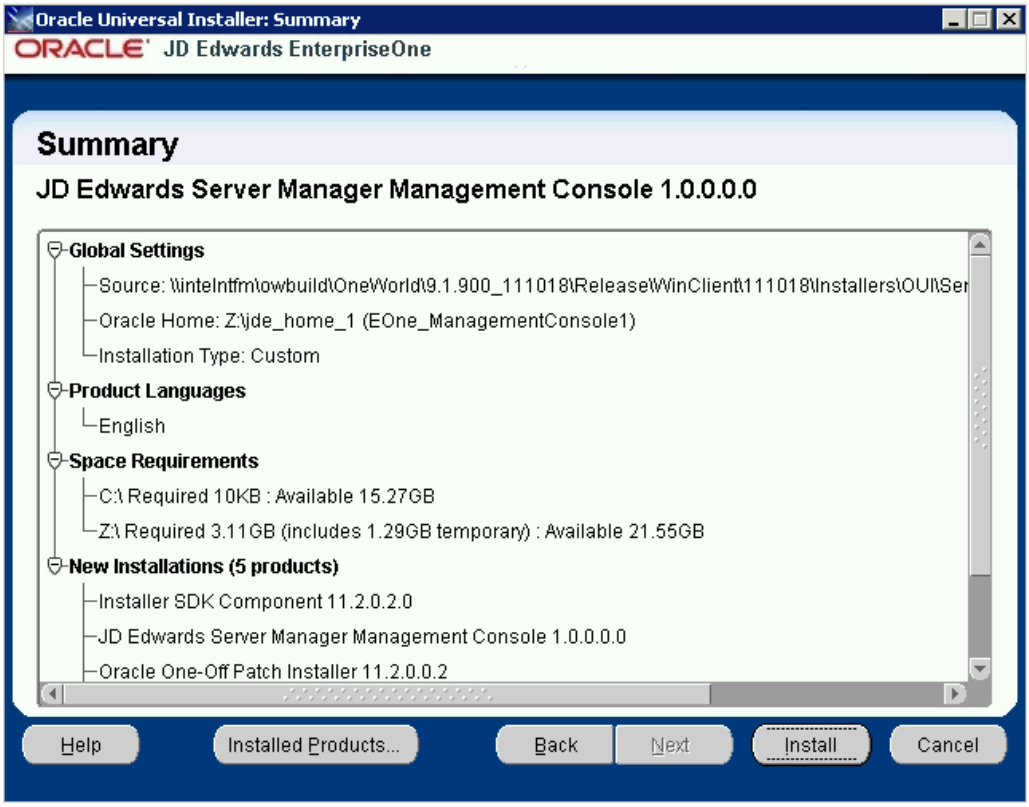
6. On Select Upgrade Location, click the radio button(s) for each home you want to upgrade.
7. Click the Next button.



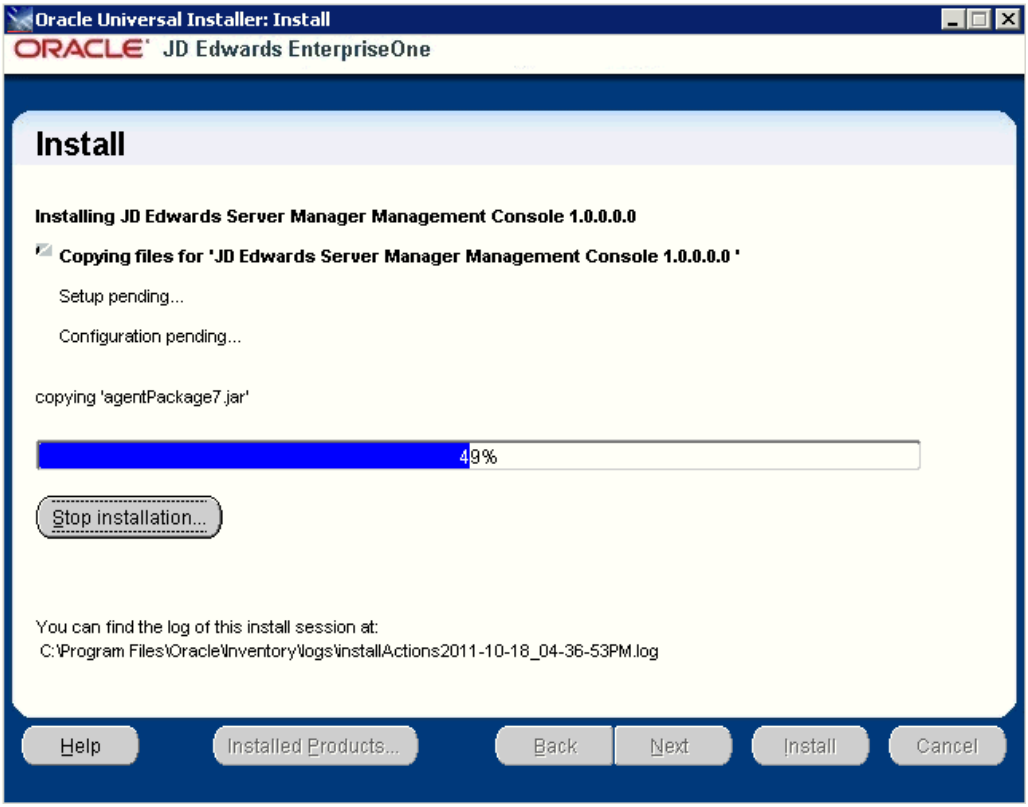
8. On Enter Existing Admin Password, enter the valid jde_admin password for the Server Manager to be upgraded.

> **Caution:** The installer cannot verify the password you enter here. If you enter the incorrect password, the installer will proceed until it reaches a point where validation can occur. If you enter an invalid password, the result will be a corrupted Server Manager. Recovery will require a deinstall of the previous version followed by an install the new version.

9. Click the **Next** button.

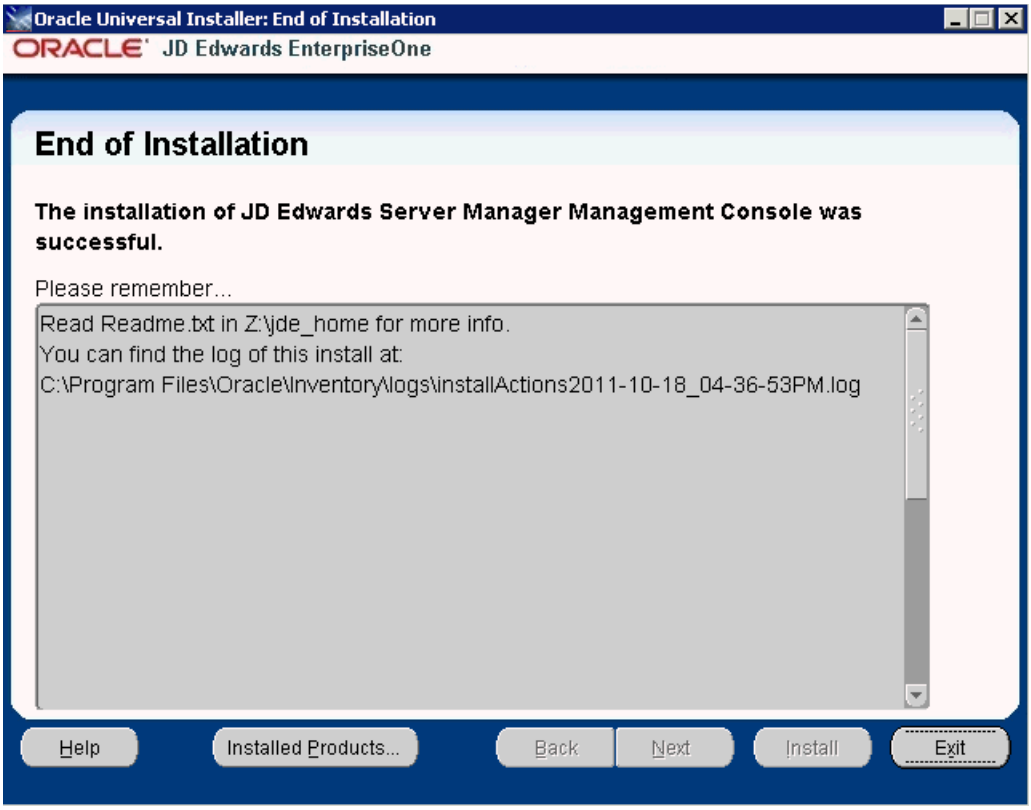


10. On Summary, confirm the selections.
11. Click the **Install** button.

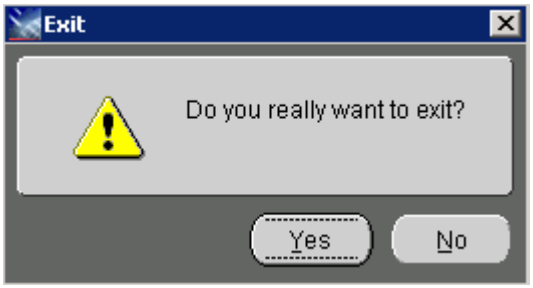


The Install progress screen is displayed. Note that this screen displays the location of the log of this installation. For example:

```
C:\Program Files\Oracle\Inventory\logs\installActions2011-10-18_
04-36-53PM.log
```



12. On End of Installation, click the **Exit** button to exit the Oracle Universal Installer for the Server Manager Management Console.



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

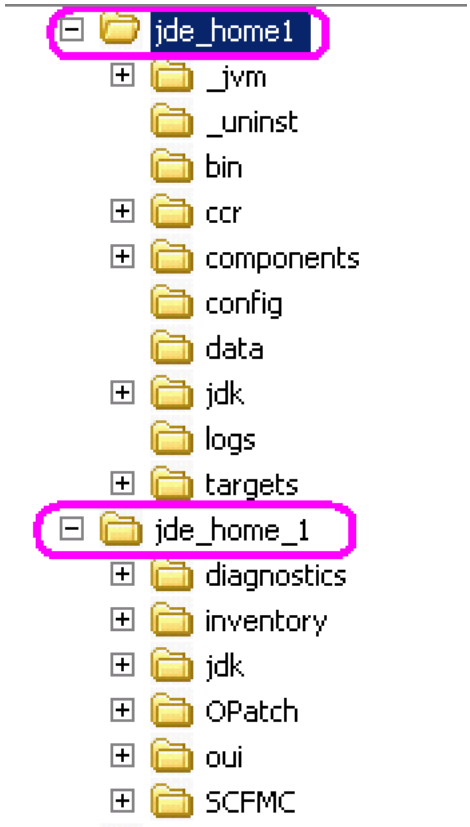
3.8.3 Post Upgrade Notes

After the Server Manager Console upgrade is complete, you might have two home folders:

- One home folder contains the Server Manager Console as a result of the upgrade
- The other home folder contains the OUI installer.

You must not delete any one of these folders. If you do, your Server Manager Console installation will be corrupted and you will not be able to reinstall or deinstall.

For example, in the below screen shot **jde_home1** is the upgraded home, while **jde_home_1** is the OUI home.



3.9 Upgrade the Server Manager Management Console with Oracle WebLogic Server 12.1.2 (Release 9.1 Update 4)

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

3.9.1 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.

3.9.2 Uninstalling Server Manager Console Installed on Oracle WebLogic Server 10.3.6

Uninstall the Server Manager Console by using the Oracle Universal Installer.

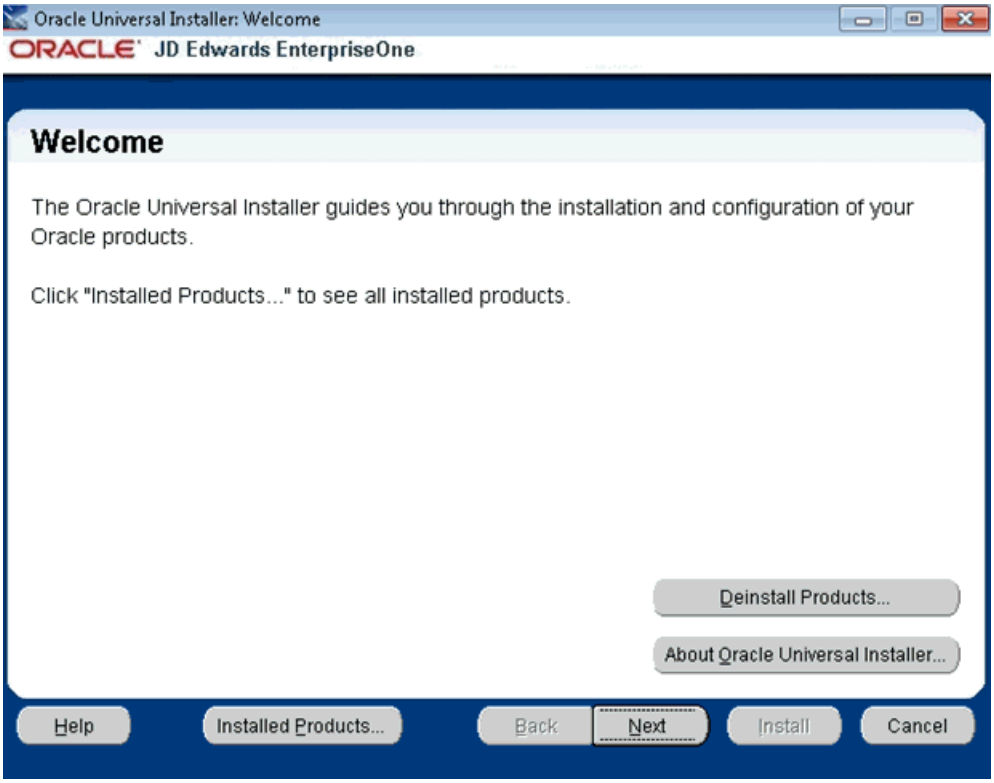
Prior to uninstalling the existing Server Manager Console, keep a backup these folders and files:

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:

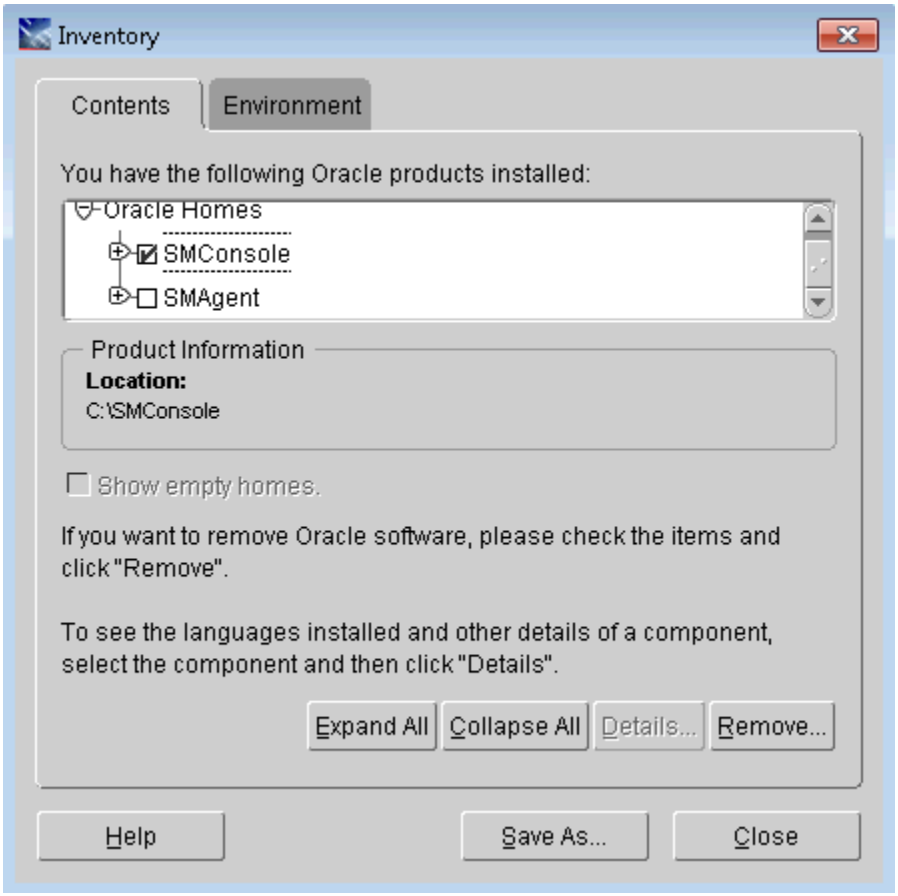
1. Invoke the Oracle Universal Installer on the Server Manager Console installed machine.

Figure 3–1 Welcome Screen



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

Figure 3–2 Inventory



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.

3.9.3 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.

http://docs.oracle.com/middleware/1212/webtier/WTINS/index.html

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 edelivery web 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:

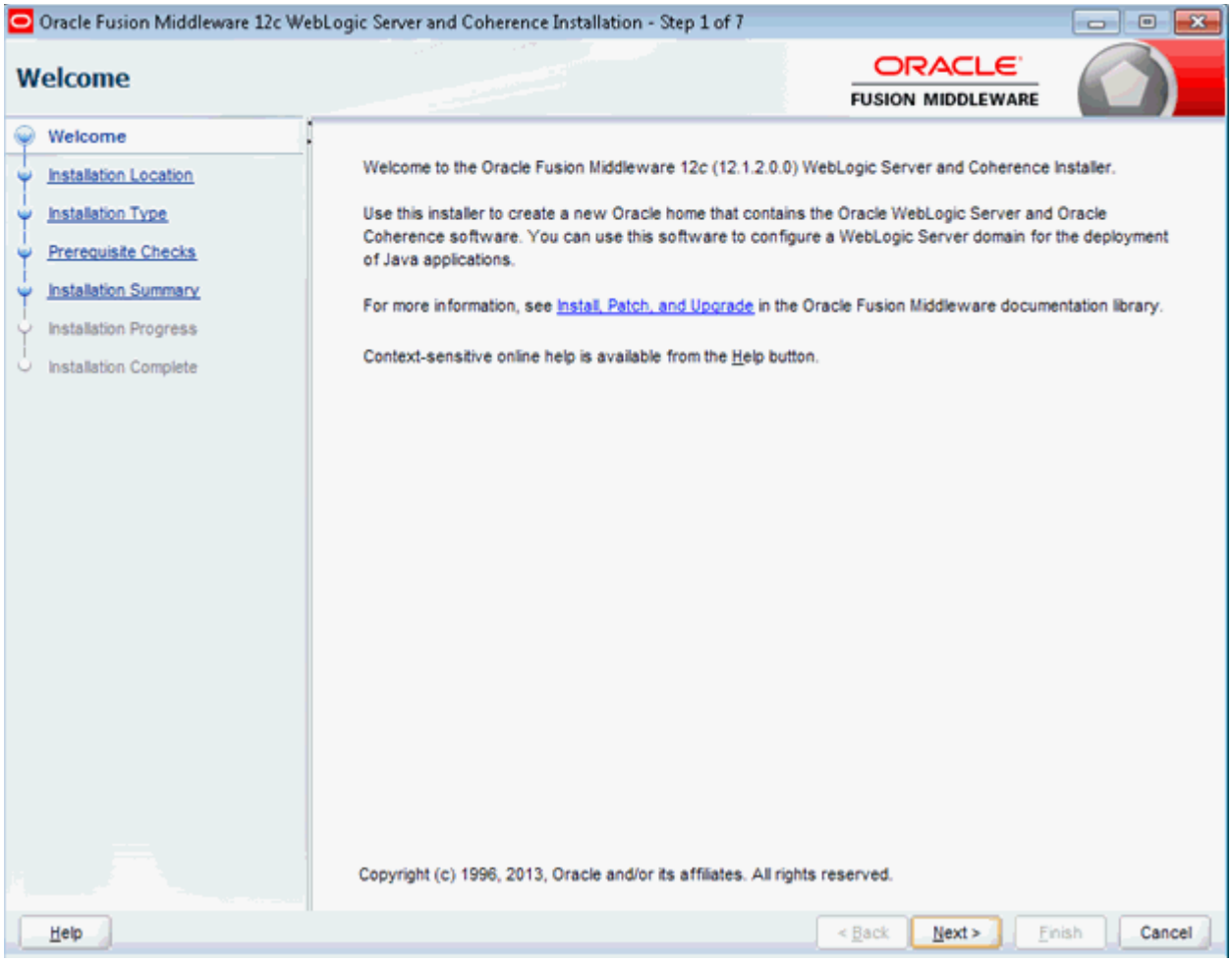
   ```
   >java -jar wls_121200.jar
   ```

   For HP-UX and Solaris use the ‘-d64’ option:

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

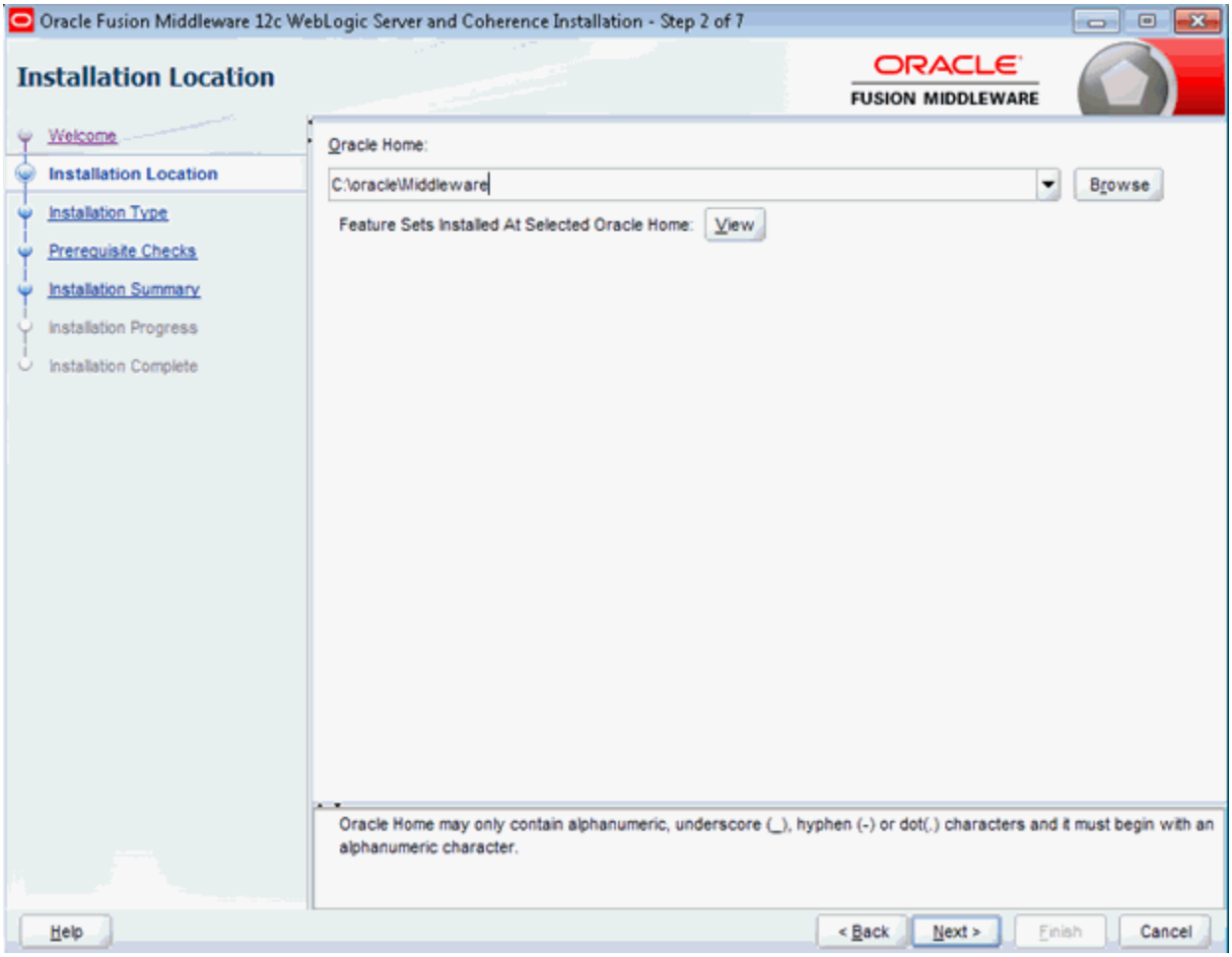
The first screen you will see is the welcome screen.

Figure 3–3 Welcome Screen



4. Click the “Next” button to begin the installation.

Figure 3–4 Installation Location

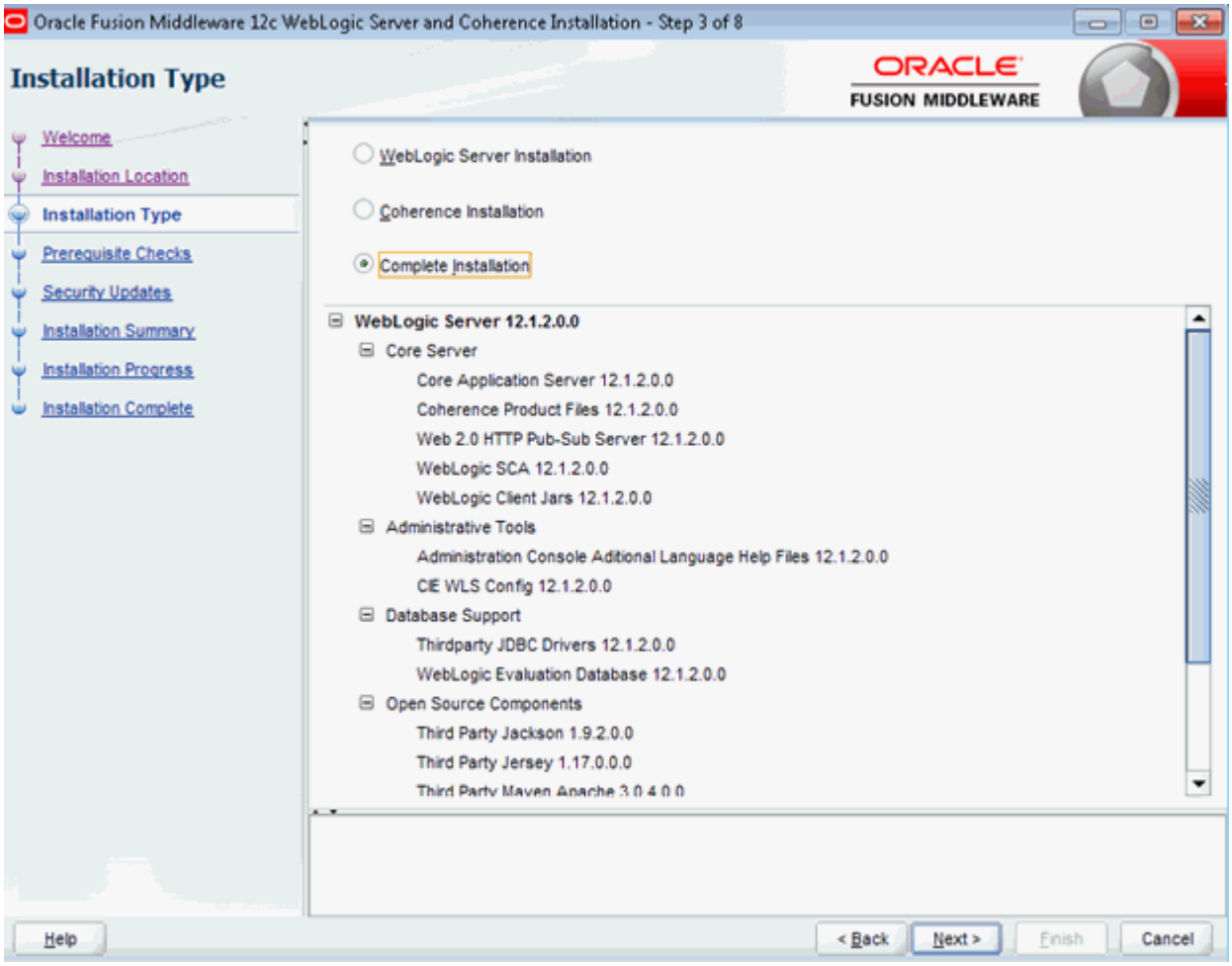


If you have an existing directory into which one or more Oracle products have already been installed, that directory can be viewed in the drop-down list. You can see which products are installed in that particular directory by clicking View next to “Features Sets Installed at Selected Oracle Home.”

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”.

Figure 3–5 Installation Type

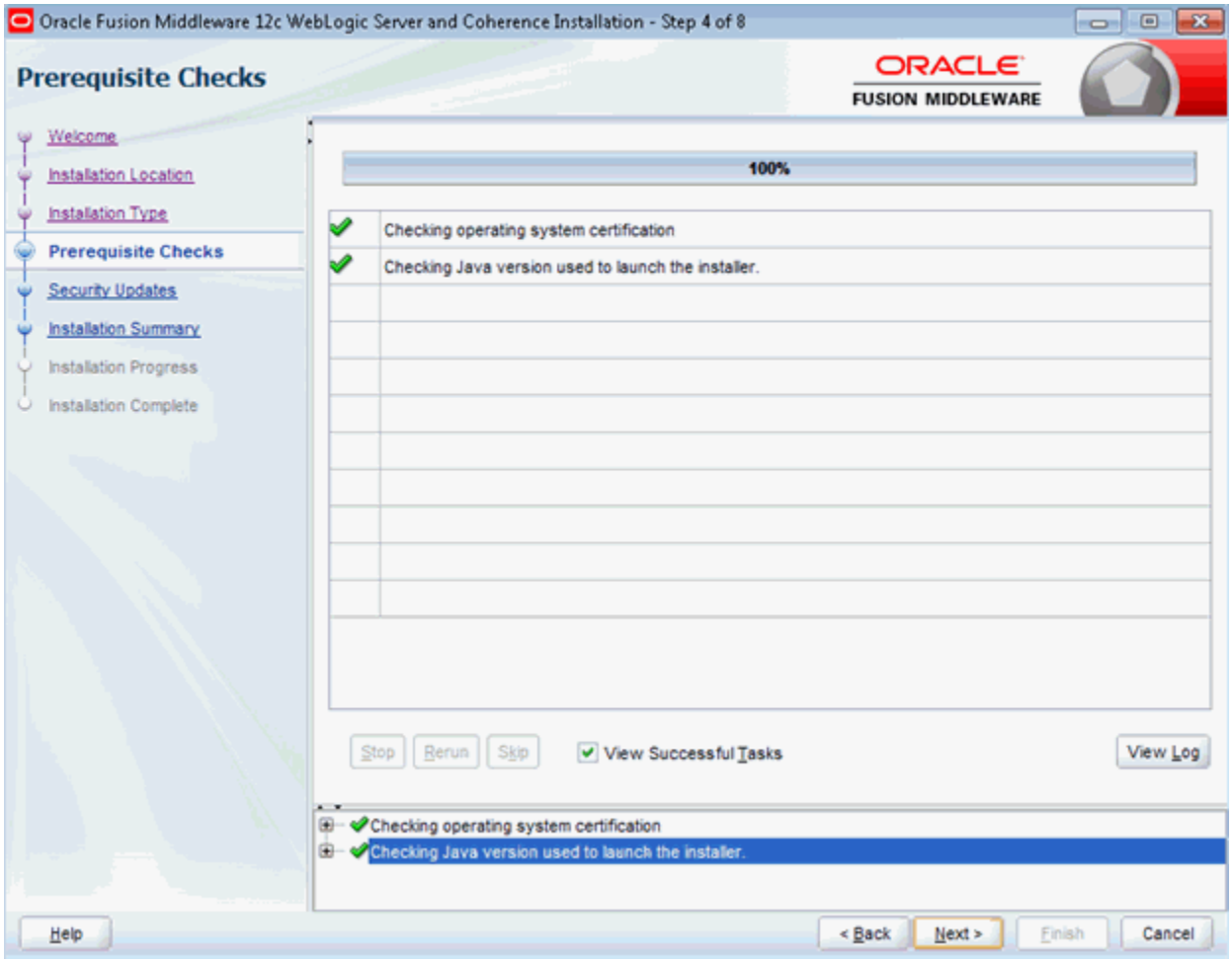


Use this screen to determine the type of installation you want to perform and consequently, which products and features are installed.

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”.

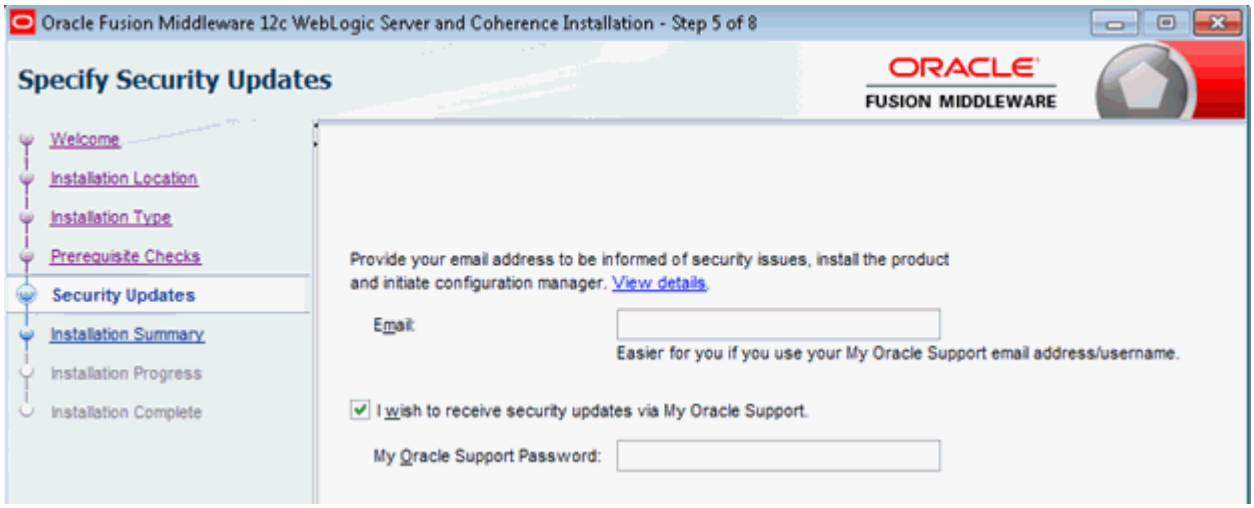
Figure 3–6 Prerequisite Checks



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”.

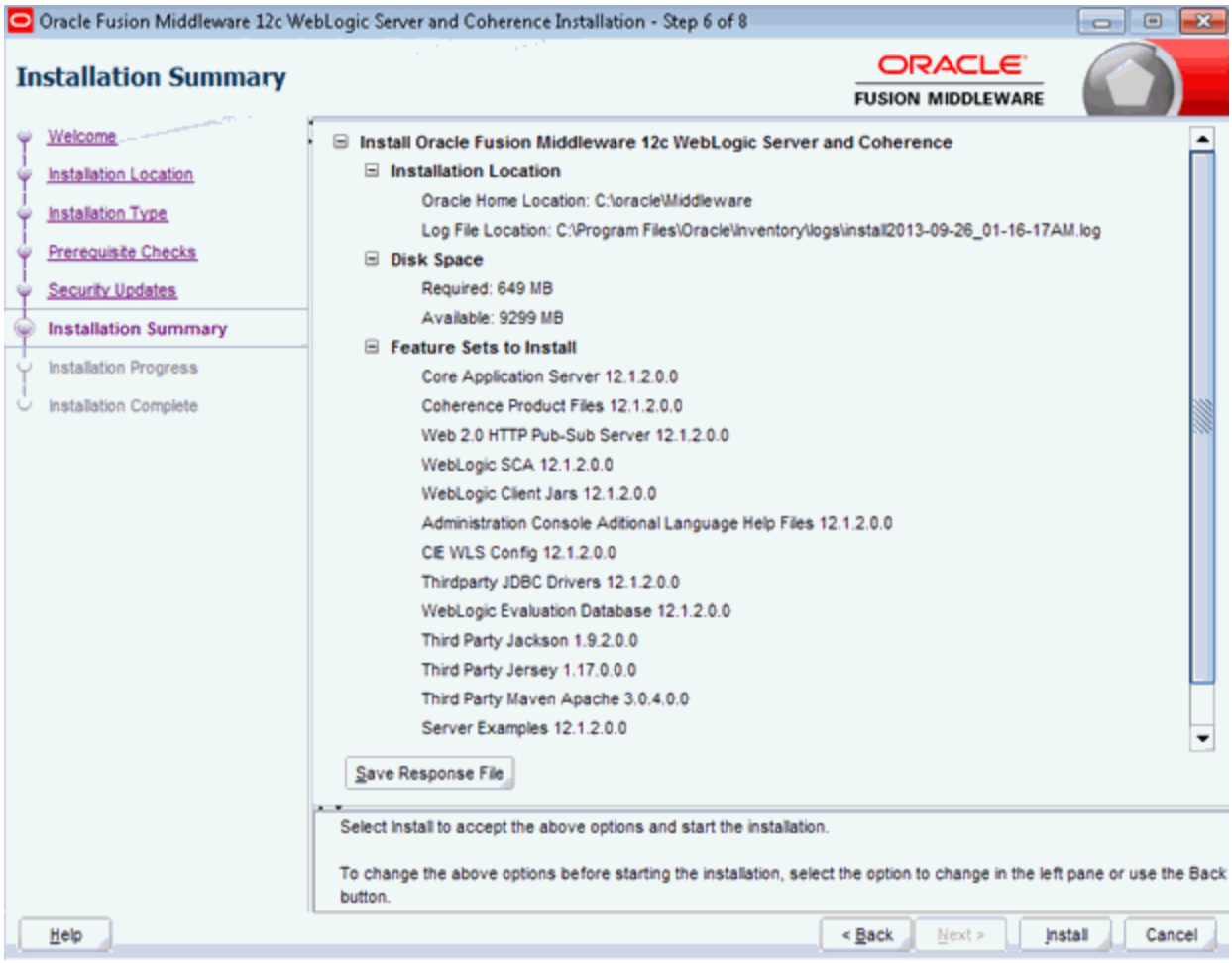
Figure 3–7 Specify Security Checks



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".

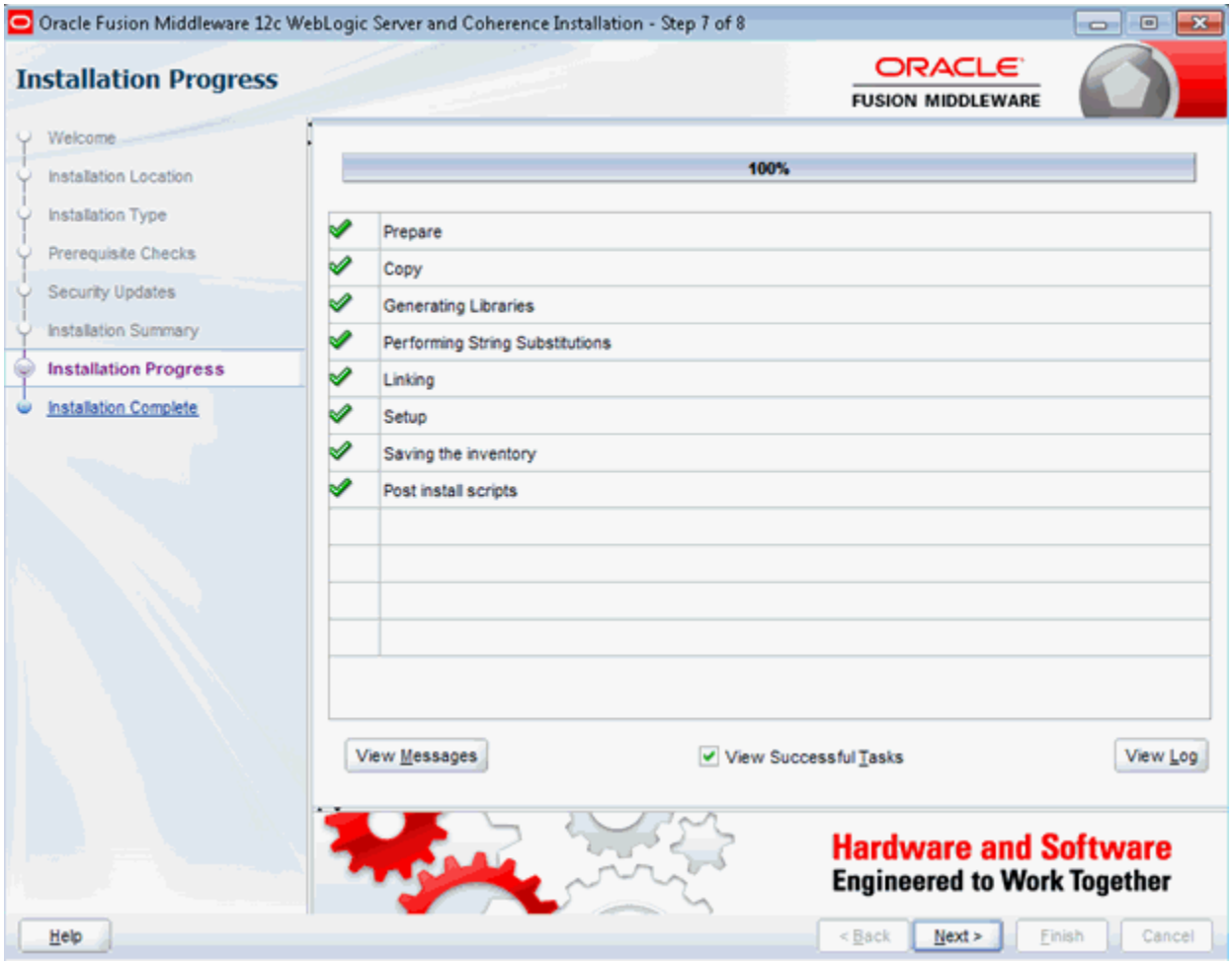
Figure 3–8 Installation Summary



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

9. Click "Install".

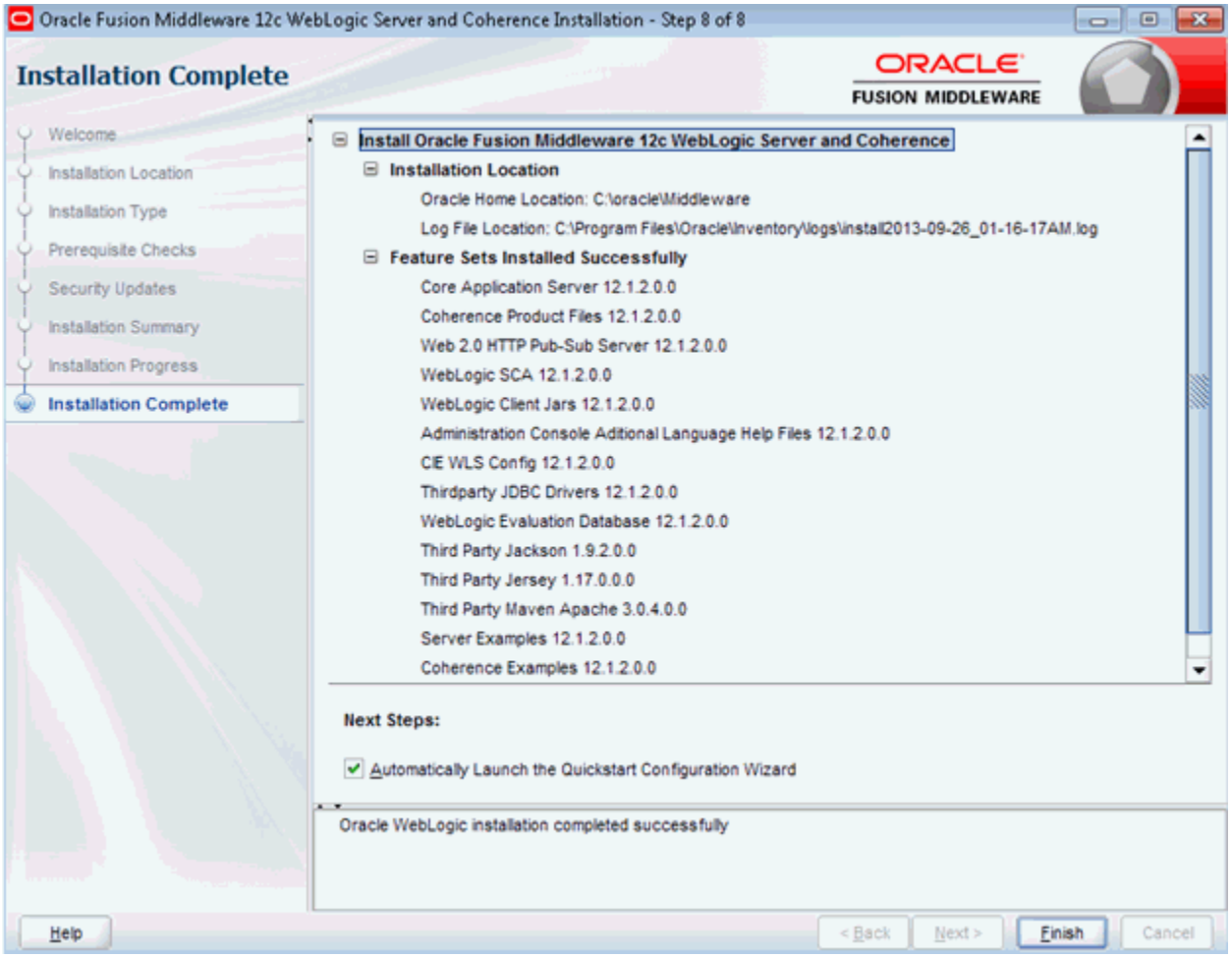
Figure 3–9 Installation Progress



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

10. Click “Next”.

Figure 3–10 Installation Complete

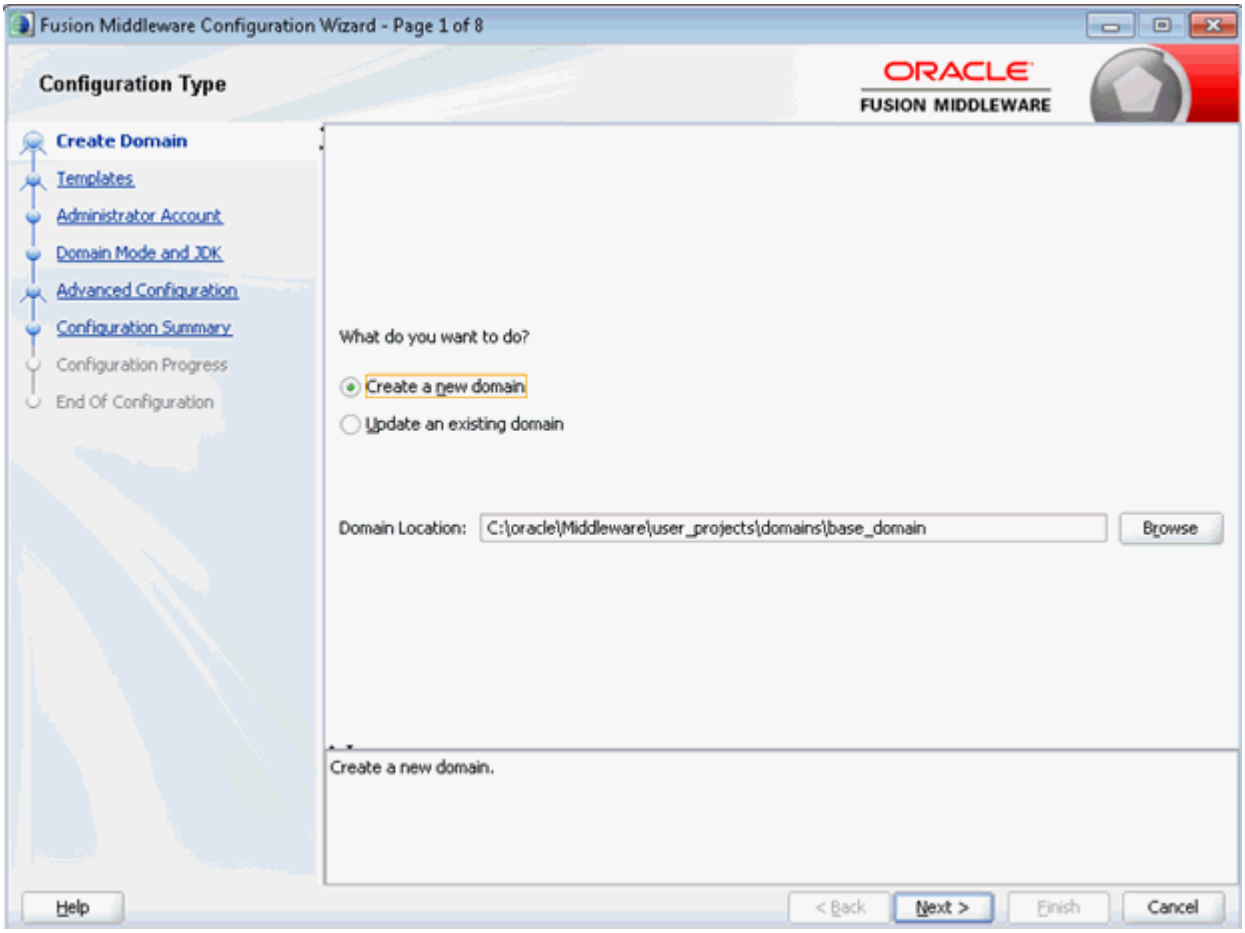


This screen appears at the conclusion of the installation and provides a summary of the products and features that were installed. Click “Finish”.

11. Create a domain using the Configuration Wizard.

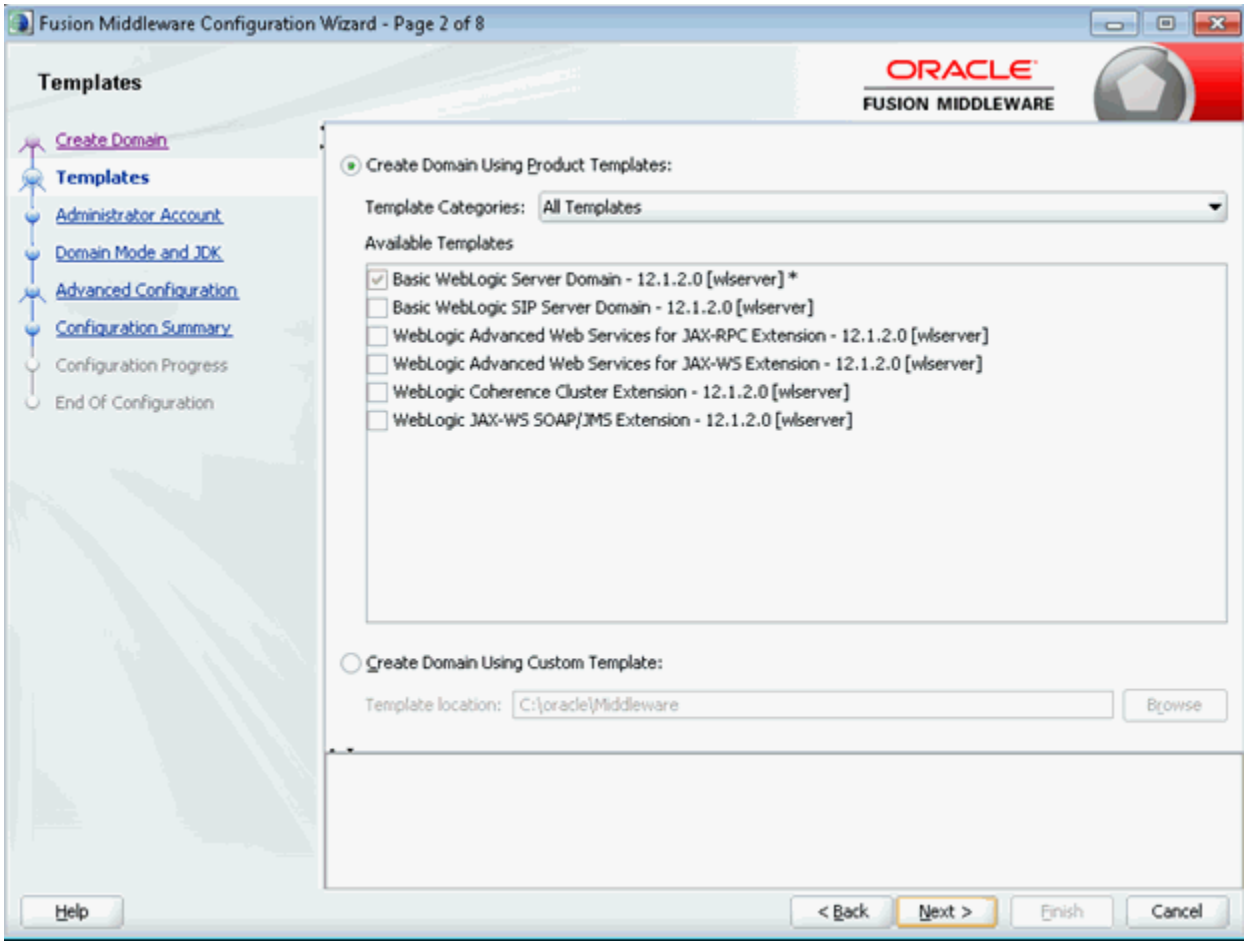
Run the Configuration Wizard to create a domain. Configuration Wizard can also be invoked by running the command < ORACLE_ HOME>\oracle_ common\common\bin\config.cmd.

Figure 3–11 Configuration Type



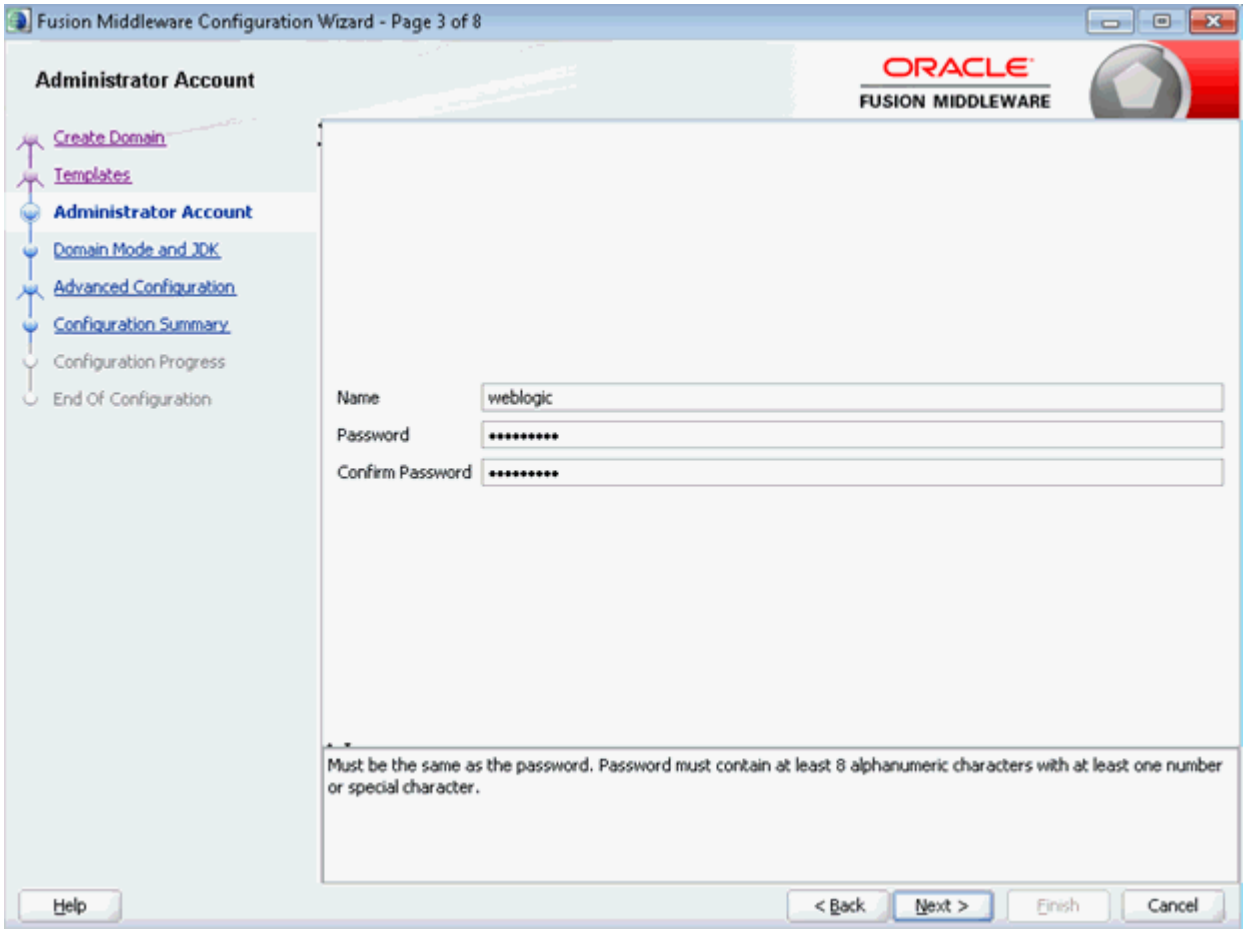
12. Provide the domain location. The domain location is `C:\Oracle\Middleware\user_projects\domains\base_domain` and the base_domain is the domain name. Click "Next".

Figure 3–12 Templates



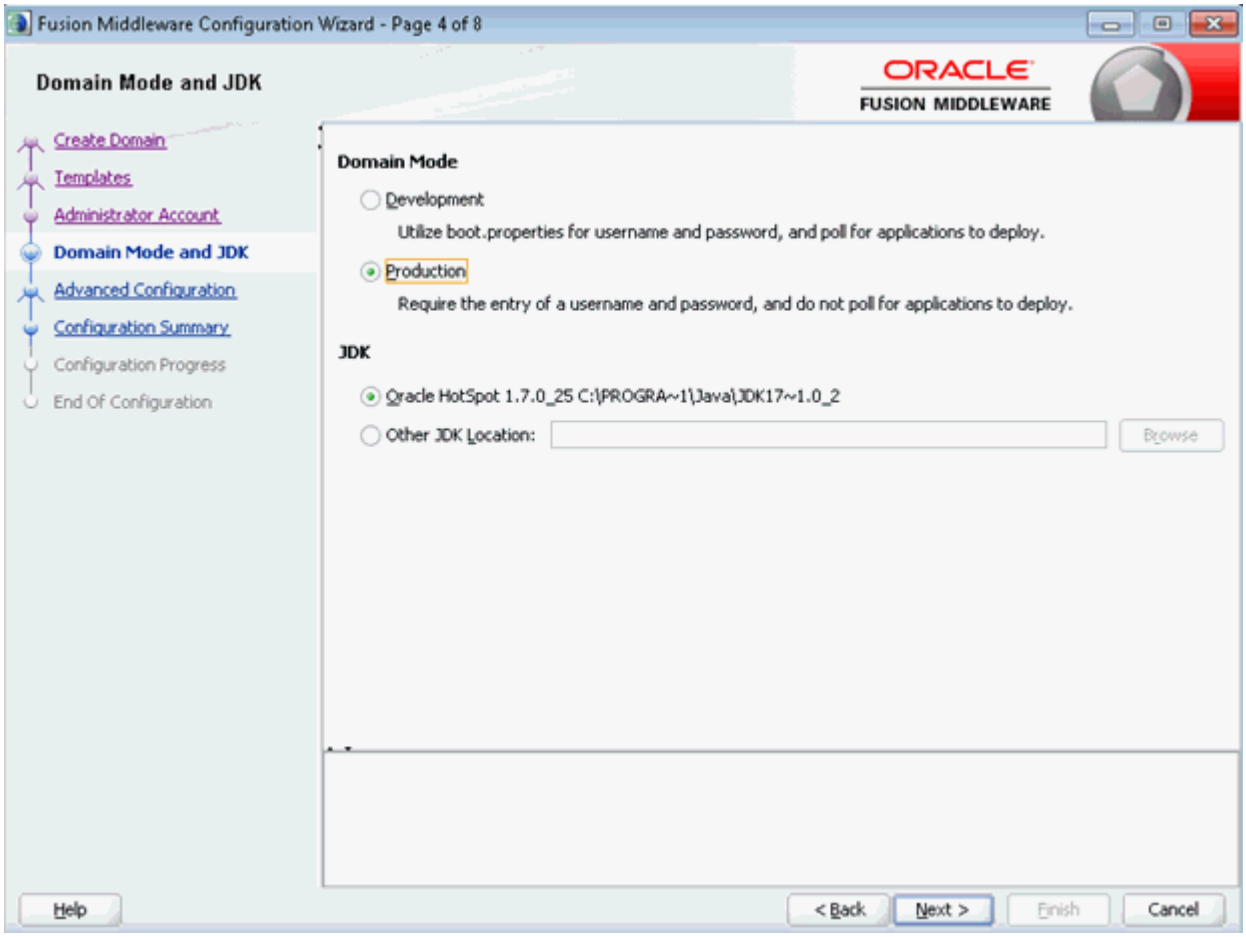
13. Select the template “Basic WebLogic Server Domain” and Click “Next”.

Figure 3–13 Administrator Accounts



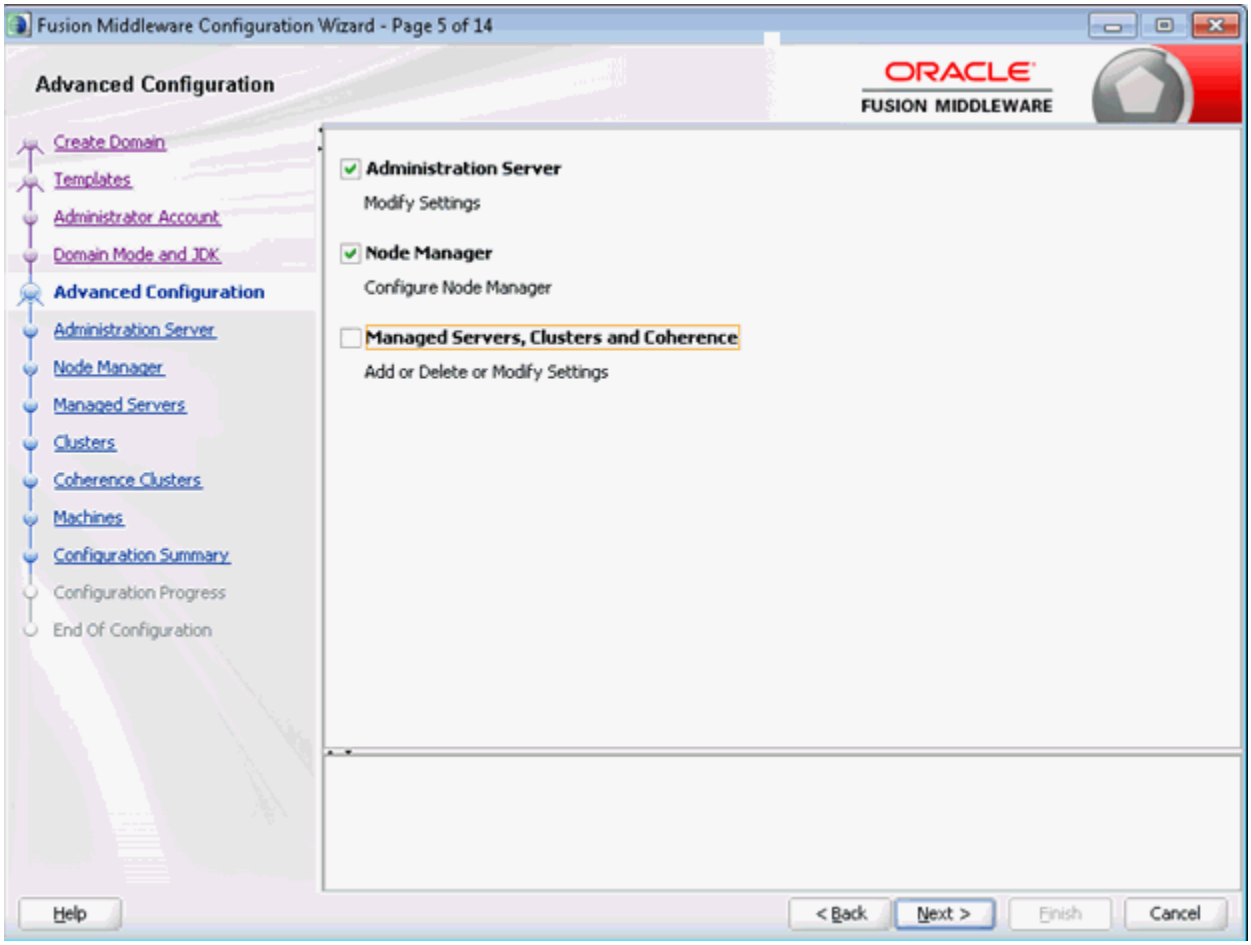
14. Provide the Administrative Username/Password for the domain and Click “Next”

Figure 3–14 Domain Mode and JDK



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”.

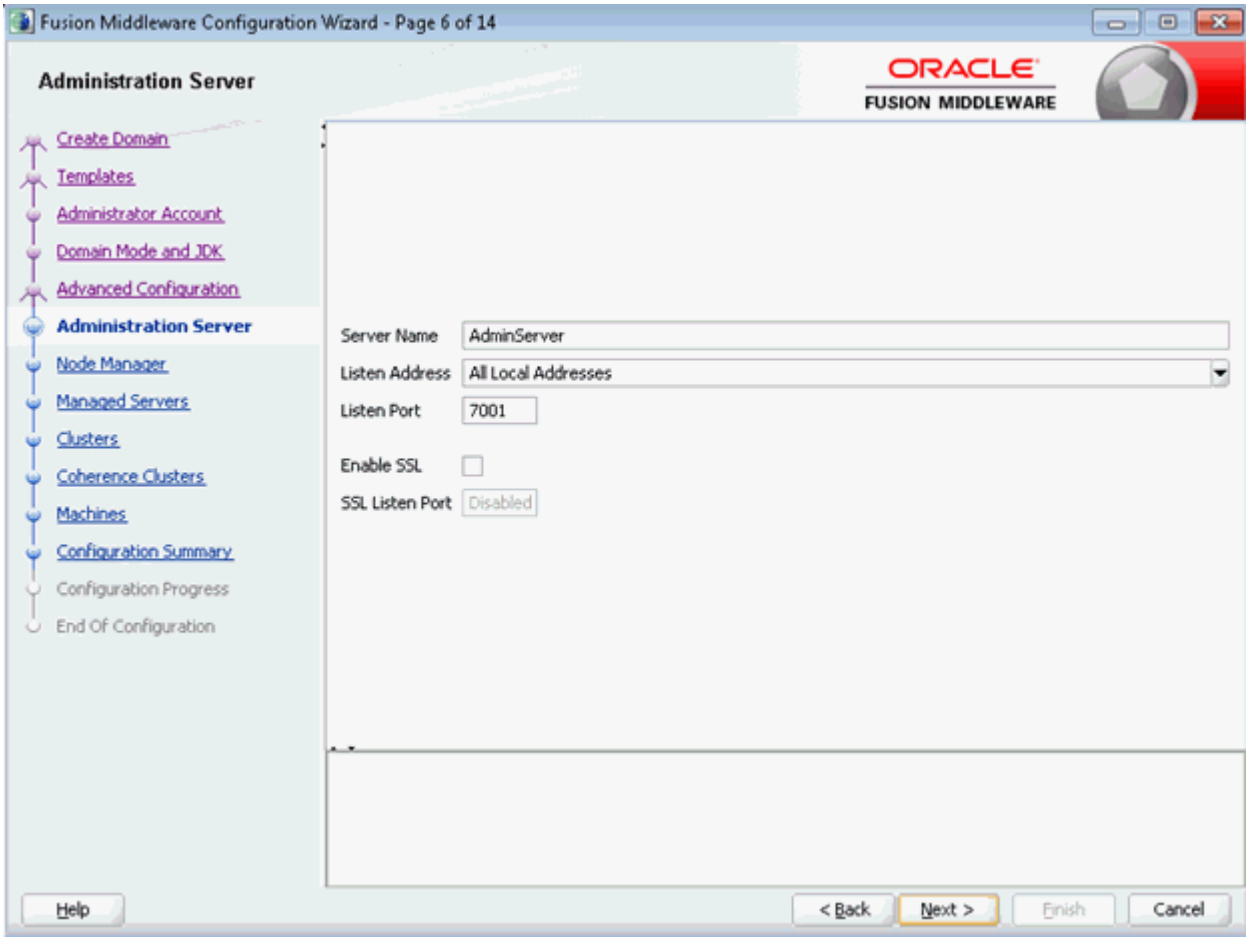
Figure 3–15 Advanced Configuration



16. On Advanced Configuration, select these check boxes to modify the server settings:
    - Administration Server
    - Node Manager

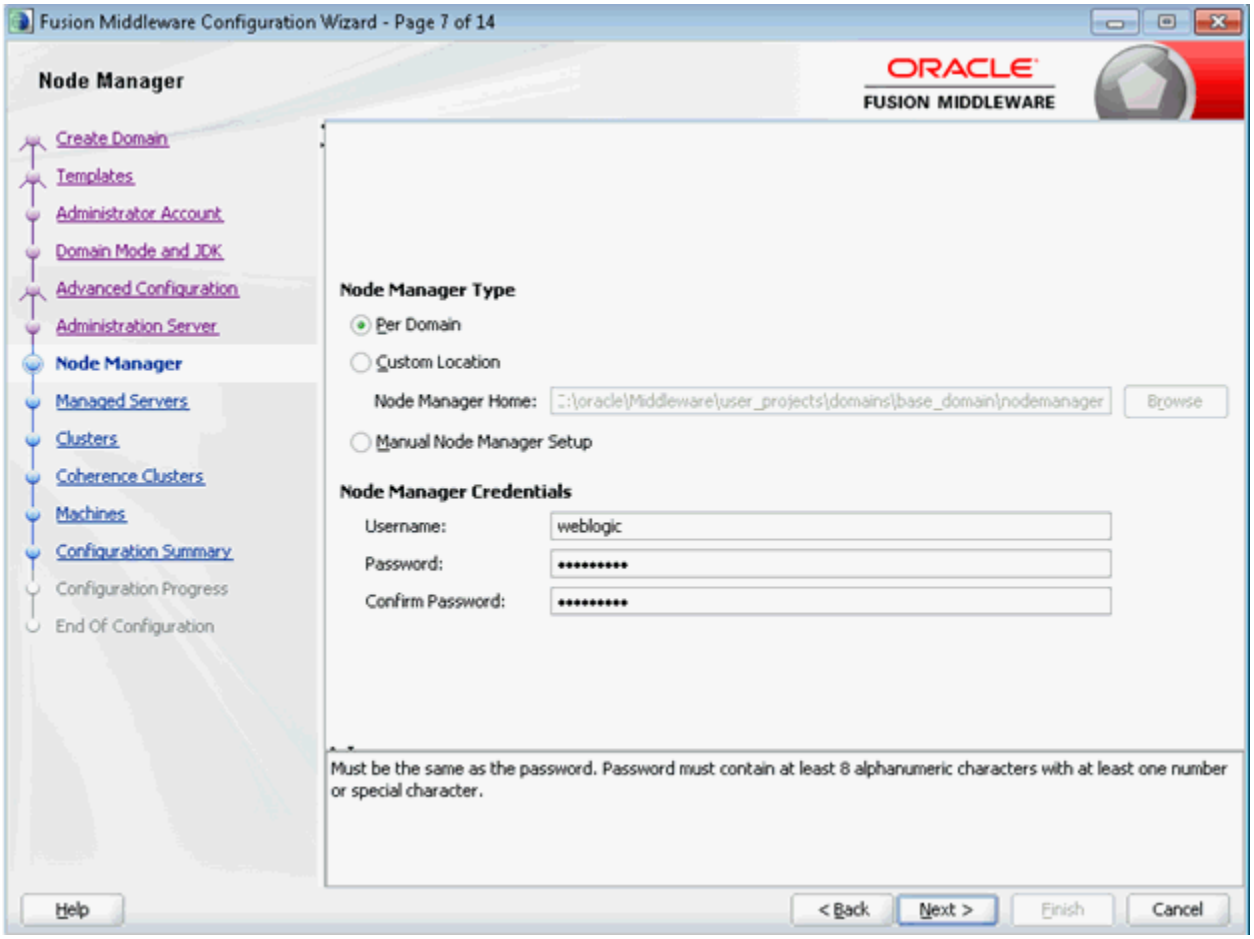
    Click “Next”.

Figure 3–16 Administration Server



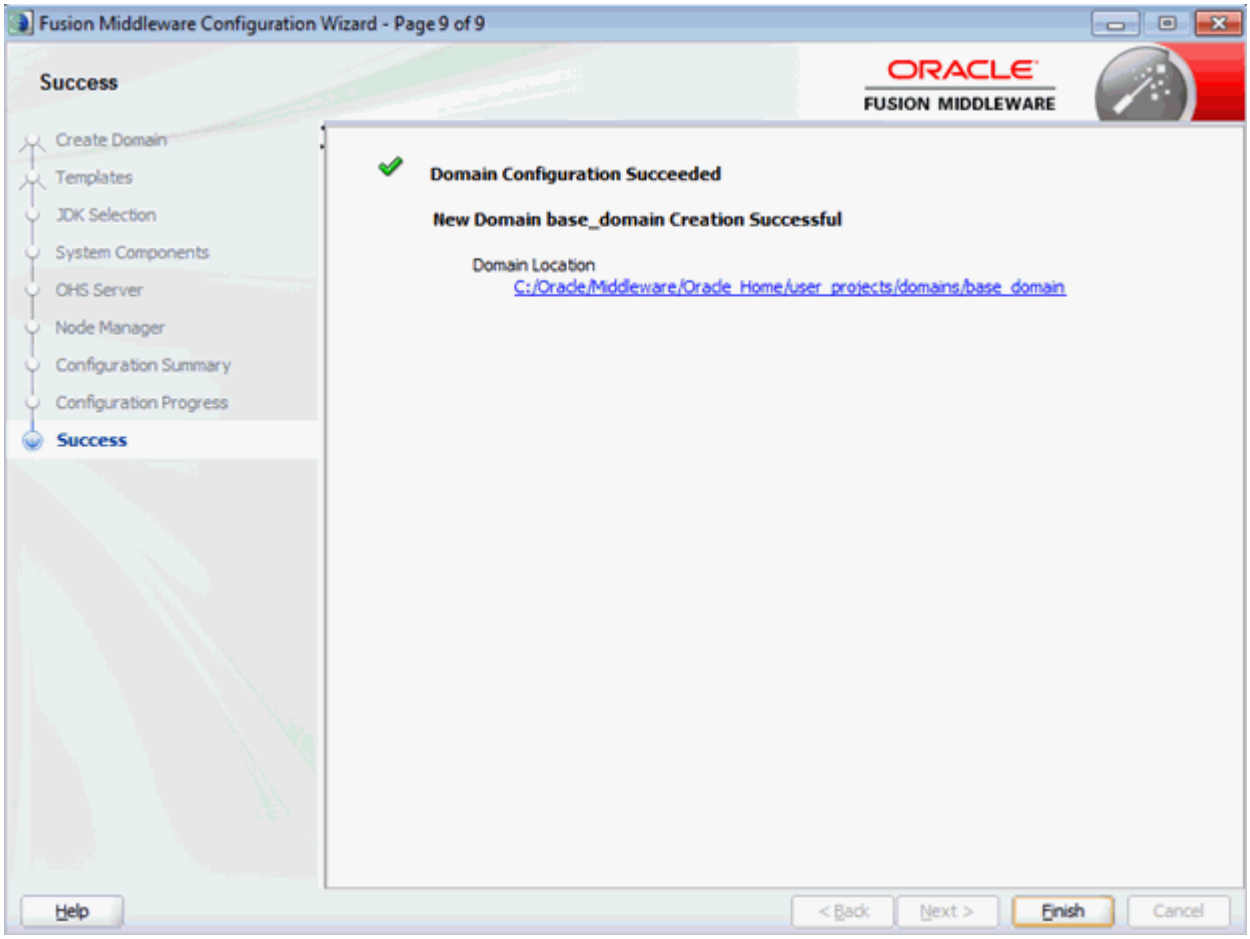
17. You may change the Listen Port on this screen. Click “Next”.

Figure 3–17 Node Manager



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

Figure 3–18 Success



19. Domain creation is successful. Click “Finish”.
20. Start Node Manager.

    Node Manager can be started by running the command `startNodeManager.bat` available at:

    `<ORACLE_ HOME>\user_projects\domains\base_domain\bin`
21. Start WebLogic Server.

    HTTP Server can be started by running the command `startComponent.bat` available at:

    `< ORACLE_ HOME>\user_projects\domains\base_domain\bin`
22. Run the command `startWebLogic.bat`.

3.9.4 Installing Server Manager Console on WebLogic Server 12.1.2

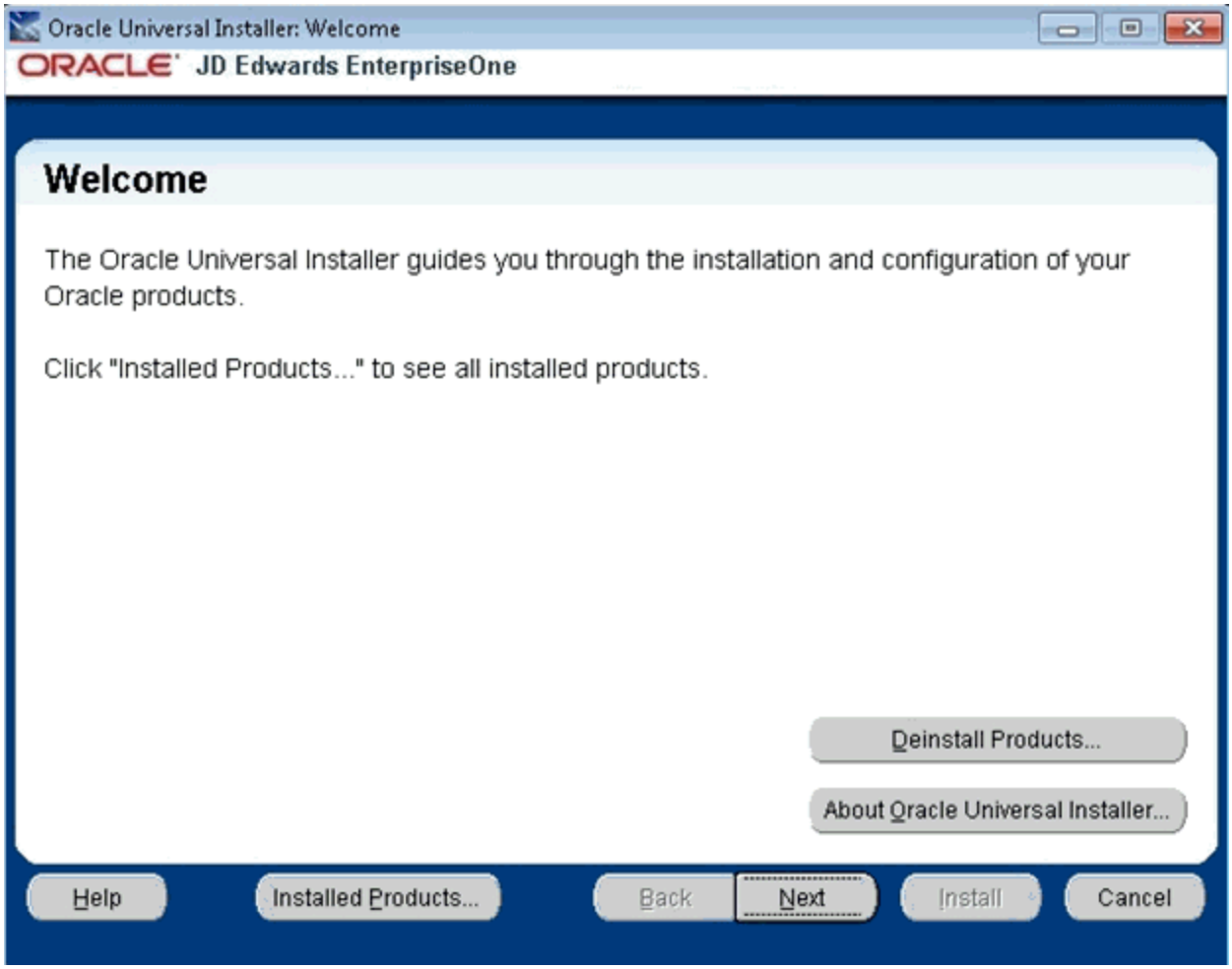
To install the Server Manager Console:

1. Change to the directory in which you extracted the Server Manager Console installer.
2. Launch the OUI installer as follows:

   Using “Run As Administrator”, run the `setup.exe` from the directory (e.g C:\SM_ Console\Disk1\install) in which you unzipped the installer.

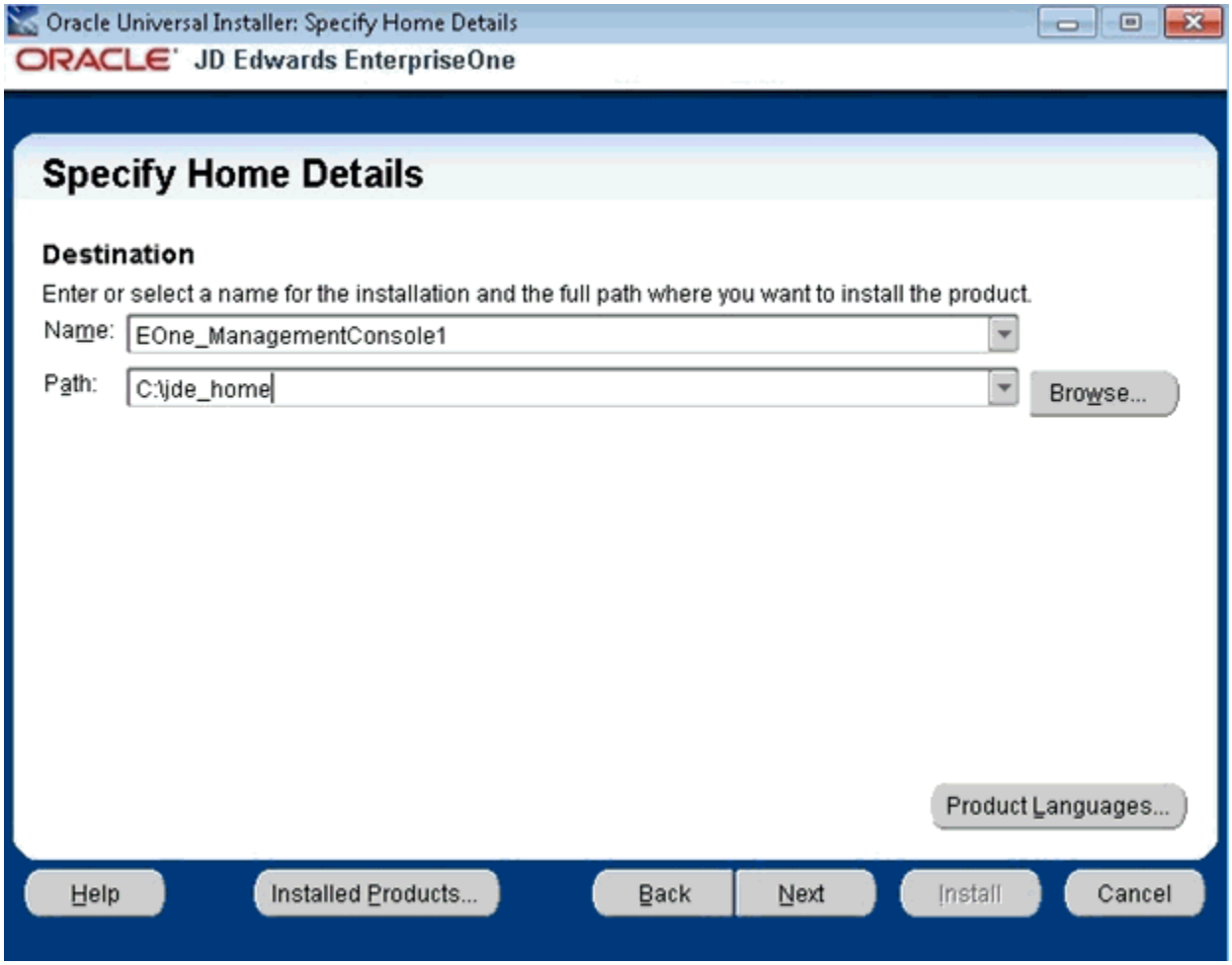
The Windows Command window starts indicating that Windows is preparing to launch the Oracle Universal Installer for the Server Manager Management Console.

Figure 3–19 Welcome Screen



3. On Welcome, click the Next button.

Figure 3–20 Specify Home Details



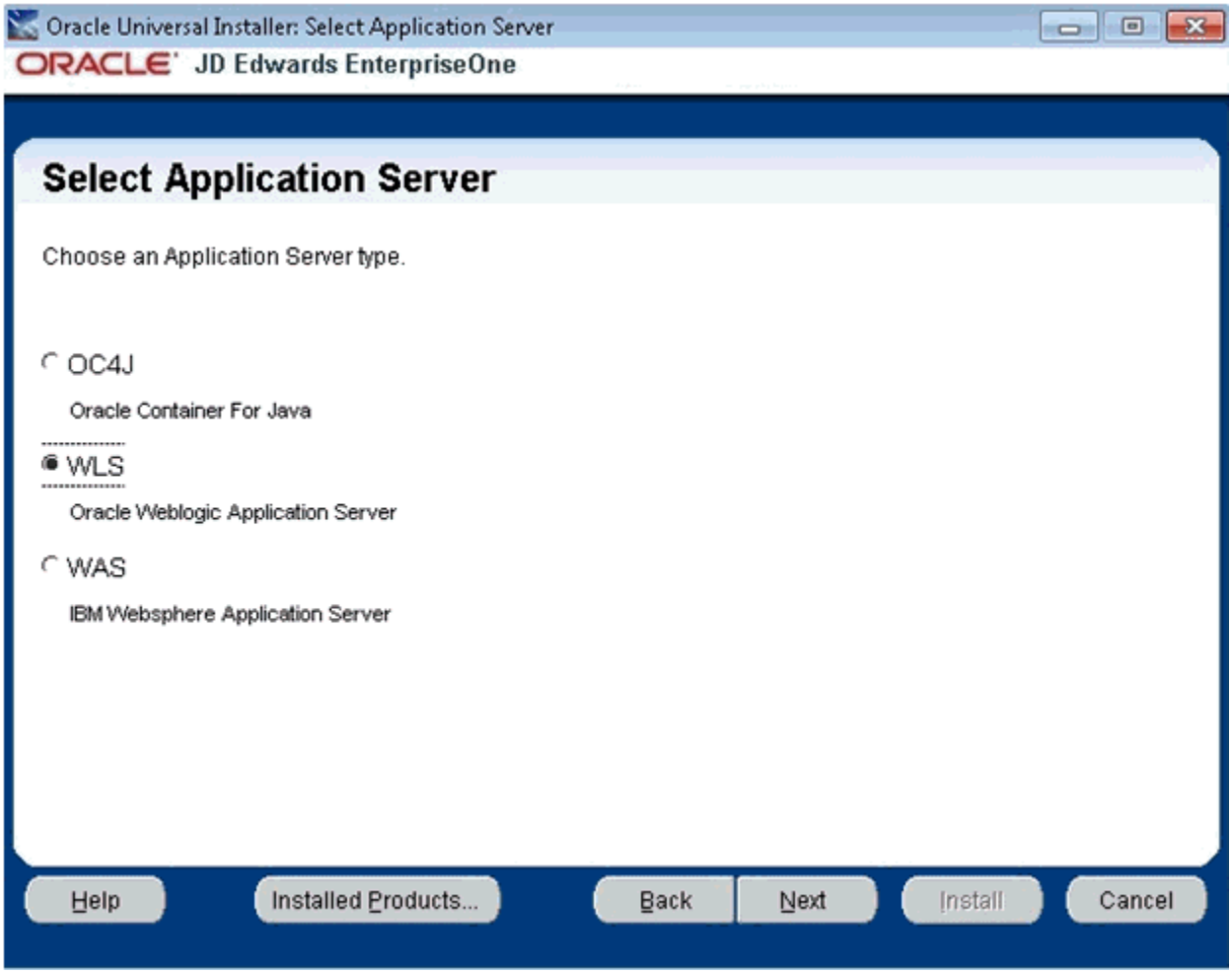
4. On Specify Home Details, complete the **Name** field.

   On Specify Home Details, complete the Name field.

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

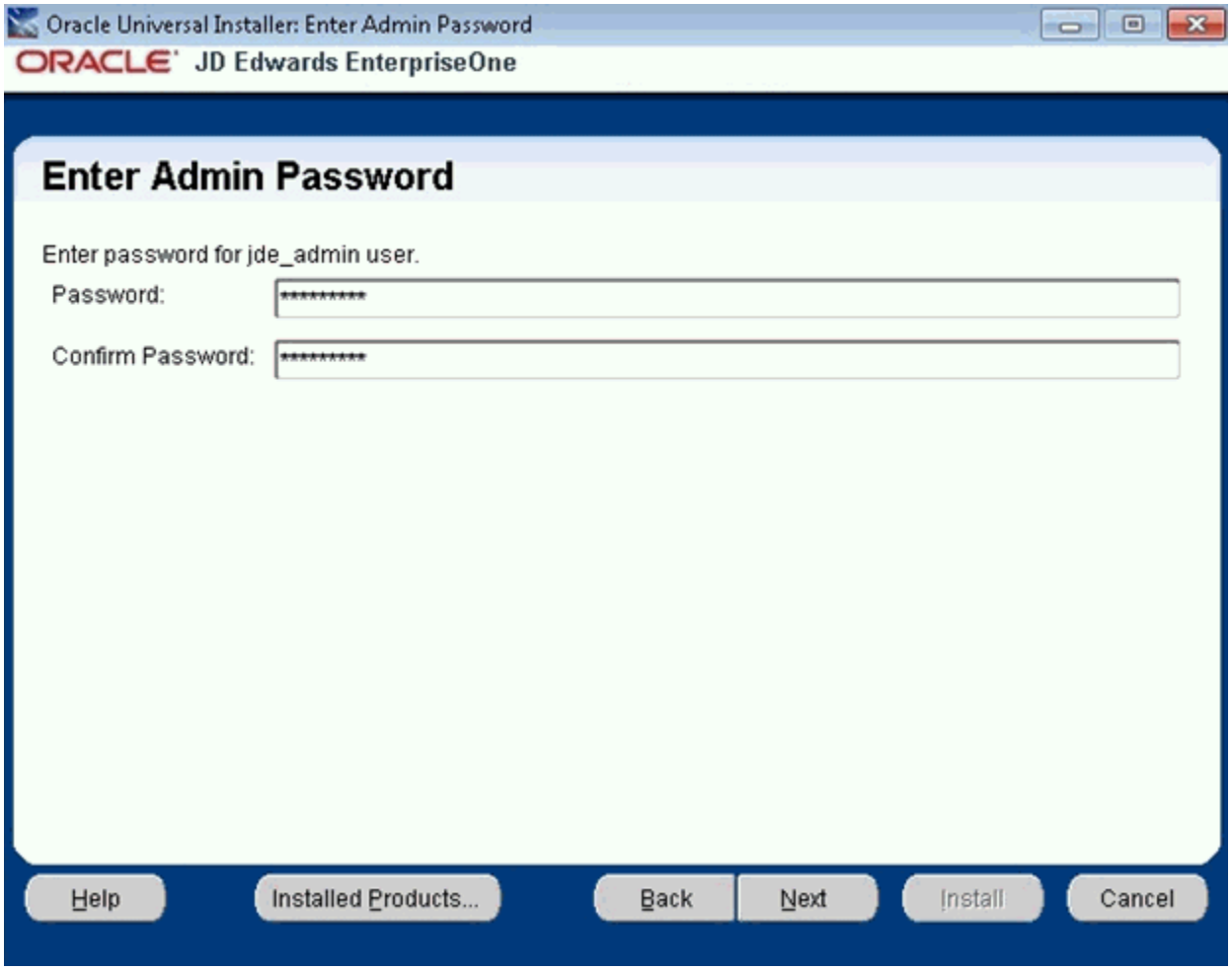
> **Note:** If there is an existing installation of the Management Console with the default name, the installer will append the default name with a number to make it unique. For example, EOne_ManagementConsole1.

Figure 3–21 Select Application Server



5. On Select Application Server, select the **WLS** radio button.
6. Click the Next button.

Figure 3–22 Enter Admin Password



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: ! @ # $ _

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.

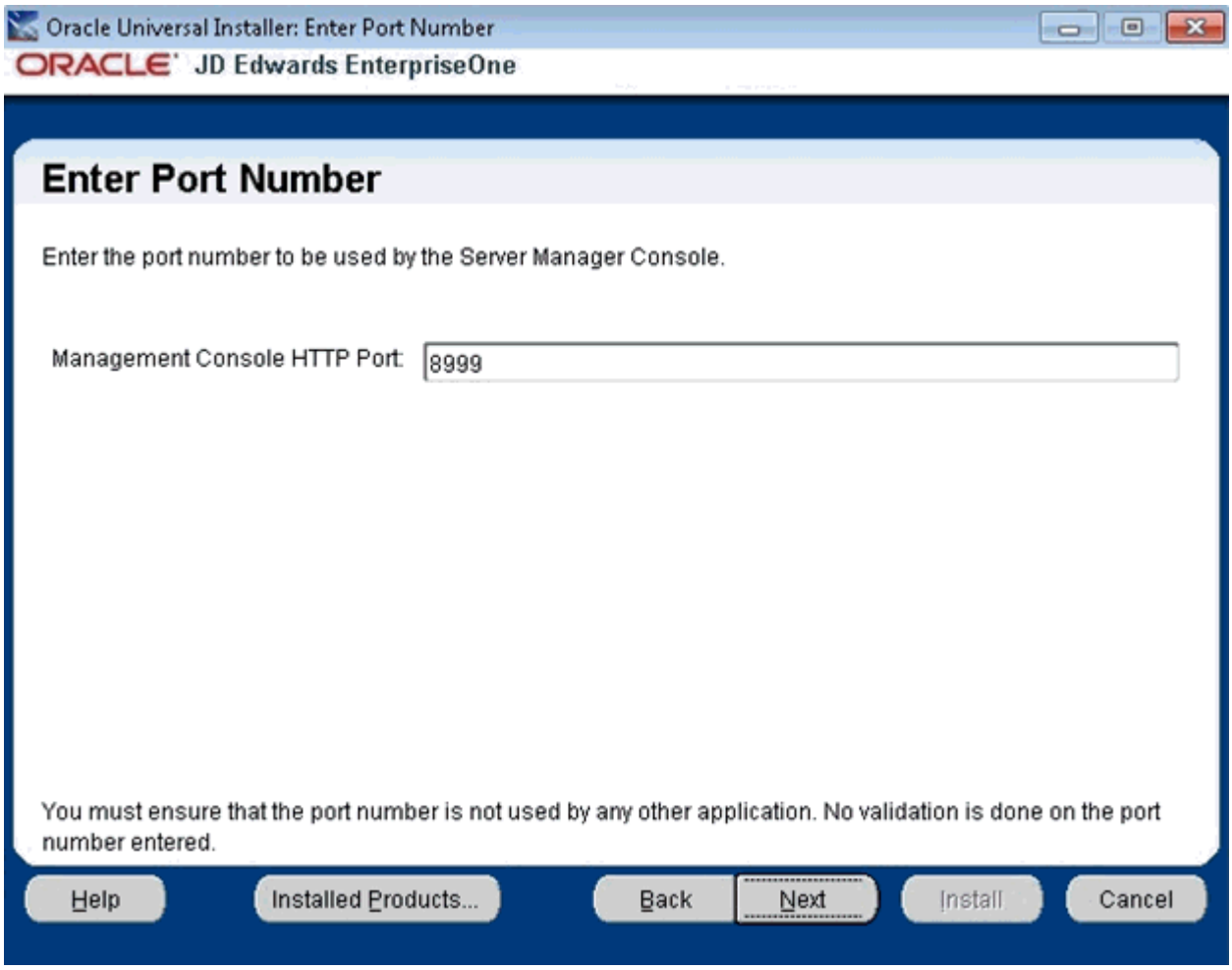
Caution: Because there is no programmatic way to retrieve a lost or forgotten password, it is critical that you remember and safeguard this password. If the password is forgotten or lost, the only recovery is a complete reinstallation of Server Manager.

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.

Figure 3–23 Enter Port Number



9. On Enter Port Number, complete the **Management Console HTTP Port** field.

   Enter the port on which the previous Server Manager Console was installed. Assume that the previous server manager was installed on port 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.

10. Click the Next button.

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

    - Install Directory

      Enter the path to the WebLogic installation directory (wlserver).

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

      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: **DNDEDASVM4**

    - Node Manager Machine Name

      Enter the logical name of the nodemanager machine associated with the domain. This is not the physical machine name.

    - 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.

    - Admin User Name

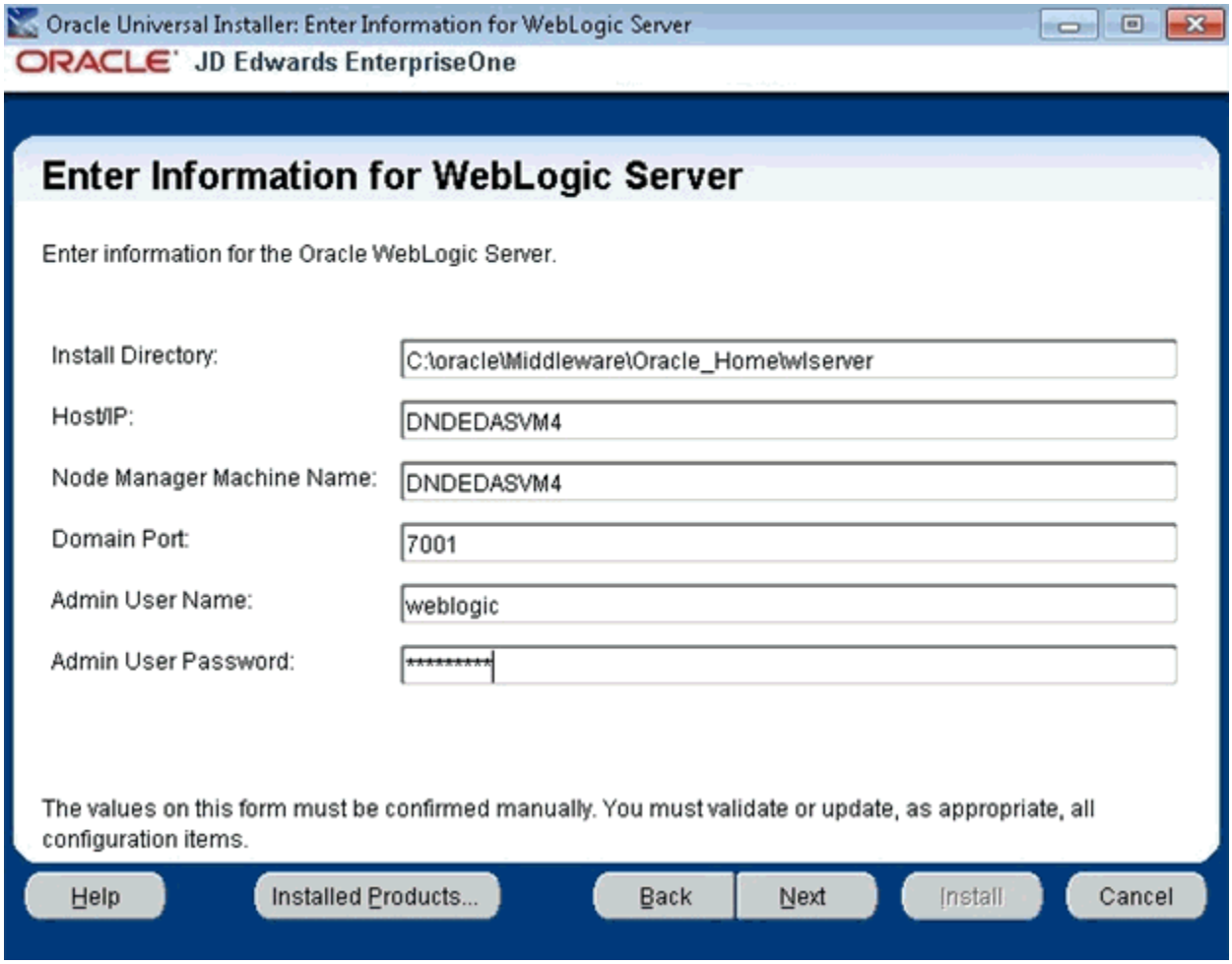
      Enter the user name of the WebLogic Server admin account.

    - Admin User Password

      Enter the password for the WebLogic Server admin account.

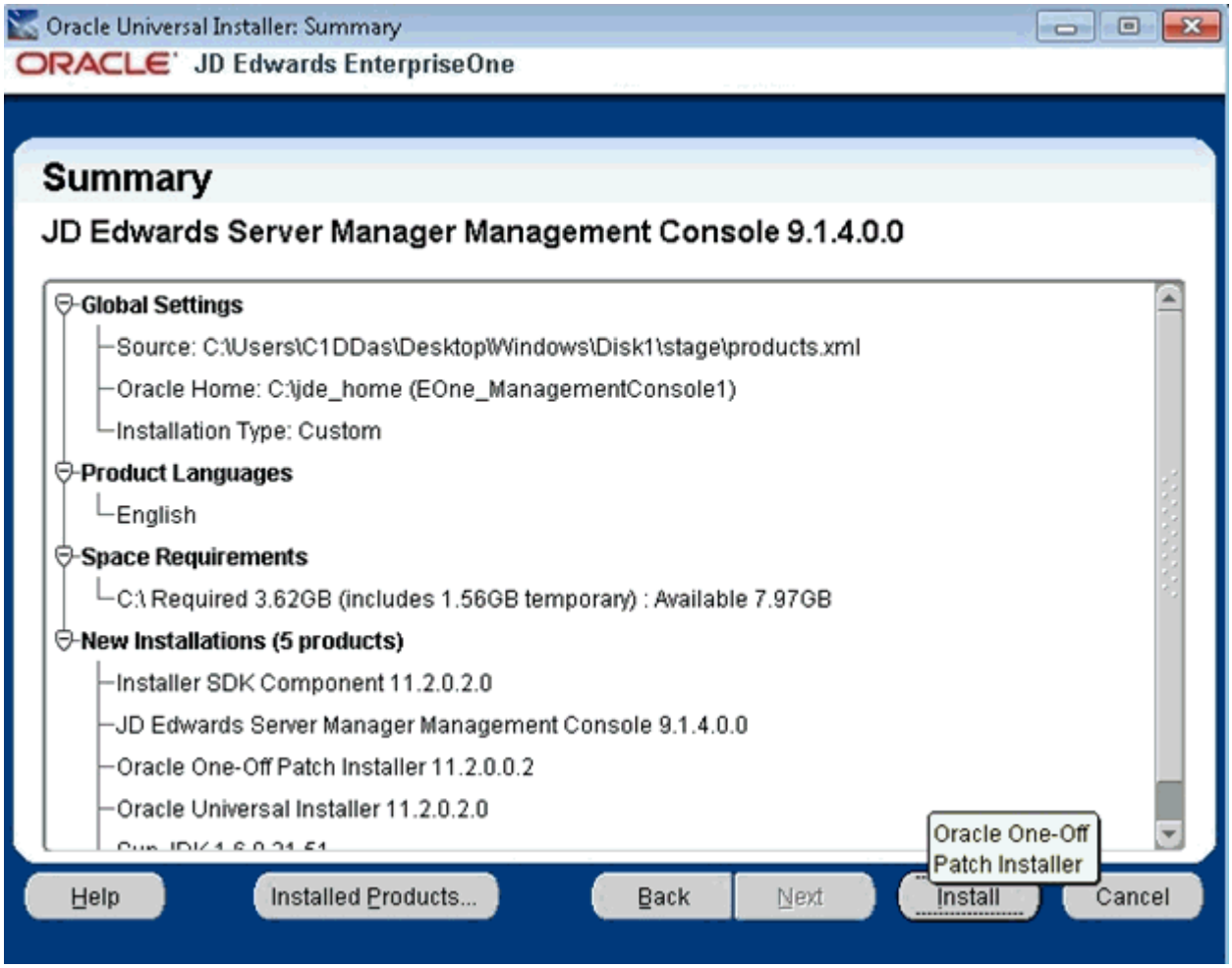
      Caution: The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items. If you enter invalid values, you will have to re-run the installer with the correct values.

Figure 3–24 Enter Information for WebLogic Server



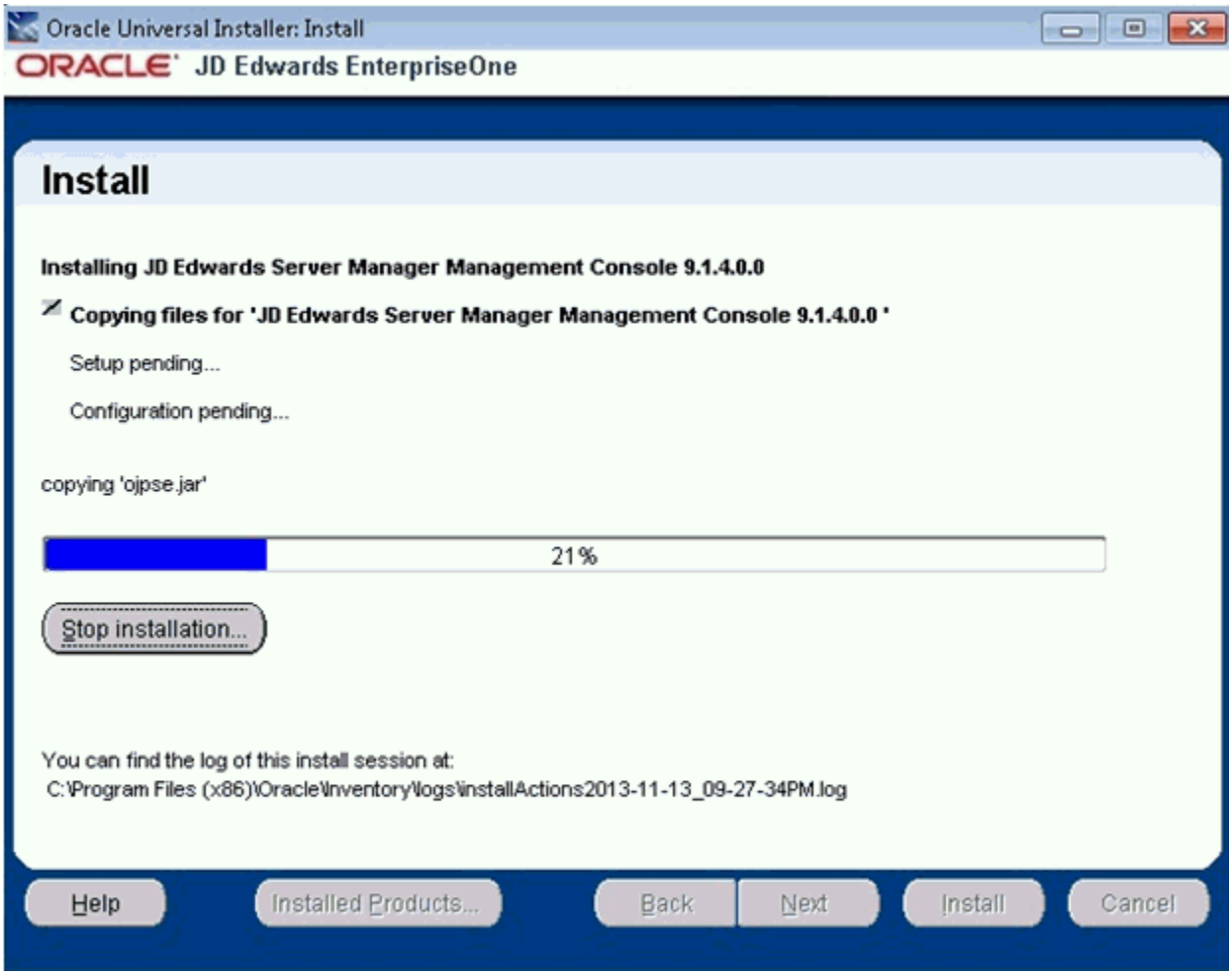
12. Click the Next button.

Figure 3–25 Summary



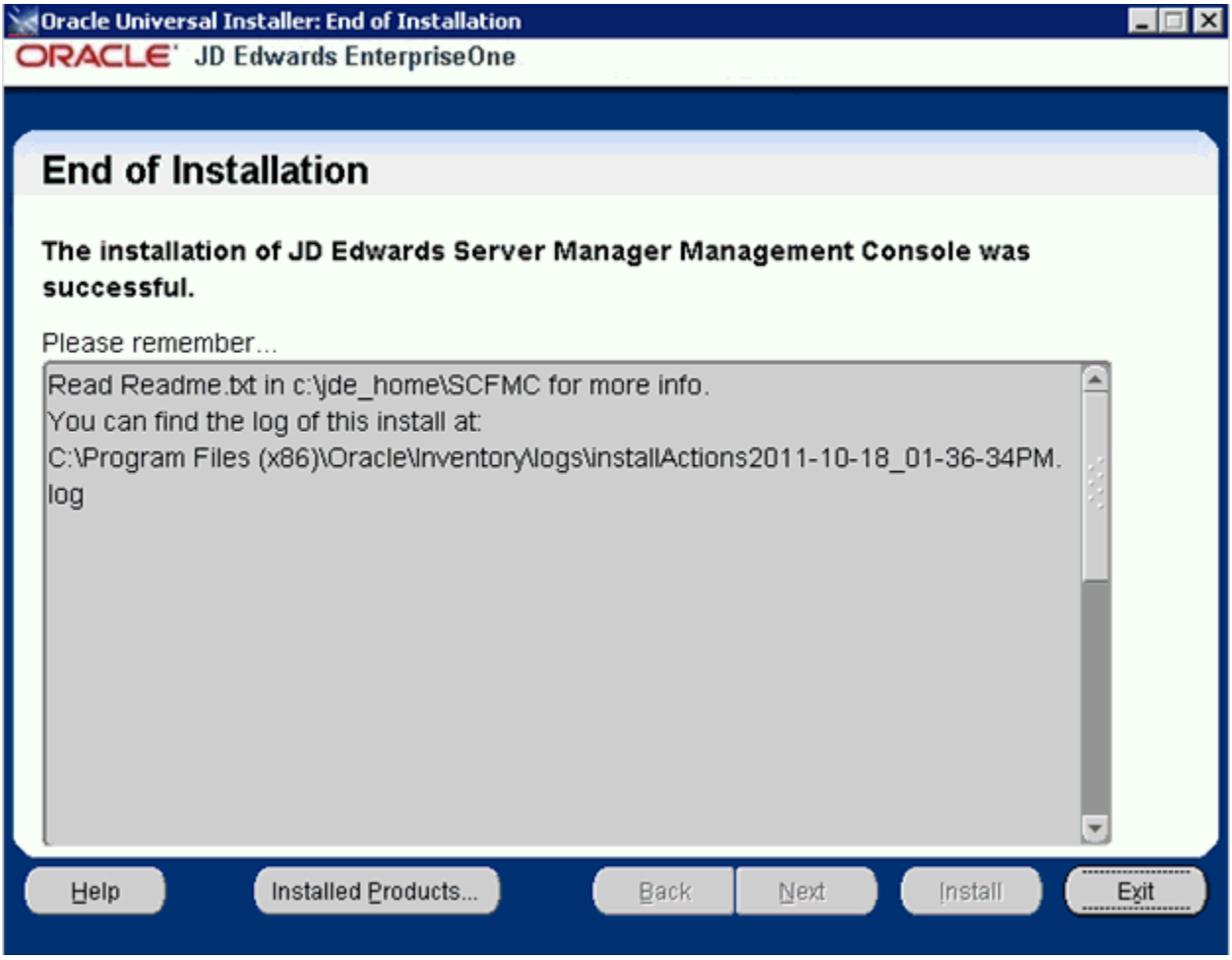
13. On Summary, verify your selections and click the Install button to begin the installation.

Figure 3–26 Install



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

Figure 3–27 End of Installation



14. On End of Installation, verify the installation was successful.
15. Click Exit to exit the Oracle Universal Installer for the Server Manager Management Console.

Figure 3–28 Exit

16. On the Exit dialog, click the Yes button.

3.9.5 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.

3.10 Manually Installing a JDK or JRE on AIX

For AIX platforms running the Server Manager agent, the agent java version must be upgraded manually in order for the agent to continue communicating with the Management Console.

To manually update the java version:

1. Download and install a 1.6 JDK or JRE to the AIX machine to be upgraded.
2. On the AIX machine running the Server Manager agent to be upgraded, sign on as the user that owns the Server Manager directory structure.
3. Stop the Server Manager agent using the {agent-home}/bin/stopAgent script.
4. Locate the directory named "jdk" under the installation location for the Server Manager agent.
5. Rename the "jdk" directory to "jdk_original".
6. Copy the 1.6 JDK directory to the Server Manager agent install location. Make sure the new directory is named 'jdk'. Alternately, you can create a soft link named 'jdk' from the Server Manager agent install location to the 1.6 JDK.
7. Start the Server Manager agent using the {agent-home}/bin/startAgent script.

At this point the Server Manager agent should be able to communicate with the Server Manager console. You can now update the Server Manager agent version normally.

3.11 Deinstall the Server Manager Management Console for Tools Release 9.1

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

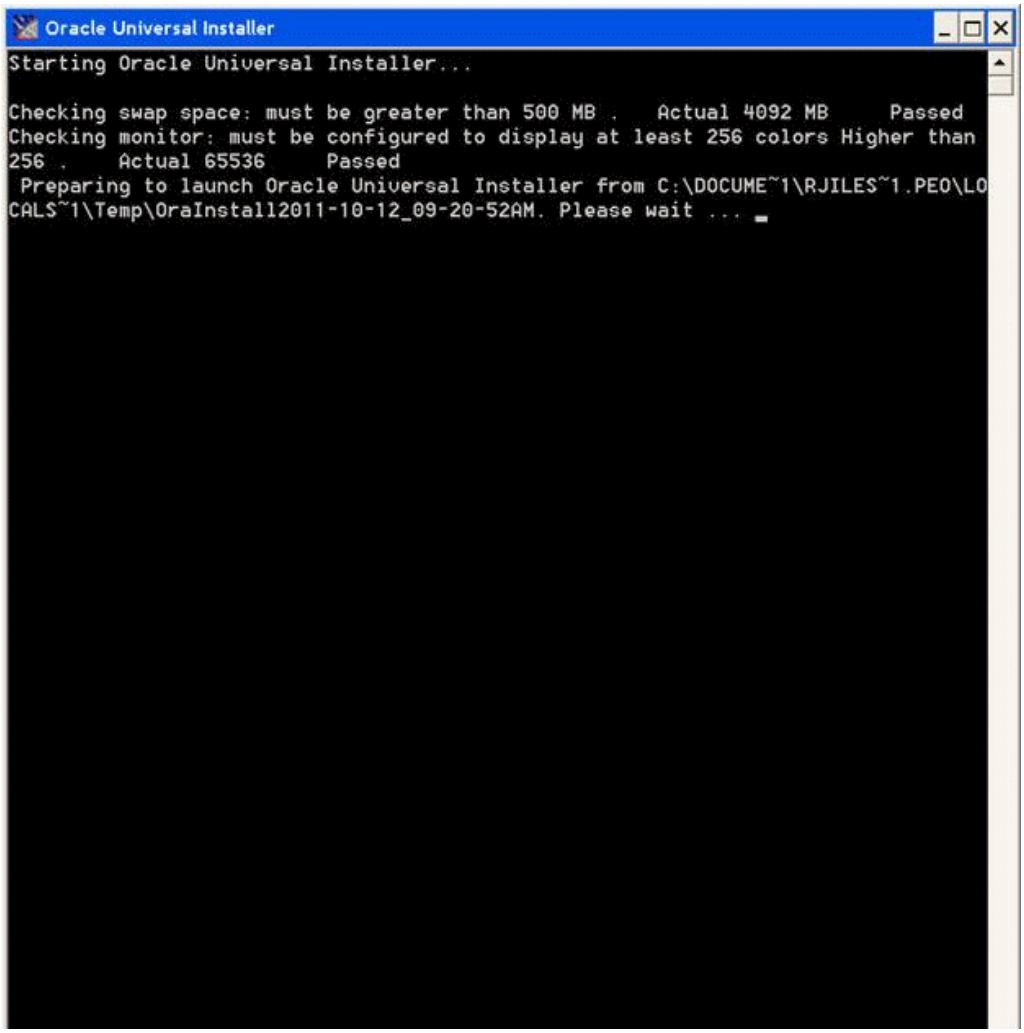
Ensure the Administration Server (or deployment manager) of the WAS Profile is running.

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.

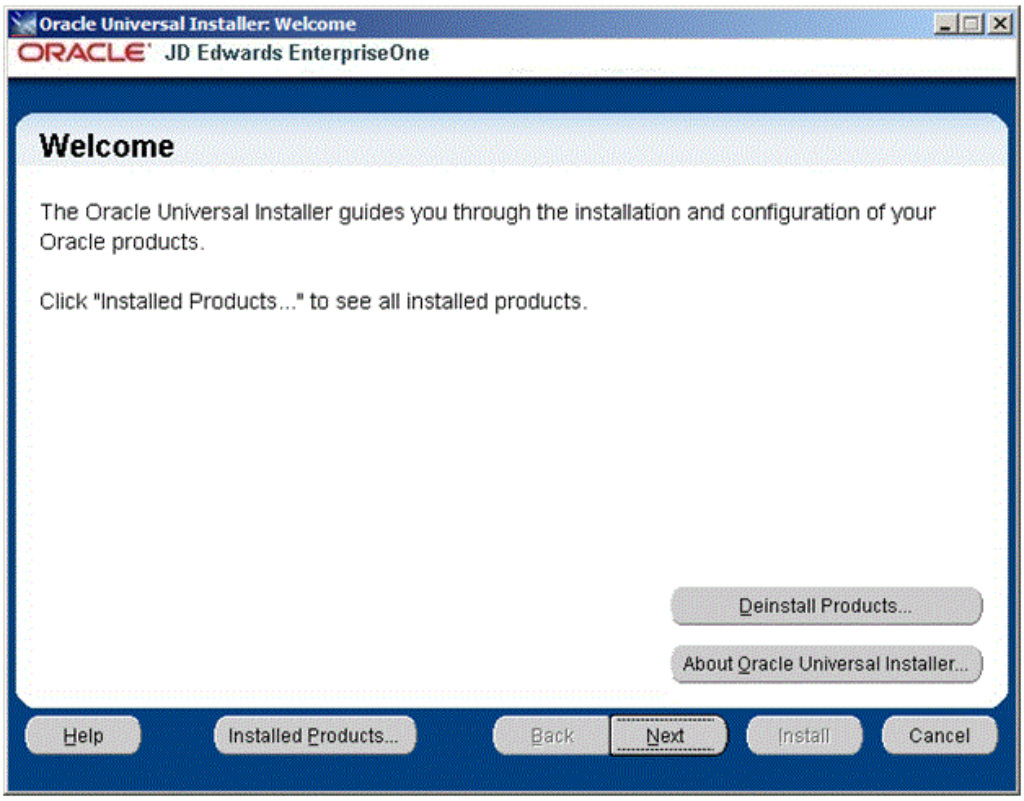


   Linux and Solaris

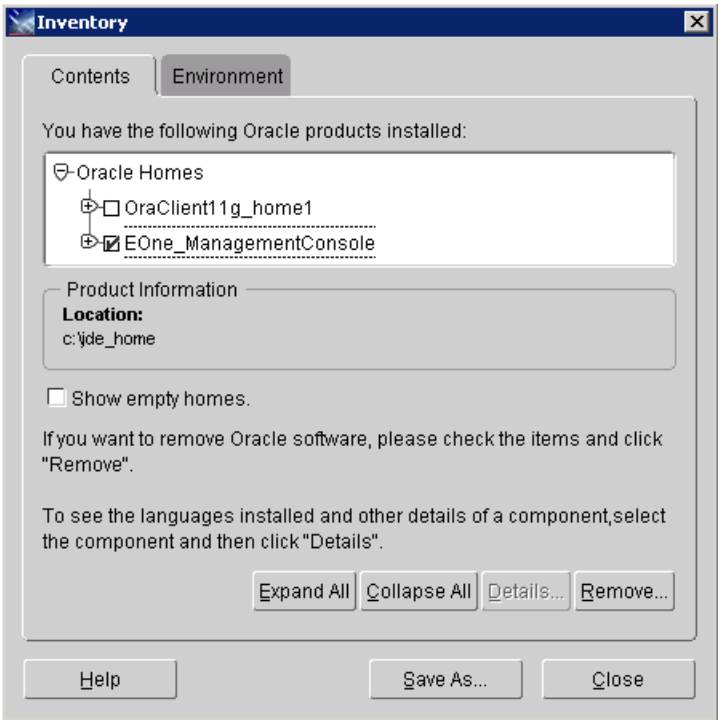
You can invoke the deinstaller/uninstaller by re-running the Server Manager Console installer. If the installer software has been deleted, you can still launch it using this command:

```
$ORACLE_HOME/oui/runInstaller
```

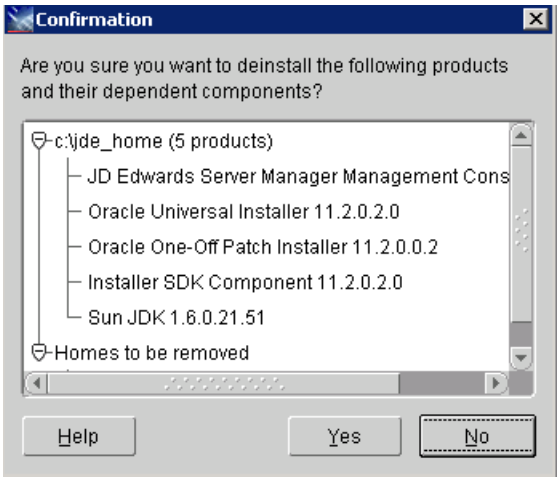
It will take a minute or so for the initialization to complete. Upon completion the OUI Welcome panel displays:



2. On Welcome, click the **Deinstall Products …** button.

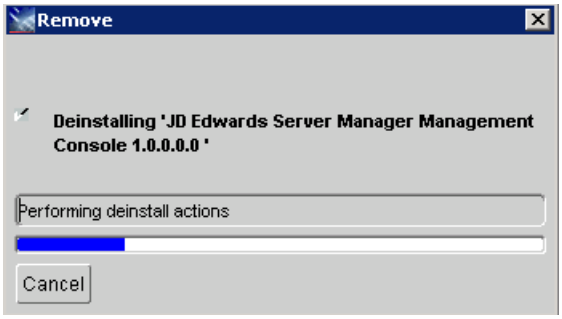


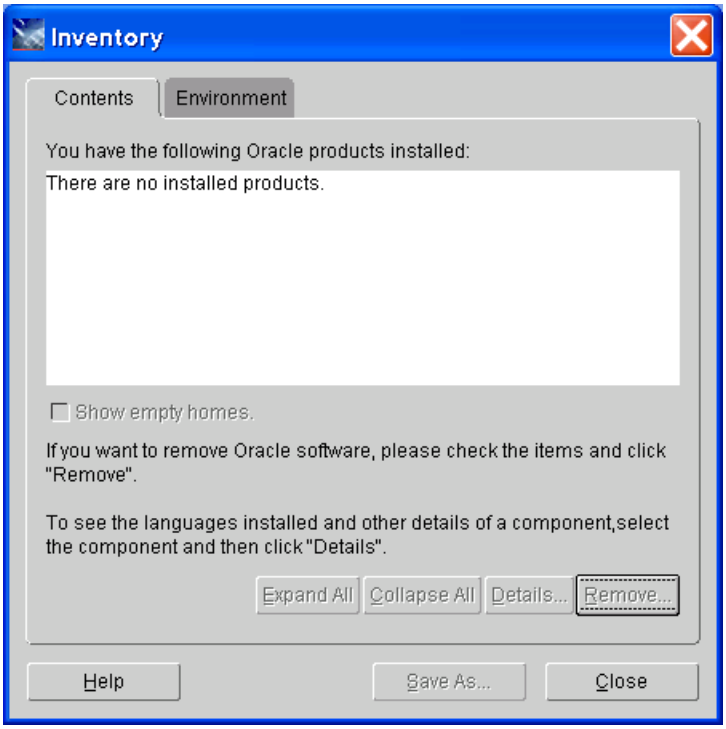
3. On Inventory, select the node under Oracle Homes that corresponds to your Server Manager Management Console installation. For example: EOne_ManagementConsole
4. Once the component to be deinstall is selected, verify the **Location** in the **Product Information** portion of the screen.
5. On Inventory, with the Contents tab selected, if the selected Oracle Home is correct, click the **Remove …** button.



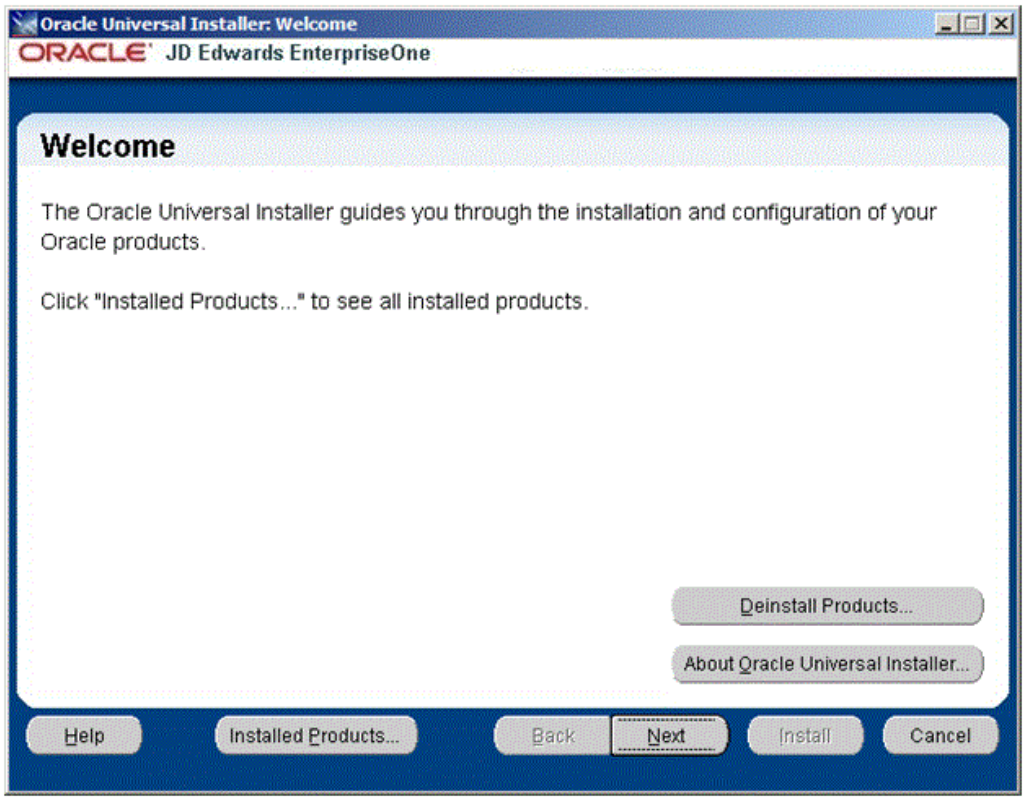
6. On Confirmation, click Yes to begin the deinstallation of the selected Oracle Home.

   The Remove progress dialog is displayed:

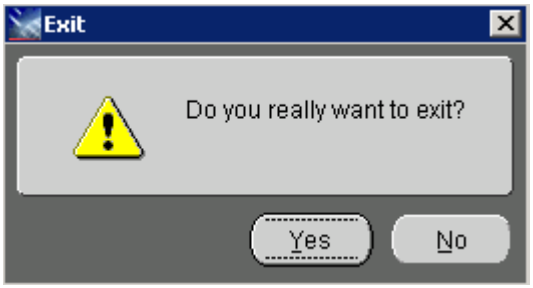




7. On Inventory, verify the selected Oracle Home is no longer displayed.
8. On Inventory, click the Close button.



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.

4

Complete the Management Console Setup Wizard

This chapter discusses:

- Section 4.1, "Access the Management Console"
- Section 4.2, "Run the Management Console Setup Wizard"

4.1 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:

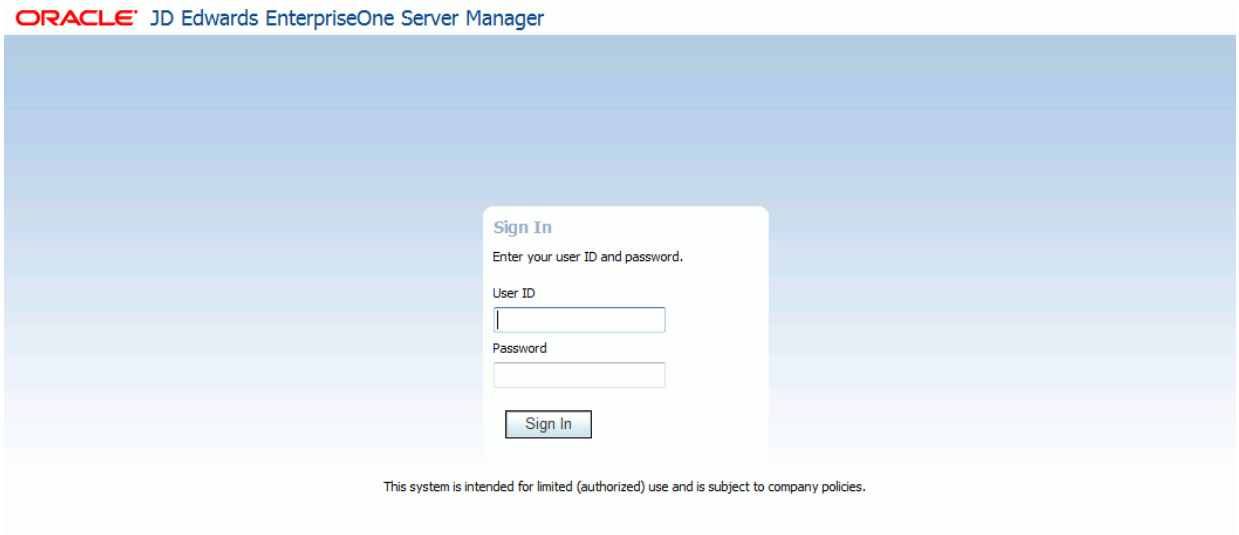
`http://servername:port/manage`

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://denlcmwn5.mlab.jdedwards.com:7000/manage/`



4.2 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:

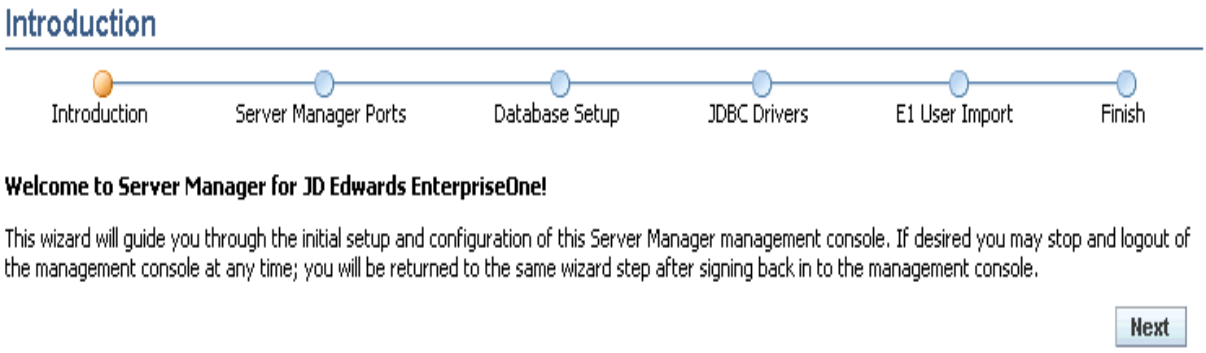
`http://servername:port/manage`

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

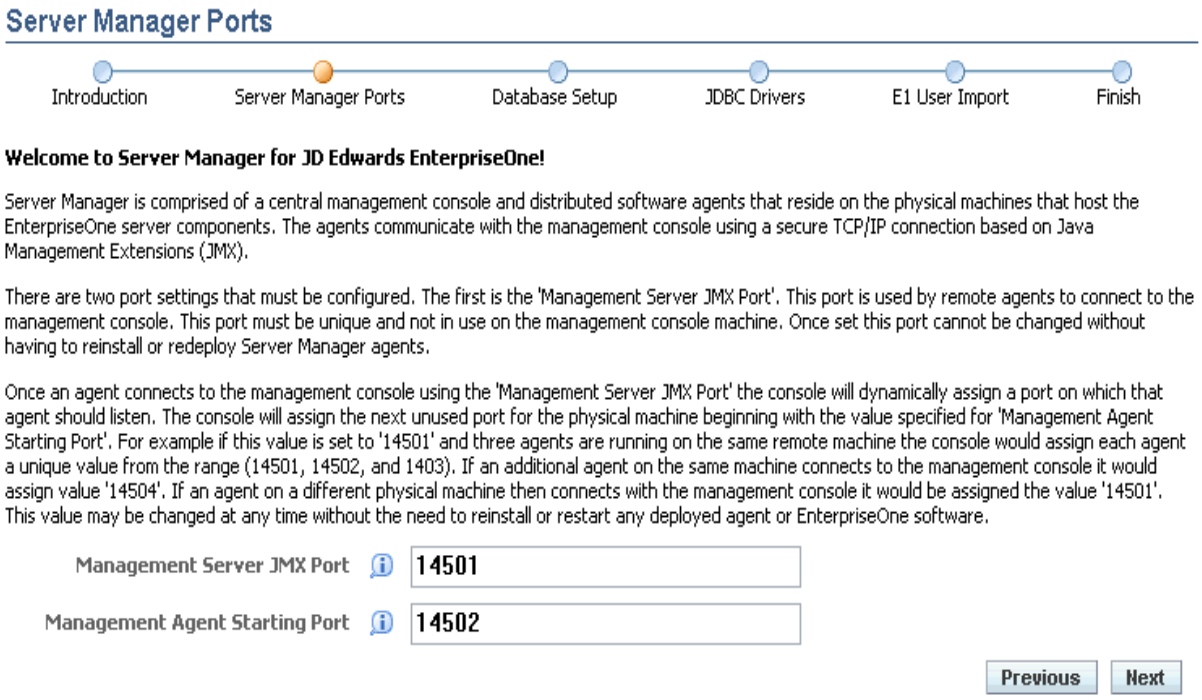
where `port` is the port you specified for the Management Console when you ran the Management Console installer.

For example:

`http://denlcmwn5.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:

   - *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*.

   - *Management Agent Starting Point*

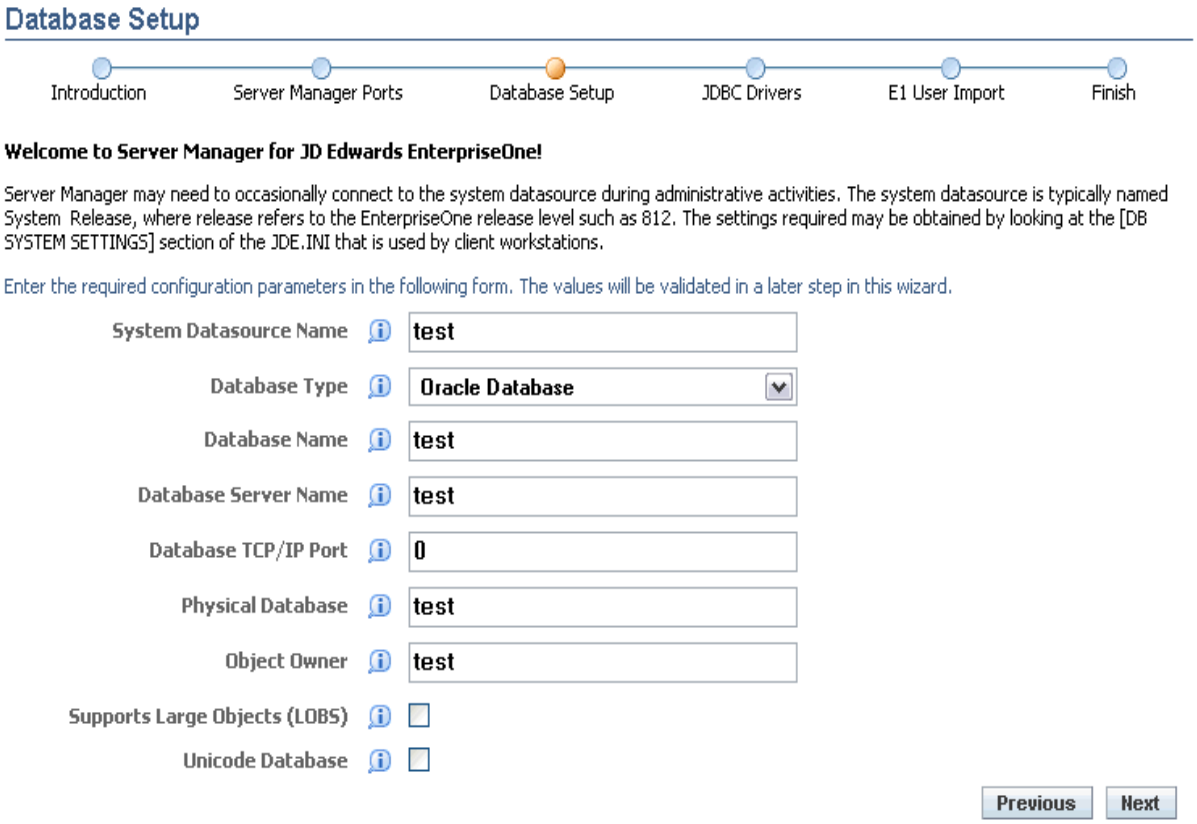
     Once a Management Agent connects to the Management Console using the *Management Server JMX Port*, the Management Console dynamically assigns a port on which that Management Agent should listen. The Management Console assigns the next unused port for the physical machine beginning with the value specified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

     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.

Tip: This document does not discuss changing the Management Agent Starting Port after installation, but it can be done through reading how to change http port in a standalone OC4J. The OC4J user guide is delivered with the Server Manager installation. An example location is:

```
c:\jde_
home\targets\oc4j\j2ee\home\default-web-app\oc4jusersguide.p
df
```

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 Web Development Client workstations (sometimes referred to as fat clients).

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

   - *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.

- *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.

- *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.

- *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.

- *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.

- *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 entitled: Chapter 12, "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:

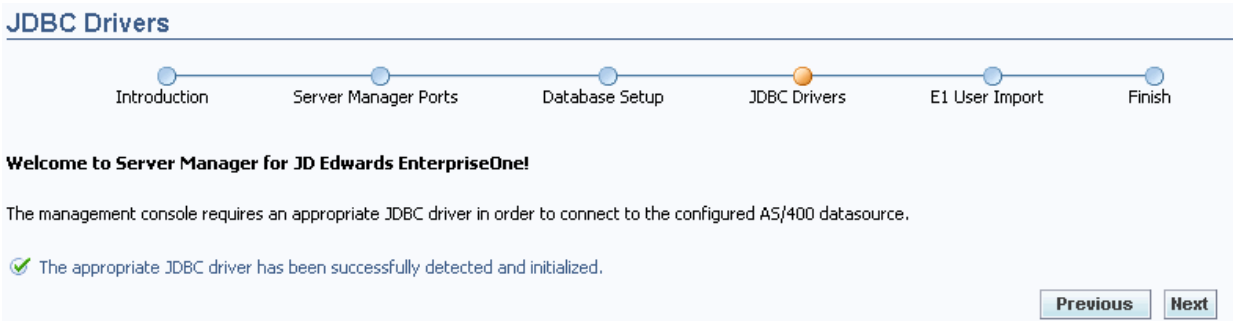
   AS400, see Substep a

   Oracle database, see Substep b

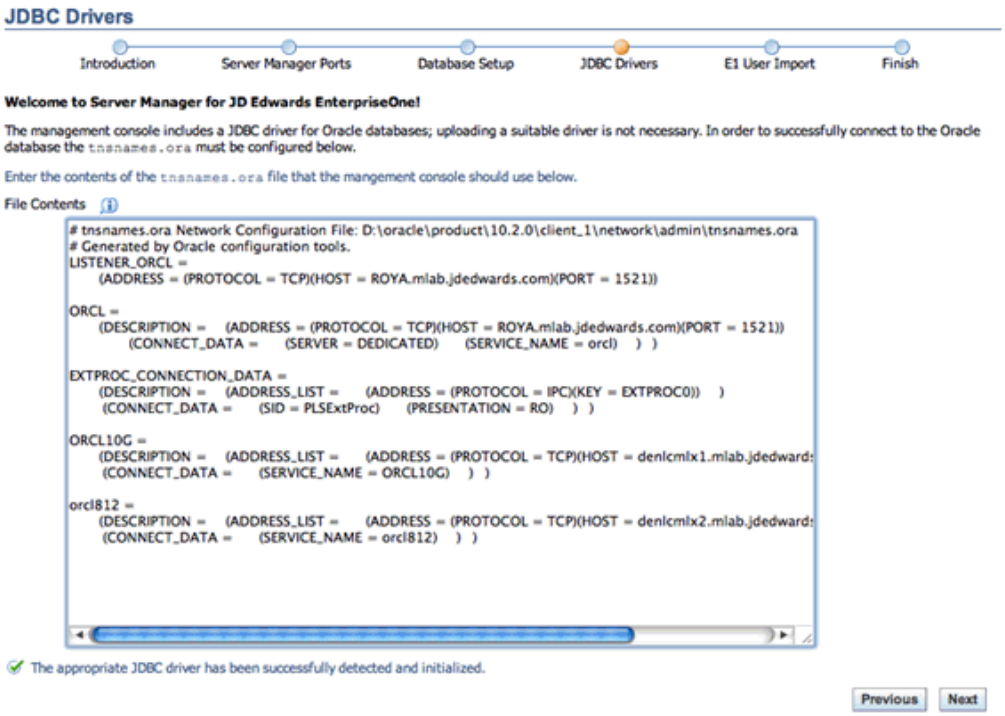
   MS SQL Server, see Substep c

   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:

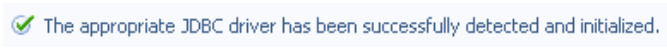


Tip: You can cut and paste the contents of the `tnsnames.ora` file from the JD Edwards EnterpriseOne Web Development Client into this form.

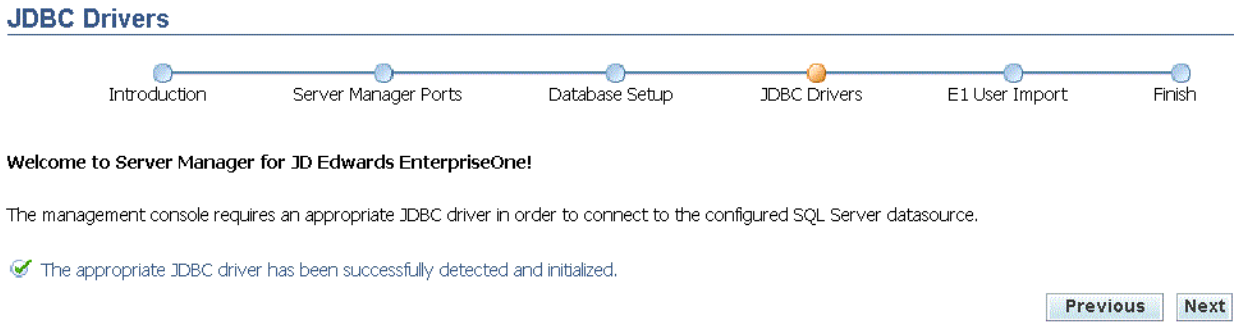
c. For Microsoft SQL Server, you are initially prompted to uploaded the `sqljdbc4.jar` file.

Note: Depending on the value that you enter for *Database Type*, the wizard chooses the appropriate next screen for JDBC Drivers.

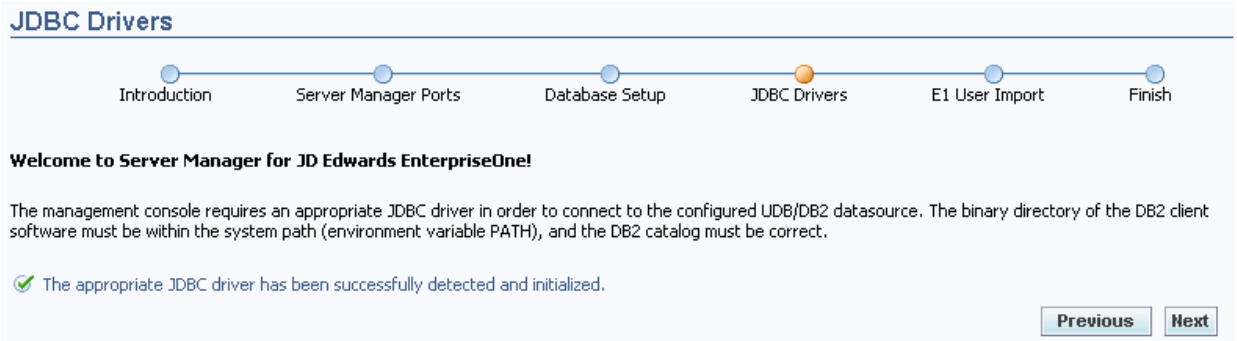
If the Management Console displays this message, you have already uploaded the appropriate driver and proceed to Step 8



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.

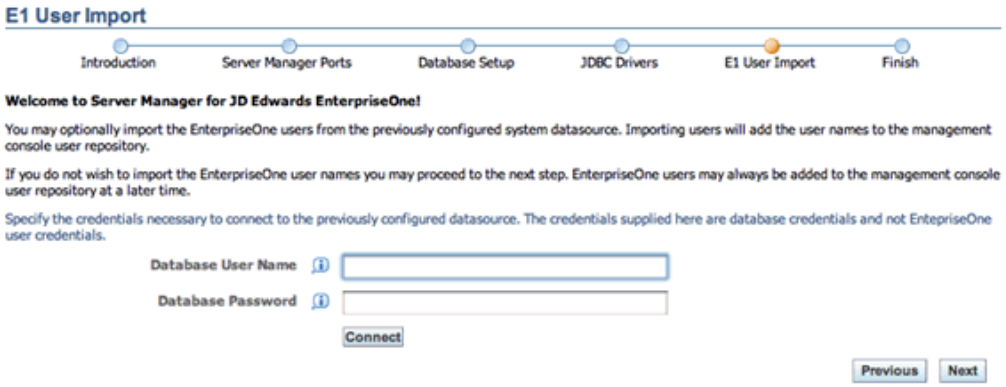


d. For IBM UDB, once the Database Setup and JDBC Drivers forms are properly completed, the last page on the JDBC Drivers portion of the wizard is displayed indicating that the appropriate JDBC driver has been successfully detected and initialized:



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 Chapter 10, "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.

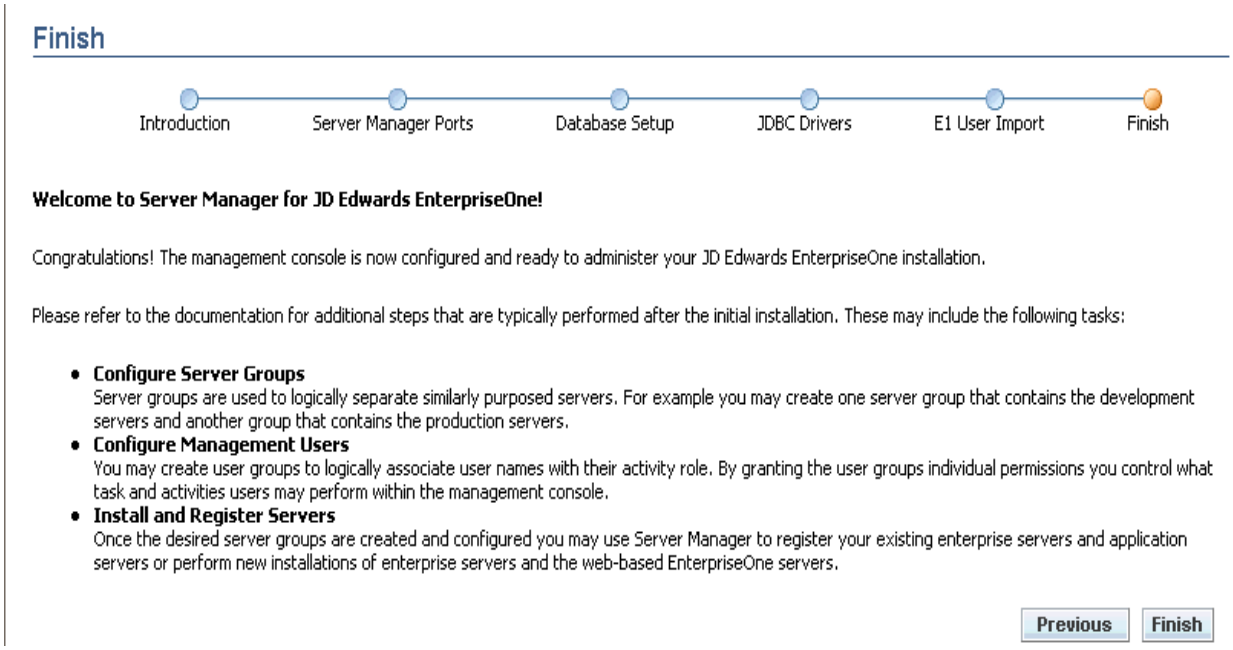
- *Database User Name*

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

- *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:

    - 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 this guide entitled: Administer Server Groups.

    - 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 this guide entitled: Administer Management Console Users and User Groups.

    - 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 this 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.

5

Install a Management Agent

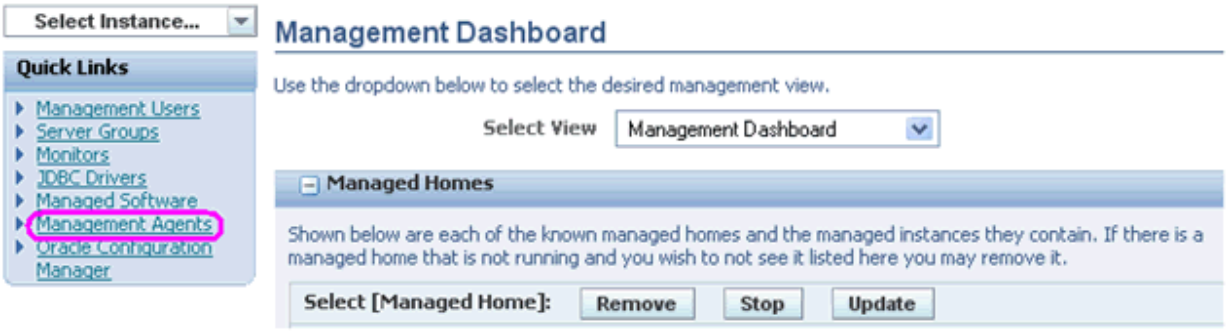
This chapter discusses:

- Section 5.1, "Obtain the Management Agent Installer Application"
- Section 5.2, "Distribute and Unzip the Management Agent Installer Application"
- Section 5.3, "Run the Management Agent Installer"
- Section 5.4, "Post Installation Steps for WebLogic 11g, WebLogic 12c, WebSphere 7.0, or WebSphere 8.5 Web Server Instances"
- Section 5.5, "Troubleshoot the Management Agent Installation"
- Section 5.6, "Deinstall a Management Agent"

5.1 Obtain the Management Agent Installer Application

To obtain the Management Agent Installer application:

1. On Management Dashboard, in the Quick Links section in the left pane, click the *Management Agents* link.



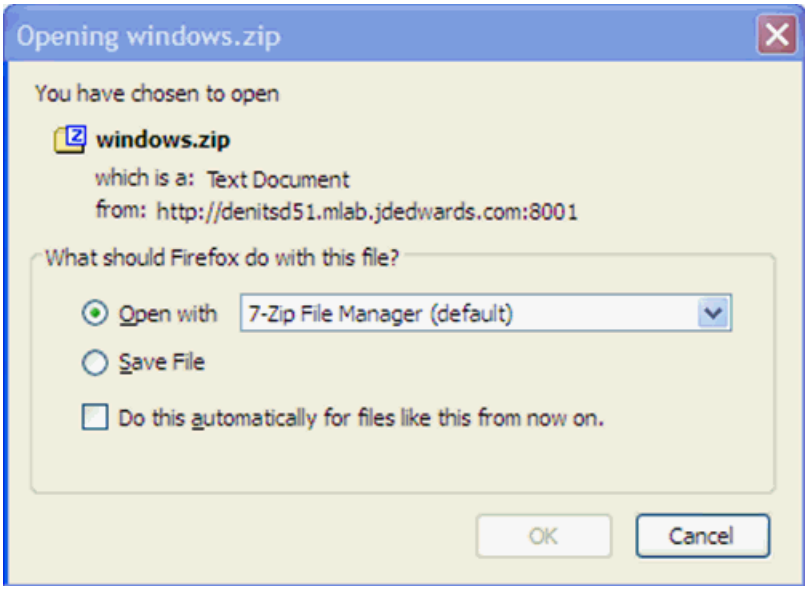
2. On the **Server Manager Agent Downloads** page, navigate to the **Management Agent Installers** section.

3. From the **Management Agent Installers** section, you can select from the available Management Agents, which are listed by operating system:

   - windows
   - linux
   - solaris
   - HP-UX on Itanium (HPIA64)
   - aix
   - 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: Section 5.2, "Distribute and Unzip the Management Agent Installer Application".

5.2 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:

- Section 5.2.1, "Microsoft Windows"
- Section 5.2.2, "UNIX"
- Section 5.2.3, "IBM i (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.

5.2.1 Microsoft Windows

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 Microsoft Windows Explorer with mapped drives:

   `windows.zip`

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

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

5.2.2 UNIX

These are the available versions of UNIX:

- Linux
- Solaris
- AIX
- HP-UX on Itanium (HPIA64) (For Tools Release 9.1 Update 3)

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 (For Tools Release 9.1 Update 3)

`hpia64.zip`

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

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

5.2.3 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, resulting in the following subfolders:

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

5.3 Run the Management Agent Installer

Running the Management Agent installer is platform-dependent:

- Section 5.3.1, "Microsoft Windows"
- Section 5.3.2, "UNIX"
- Section 5.3.3, "IBM i (OS400)"

5.3.1 Microsoft Windows

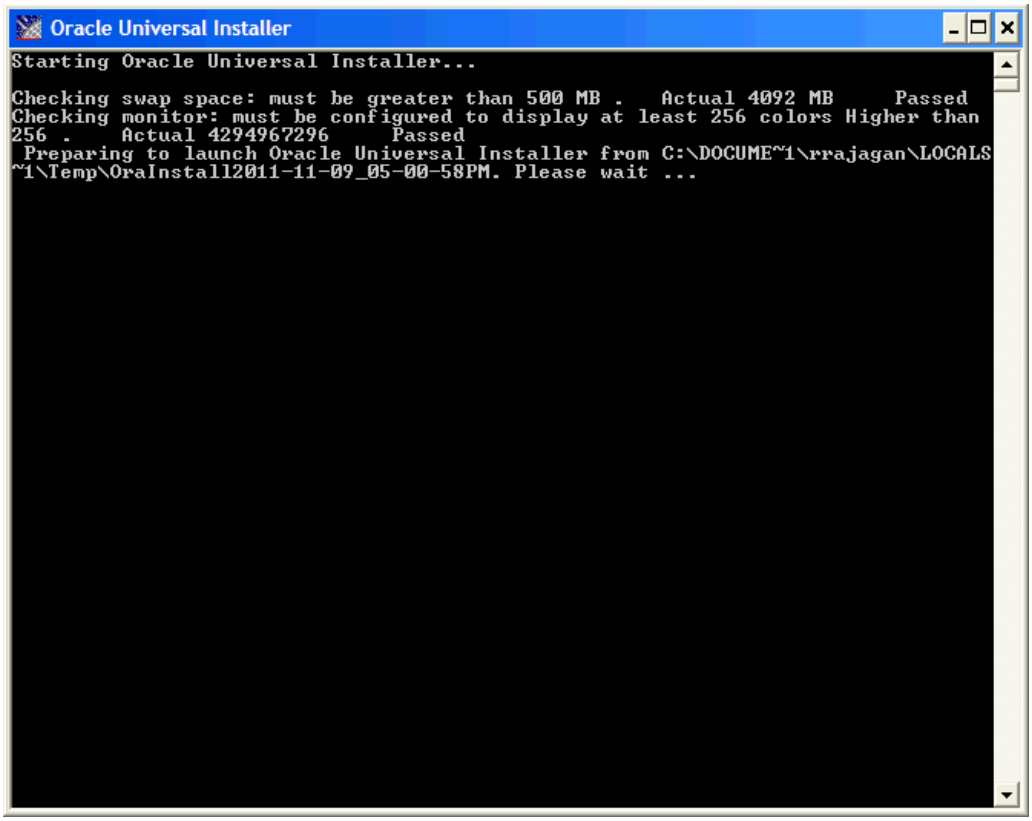
Use this procedure to run the Management Agent installer on Microsoft Windows target machines.

1. Double click this installer file to launch the installer:

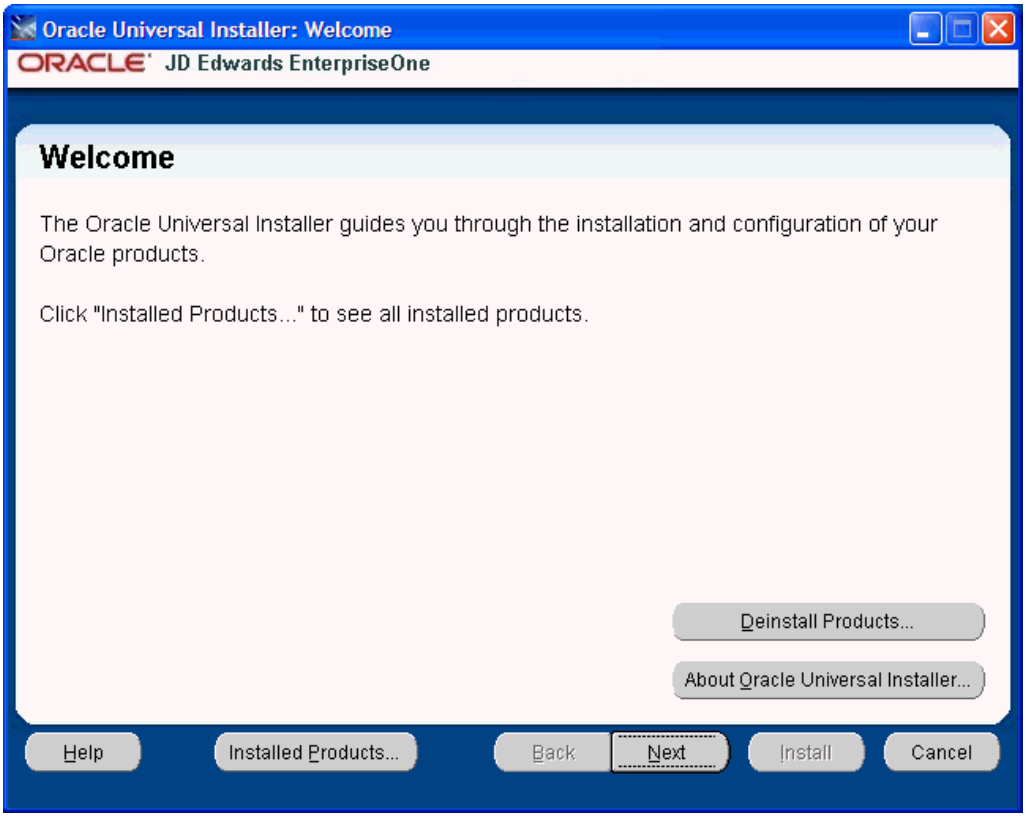
   `\Disk1\install\setup.exe`

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: Microsoft Windows

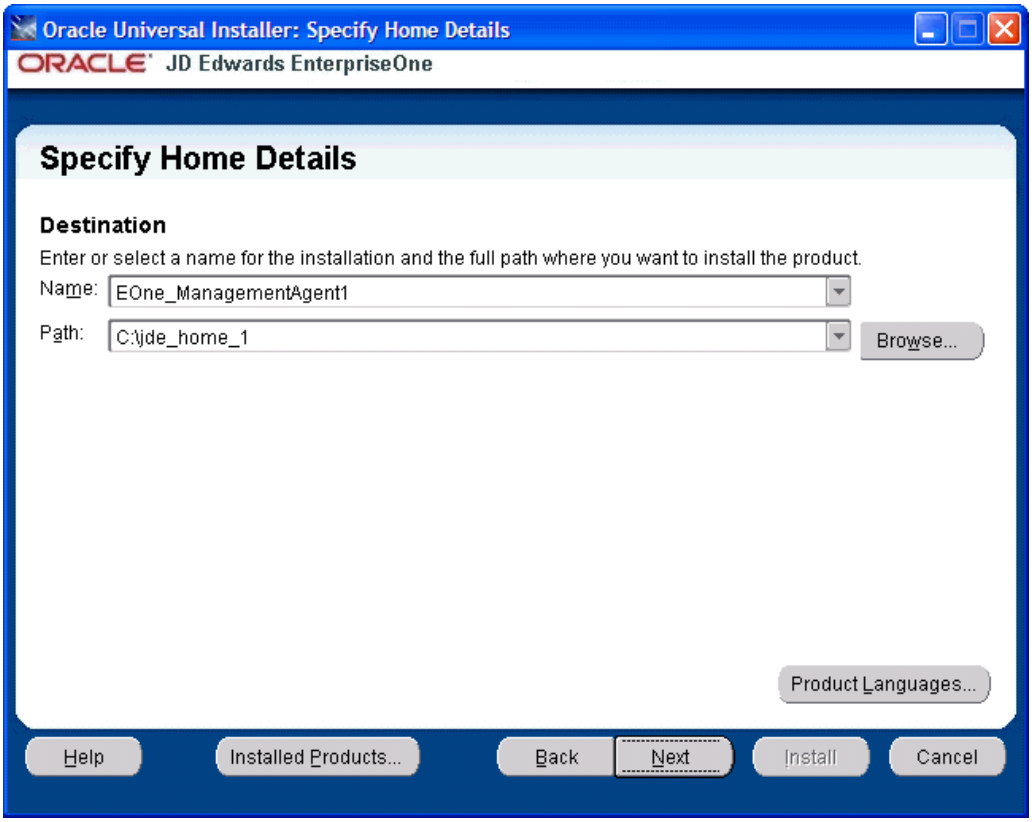
This process opens a Microsoft Windows command window as shown in the below example.



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:

- *Name:*

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

  EOne_Management_Agent

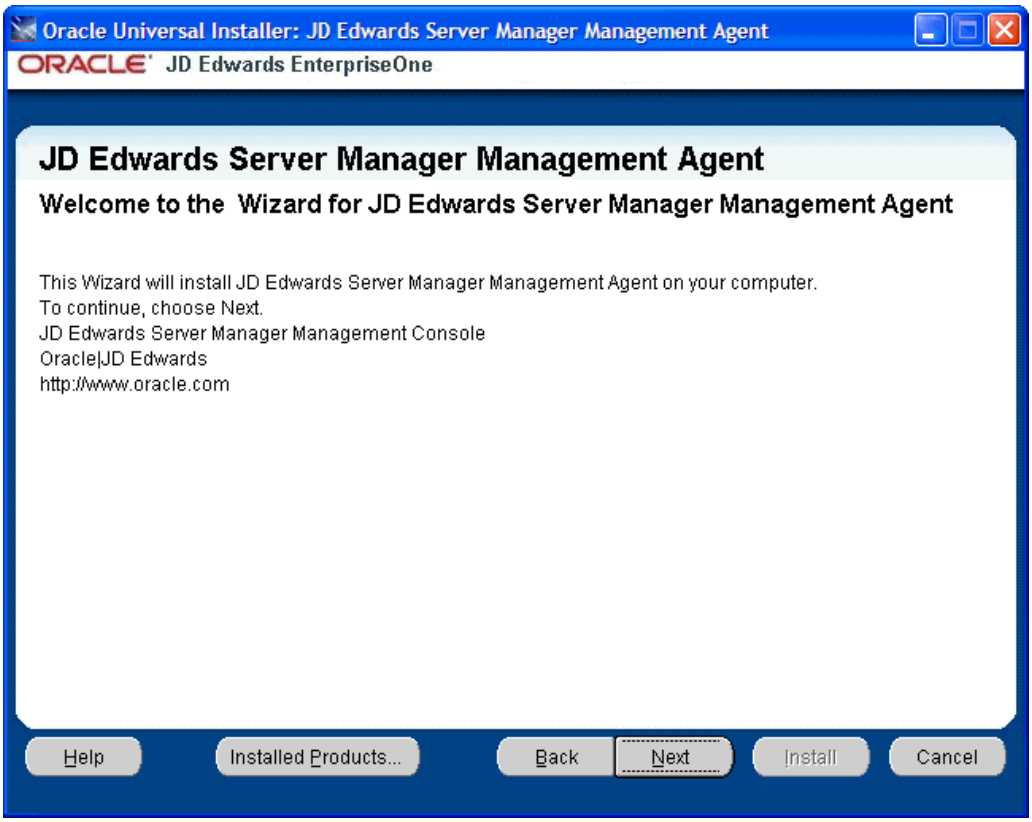
- *Path:*

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

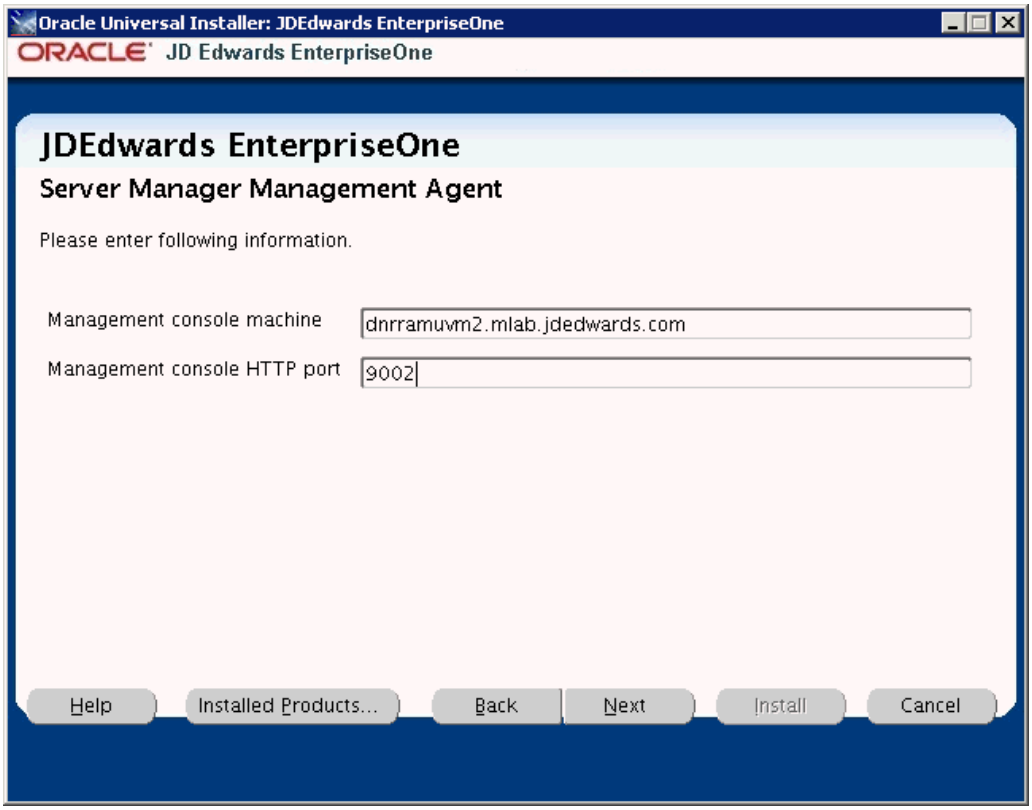
  `jde_home`

  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.



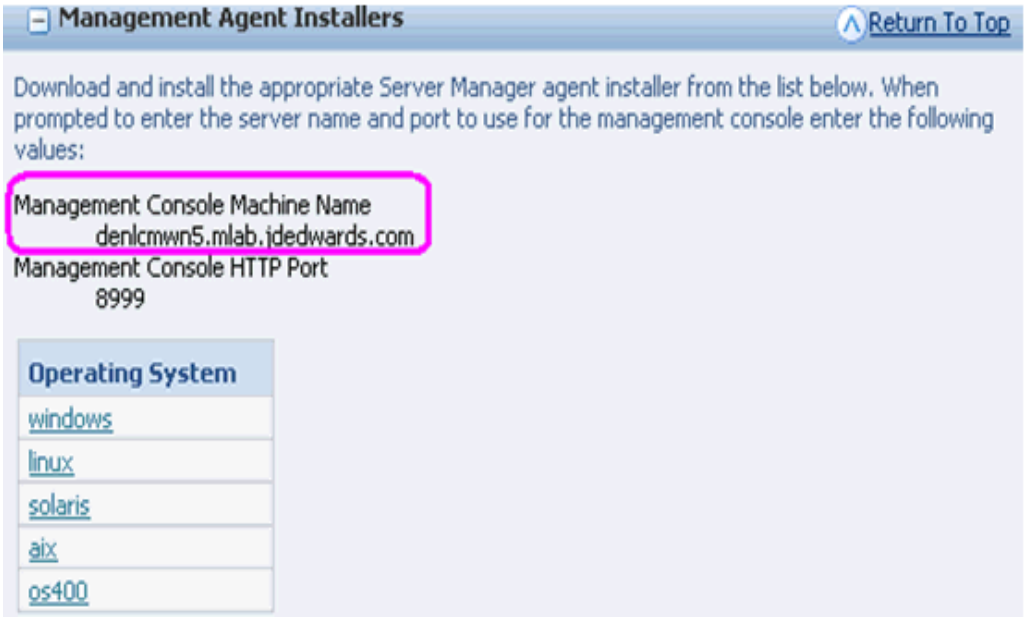
5. On Server Manager Management Agent, complete these fields:

- *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 `dnrramuvm2` you might need to specify`dnrramuvm2.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: Section 5.1, "Obtain the Management Agent Installer Application". You can also view the `readme.txt` file in the root directory of the Management Console.

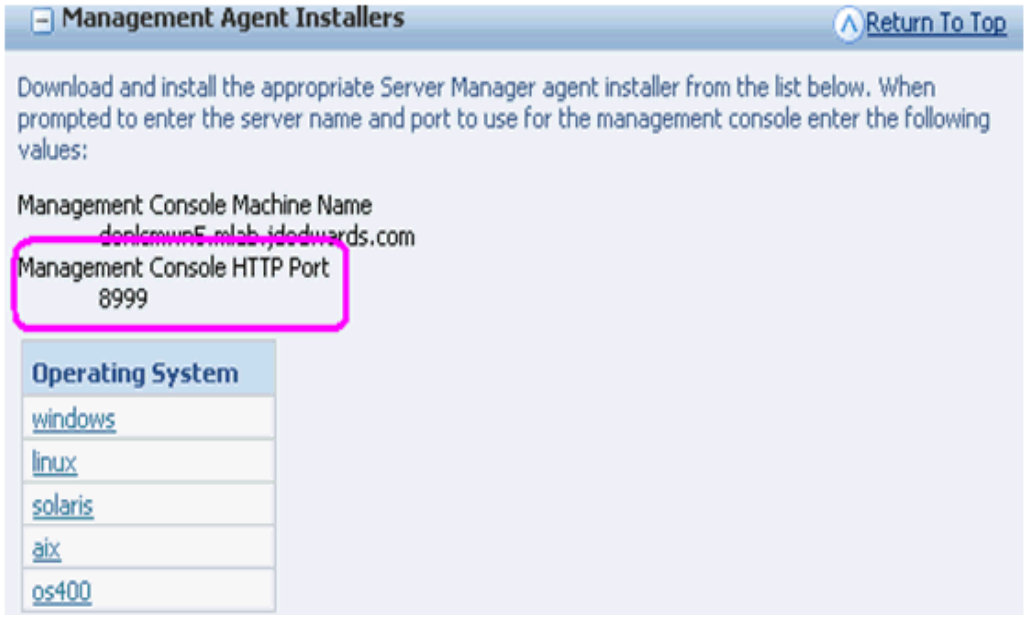


- *Management console HTTP port*

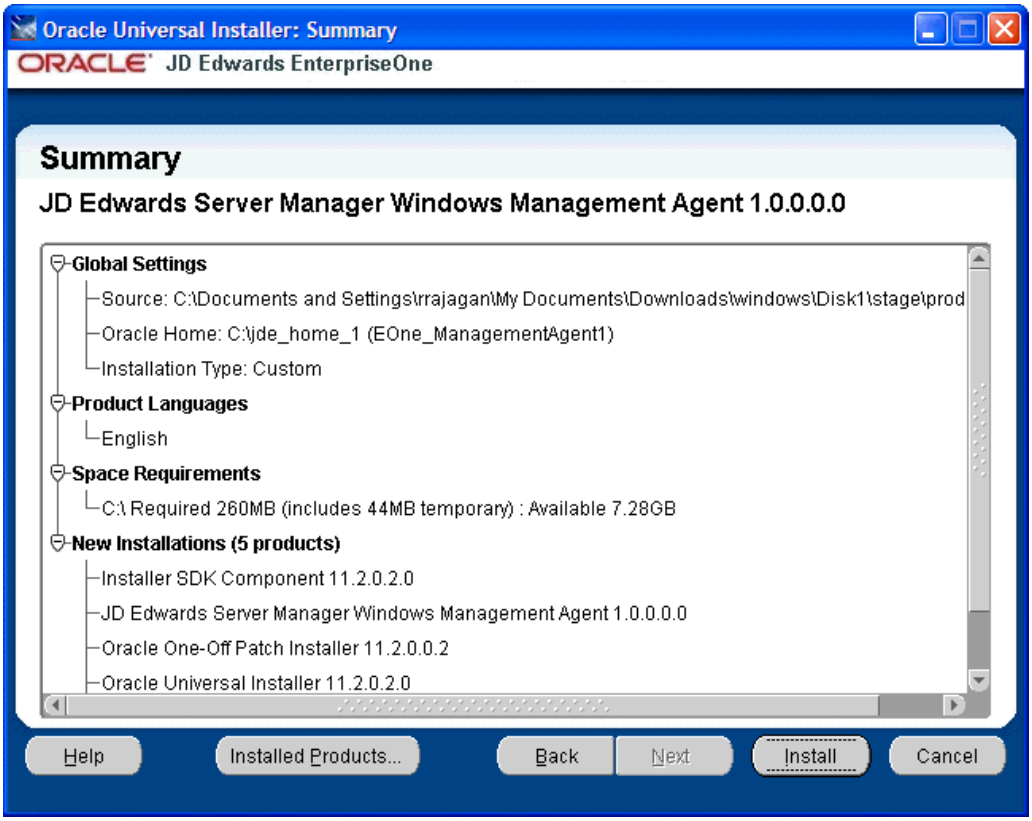
  You must specify a valid port of an existing Management Console machine.

  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.

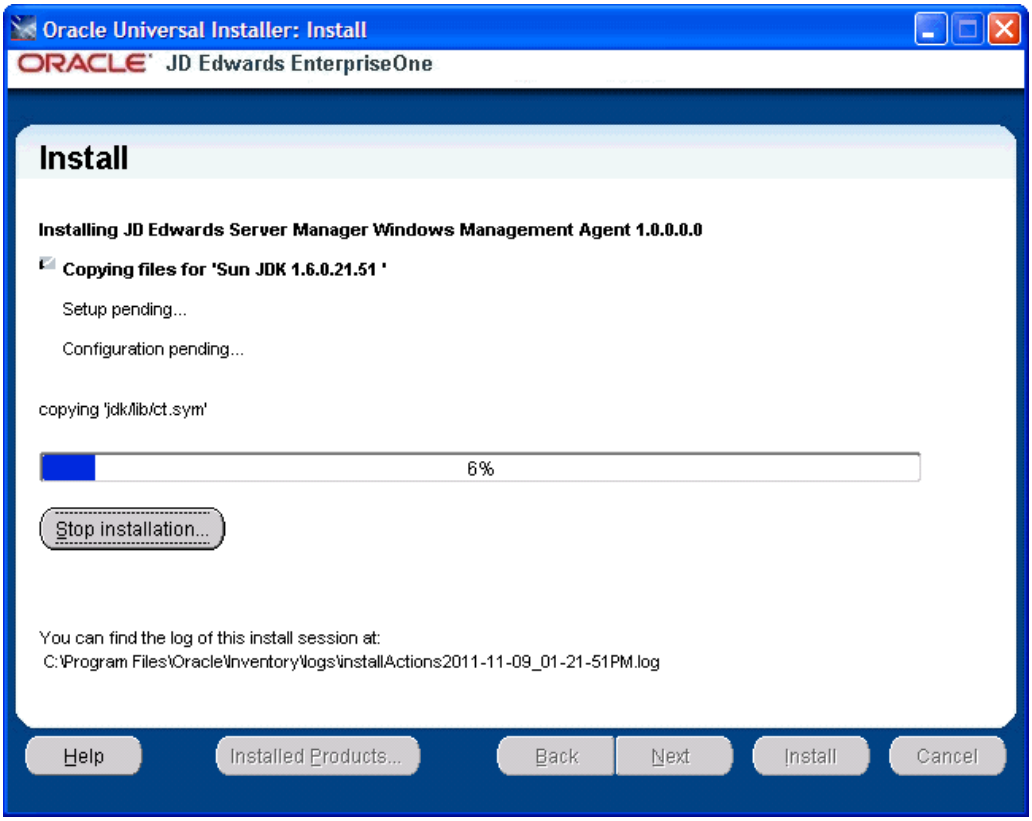
  Tip: You can determine the port of your Management Console from the information supplied on the *Management Agent Installers* screen. For navigation, refer to Step 2 in the section entitled: Section 5.1, "Obtain the Management Agent Installer Application".



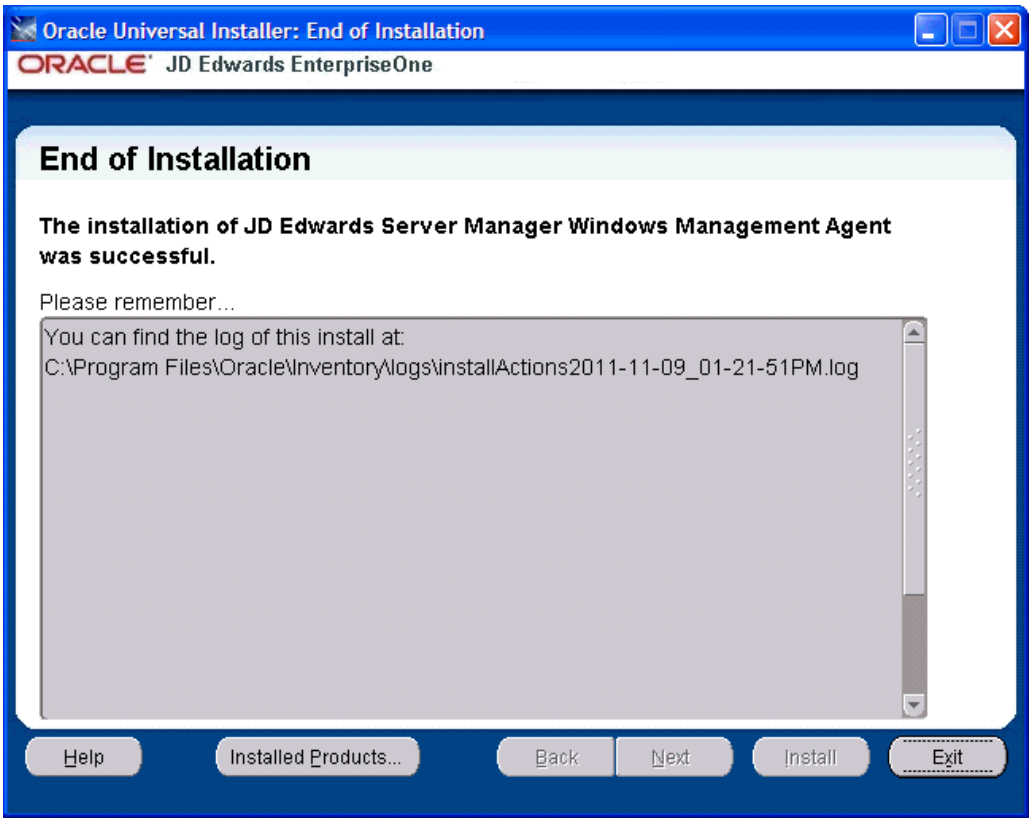
6. Click the **Next** button to verify the machine and port values.



7. 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.



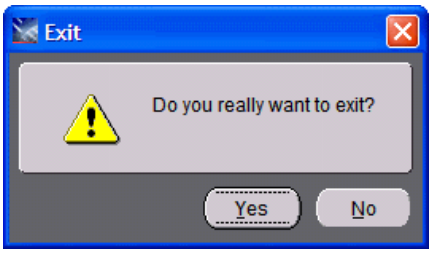
8. When the installation of the database finishes, the End of Installation screen is displayed.

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 you should always check the logs before you attempt to run the Deployment Server. The file is named log.txt and is located in the Deployment Server installation directory. For example:

```
C:\Program Files\Oracle\Inventory\logs\InstallActions\
installActionsyyyy-mm-dd_hh-mm-ssPM.log
```

---

9. Click the **Exit** button.



10. 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.

5.3.2 UNIX

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

- Linux
- Solaris
- AIX
- HP-UX on Itanium (HPIA64) (Release 9.1 Update 3)

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

- Section 5.3.2.1, "Permissions"
- Section 5.3.2.2, "/tmp location"
- Section 5.3.2.3, "Oracle User ID"
- Section 5.3.2.4, "Oracle Application Server"
- Section 5.3.2.5, "Enterprise Server"
- Section 5.3.2.6, "Graphic Mode"
- Section 5.3.2.7, "AIX and Solaris Operating Systems"

To run the Management Agent installer for UNIX, refer to this section: Section 5.3.2.8, "Running the Management Agent Installer", which follows the Notes below.

5.3.2.1 Permissions

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

5.3.2.2 /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.

5.3.2.3 Oracle User ID

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

5.3.2.4 Oracle Application Server

If you will be using the Management Agent to manage an Oracle Application Server, you must install the Management Agent as the same user as the Oracle Application Server. Therefore, before launching the installer you should switch to the appropriate user using the **su** command.

5.3.2.5 Enterprise Server

If you will be using the Management Agent to manage a UNIX-based Enterprise Server, you must install the Management Agent as the JD Edwards EnterpriseOne Enterprise Server user. For example, valid JD Edwards EnterpriseOne users might be `jdeb9`, `jde811`, `jde812`, or

jde900. Therefore, before launching the installer you should switch to the appropriate user using the **su** command. For example:

```
su - jdeb9
```

5.3.2.6 Graphic Mode

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

5.3.2.7 AIX and Solaris Operating Systems

Because the AIX operating system does not allow the Management Agent to be installed as a non-root user, you must install it as the ROOT user. On the Solaris operating system, you must install is as the oracle user. Once installed, you can change the owner of the Management Agent agent using the chown command. For example:

```
chown -R jde900:jde900 /u01/JDE_HOME
```

5.3.2.8 Running the Management Agent Installer

Use this procedure to run the Management Agent installer on UNIX-based target machines.

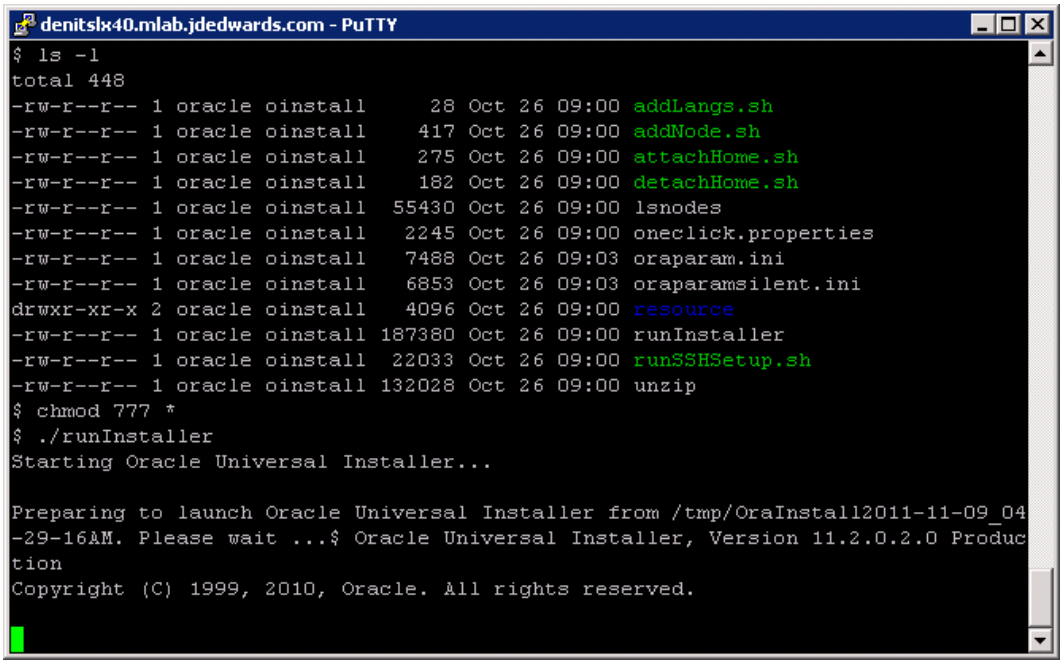
1. Run this script to launch the installer:

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

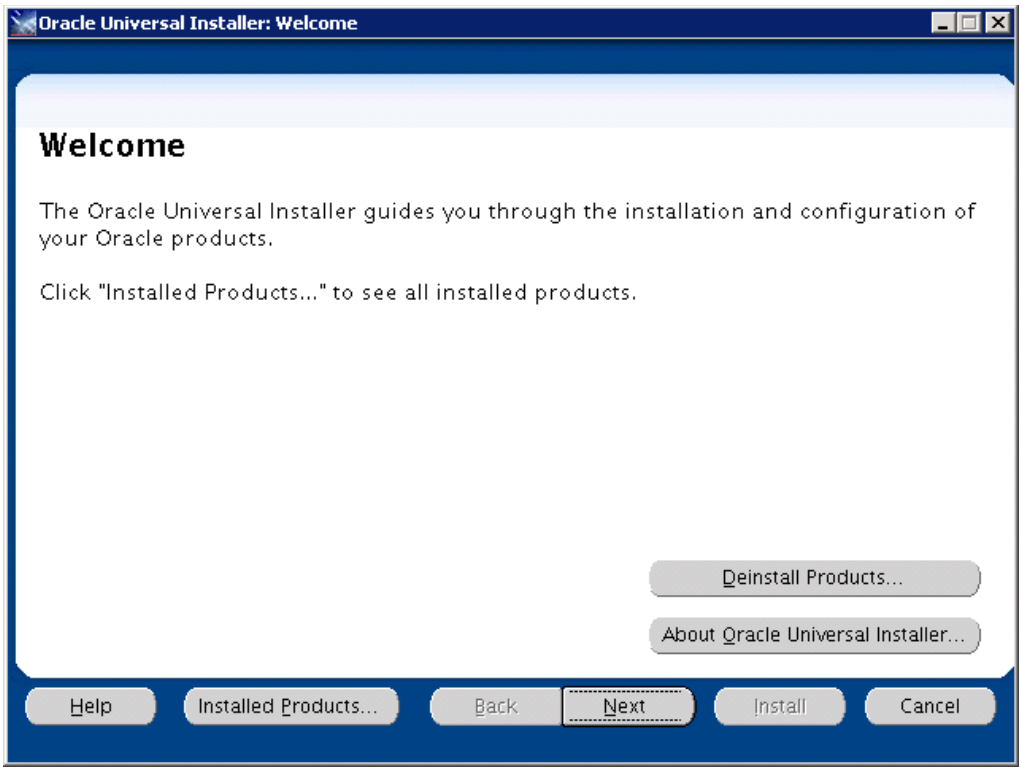
   ```
   /Disk1/install/runInstaller.sh
   ```

   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.

   The UNIX system indicates that it is preparing to launch the Oracle Universal Installer as shown in the below example.



   After the OUI installer is launched, the command window the Welcome screen is displayed.

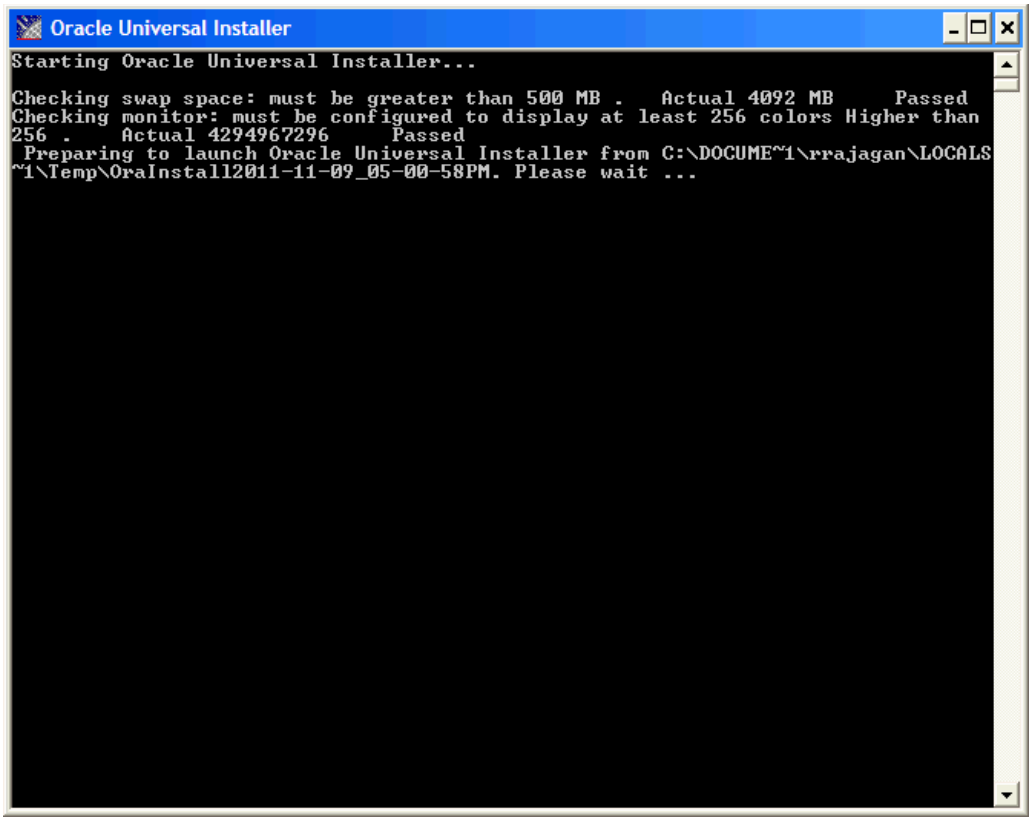


2. Double click this installer file to launch the installer:

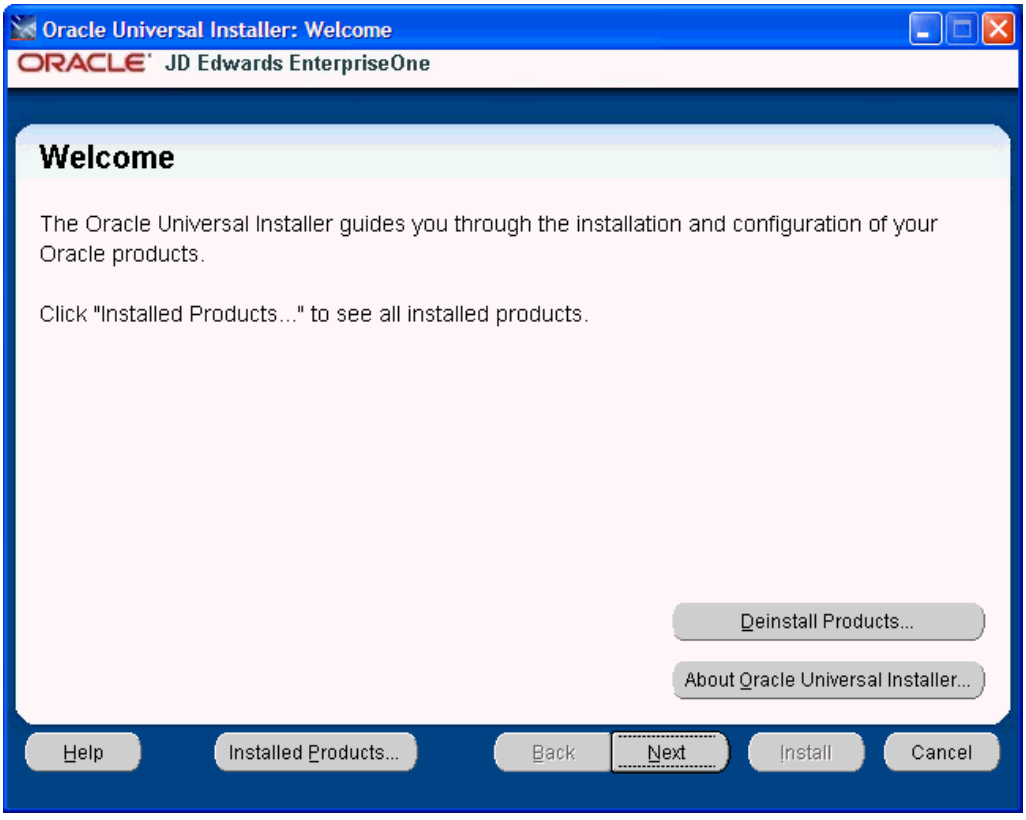
   `/Disk1/install/runInstaller.sh`

   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

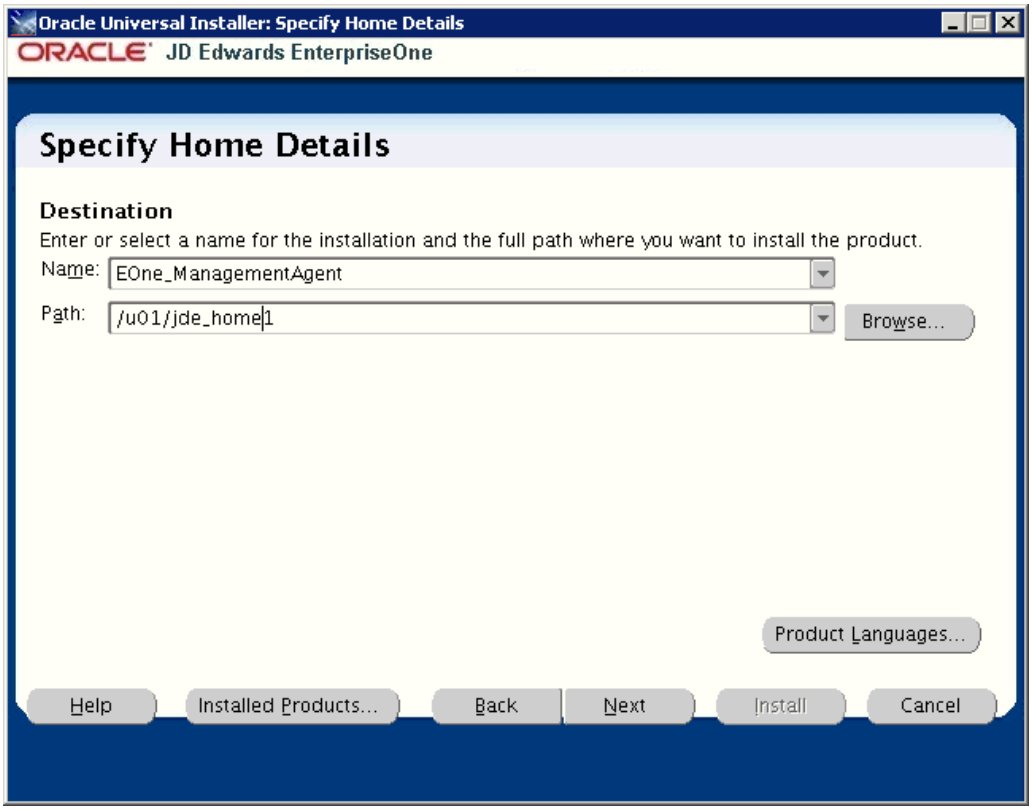
   This process opens a Microsoft Windows command window as shown in the below example.



After the OUI installer is launched, the command window is closed and the Welcome screen is displayed.



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



4. On Specify Home Details, complete these fields:

   - *Name:*

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

     EOne_Management_Agent

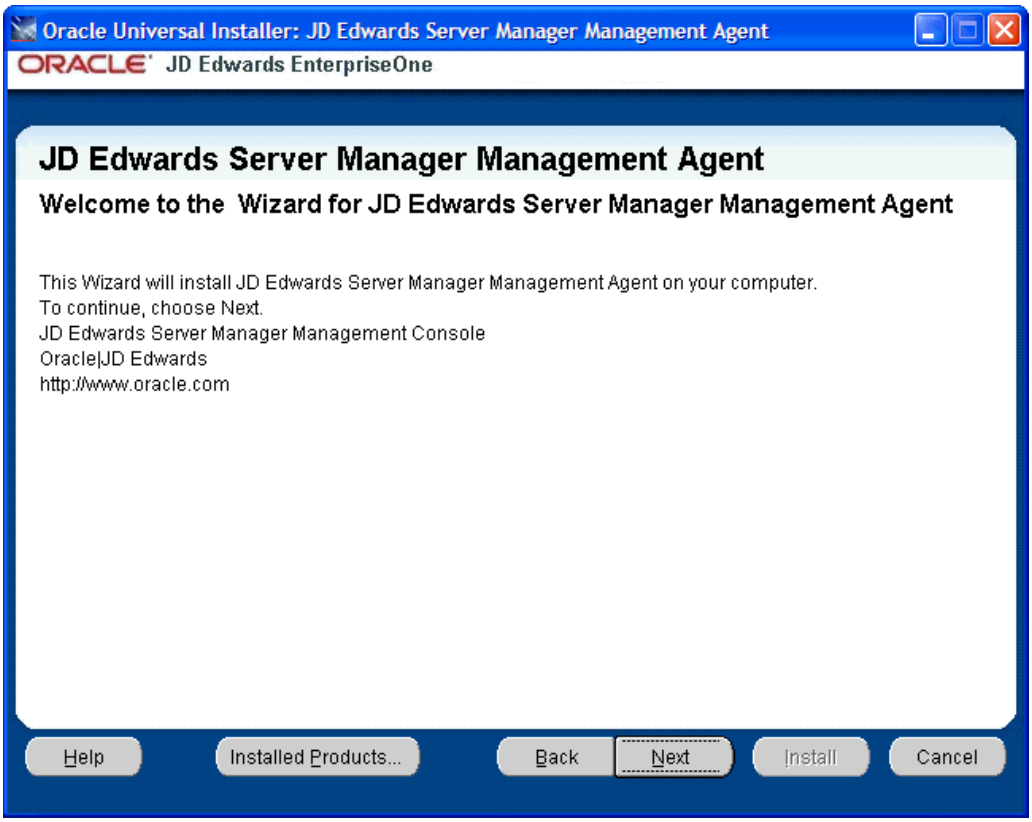
   - *Path:*

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

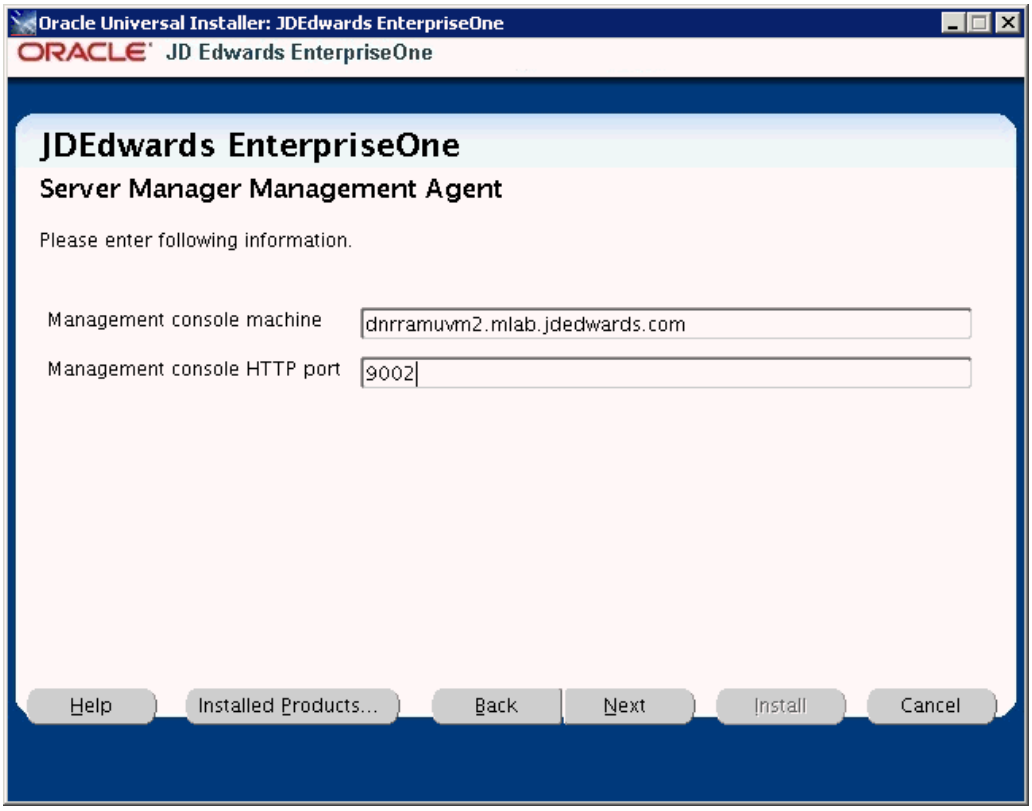
     `jde_home`

     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.



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



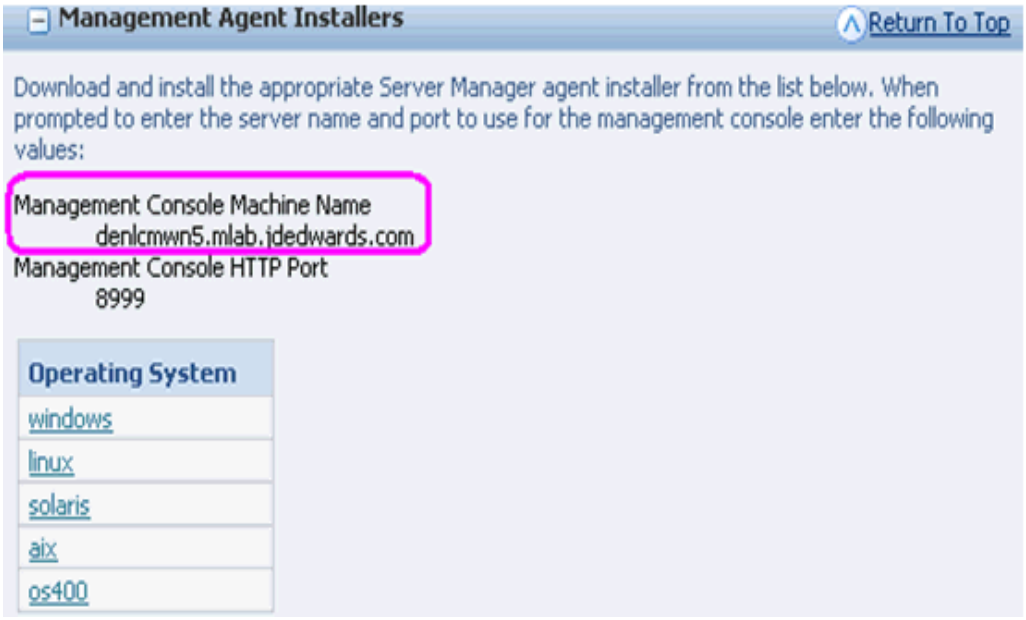
6. On Server Manager Management Agent, complete these fields:

   - *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 `dnrramuvm2` you might need to specify`dnrramuvm2.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: Section 5.1, "Obtain the Management Agent Installer Application". You can also view the `readme.txt` file in the root directory of the Management Console.

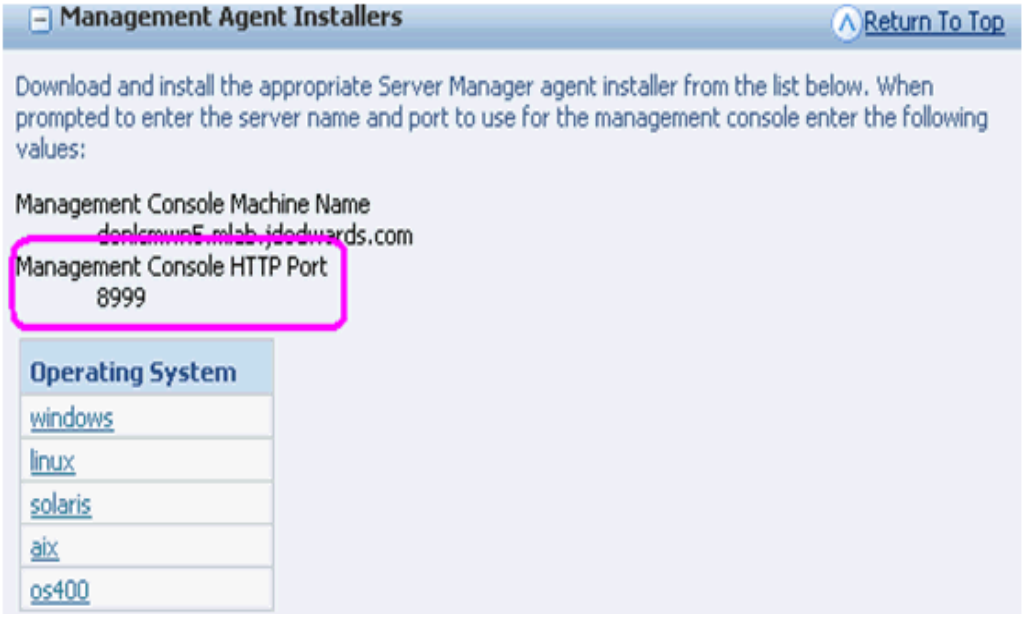


   - *Management console HTTP port*

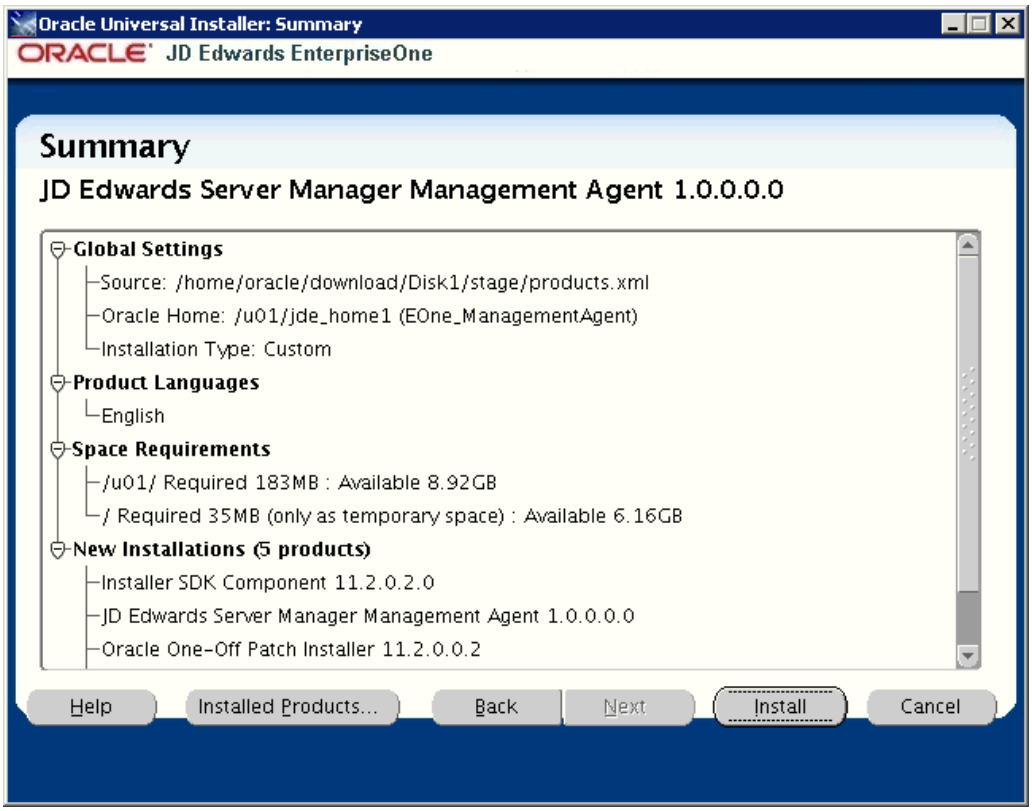
     You must specify a valid port of an existing Management Console machine.

     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.

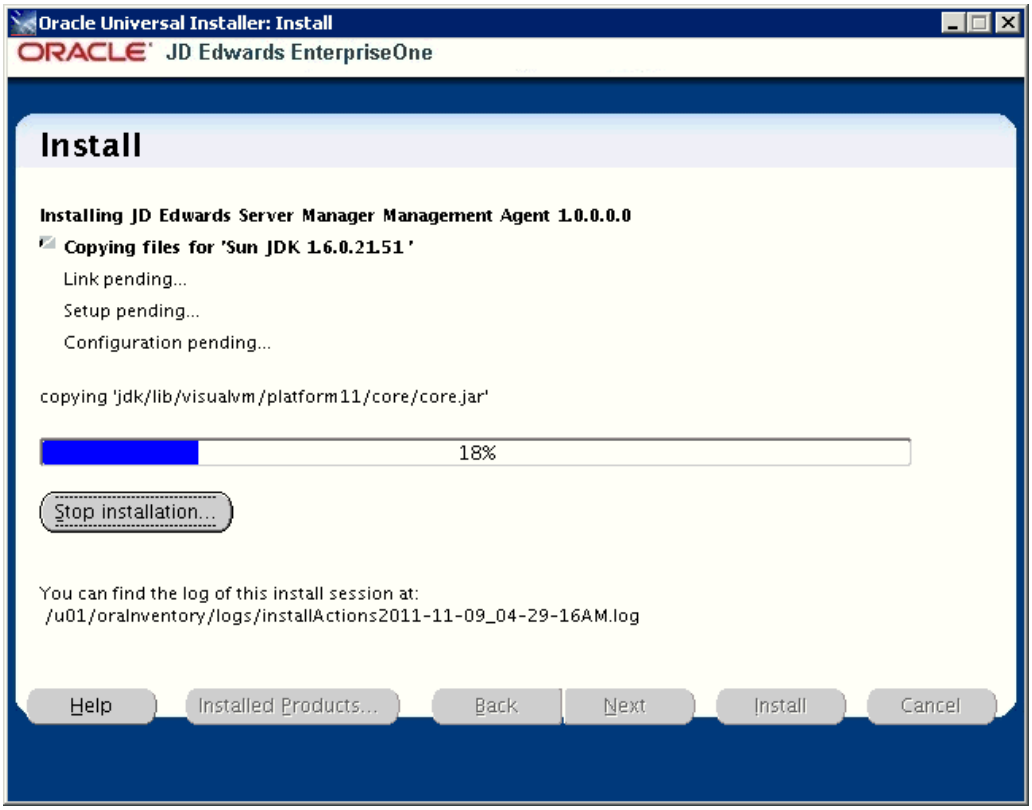
     Tip: You can determine the port of your Management Console from the information supplied on the *Management Agent Installers* screen. For navigation, refer to Step 2 in the section entitled: Section 5.1, "Obtain the Management Agent Installer Application".



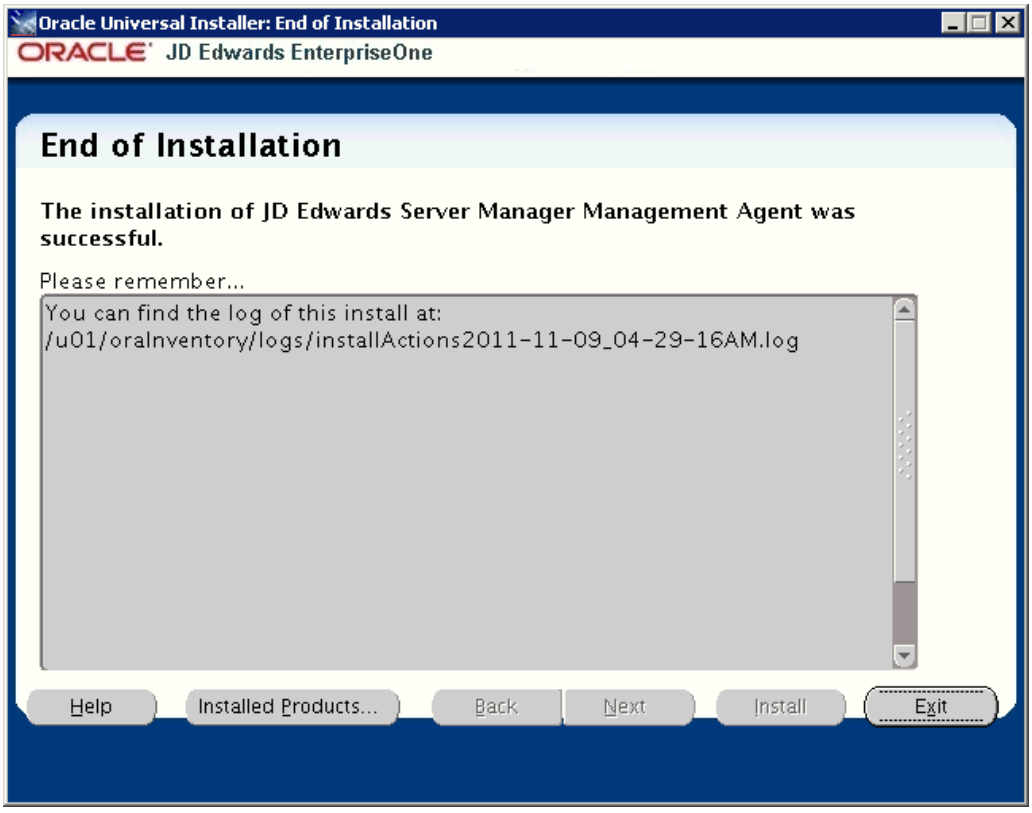
7. Click the **Next** button to verify the machine and port values.



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



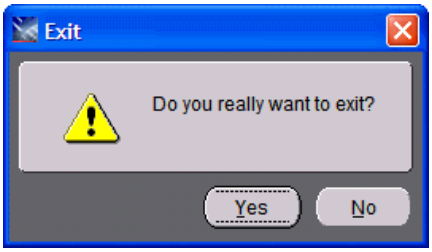
The Management Agent installer displays a panel showing the ongoing status of the installation.



9. When the installation of the database 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 you should always check the logs before you attempt to run the Deployment Server. The file is named log.txt and is located in the Deployment Server installation directory. For example:
>
> `/u01/oraInventory/logs/installActions2011-11-09_04-29-16AM.log`

10. Click the **Exit** button.



11. 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.

5.3.3 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: IBM i (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.

1. On the Microsoft Windows machine where you extracted the `.zip` file, and which is mapped to the IBM i machine, run this file:

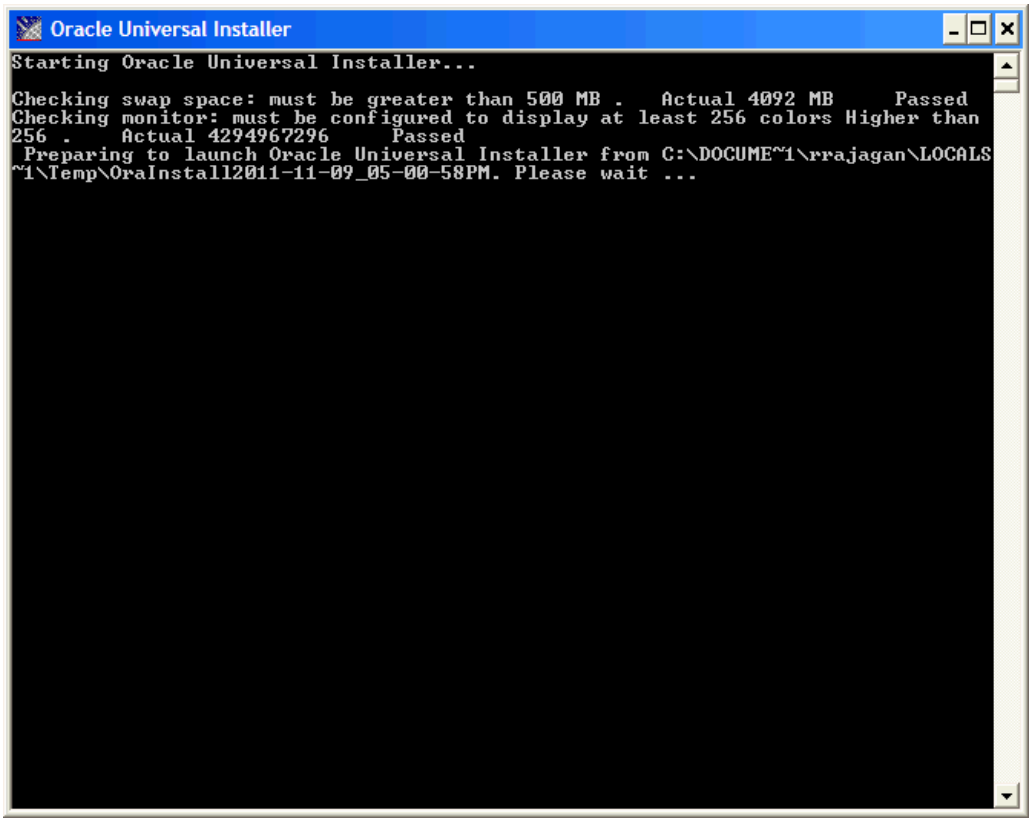
   `/Disk1/install/setup.exe`

1. On the Microsoft Windows machine where you extracted the `.zip` file, and which is mapped to the IBM i machine, run this file:

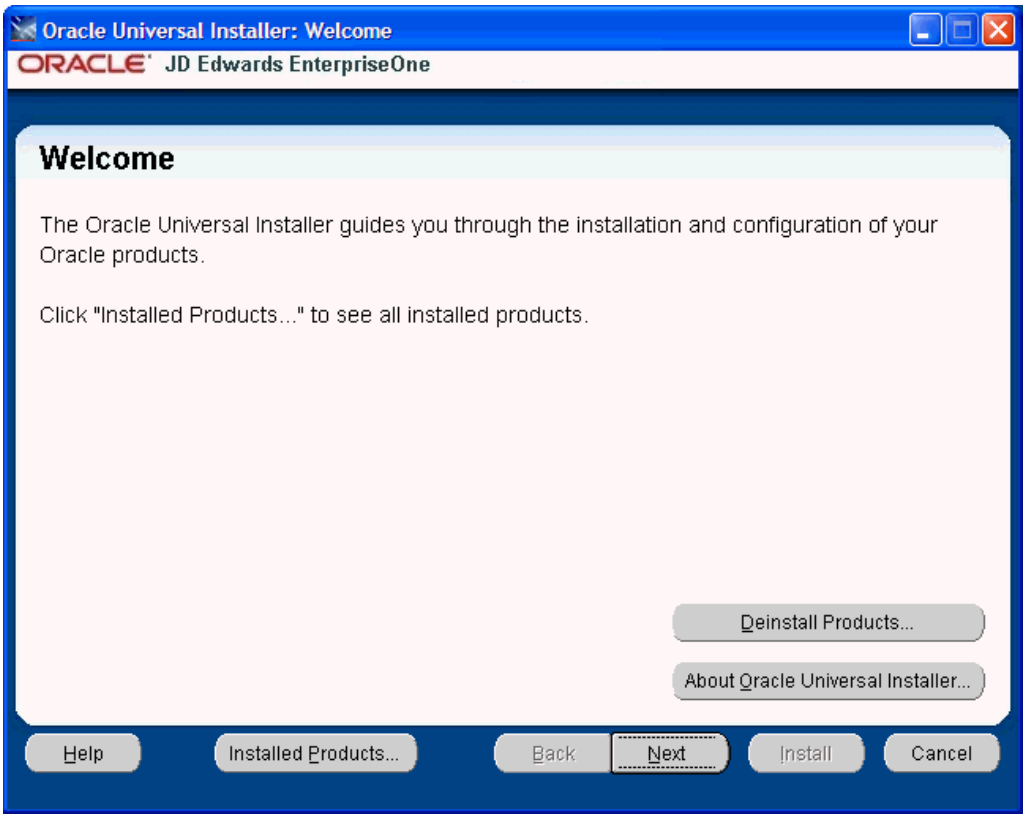
```
/Disk1/install/setup.exe
```

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: IBM i (OS400)

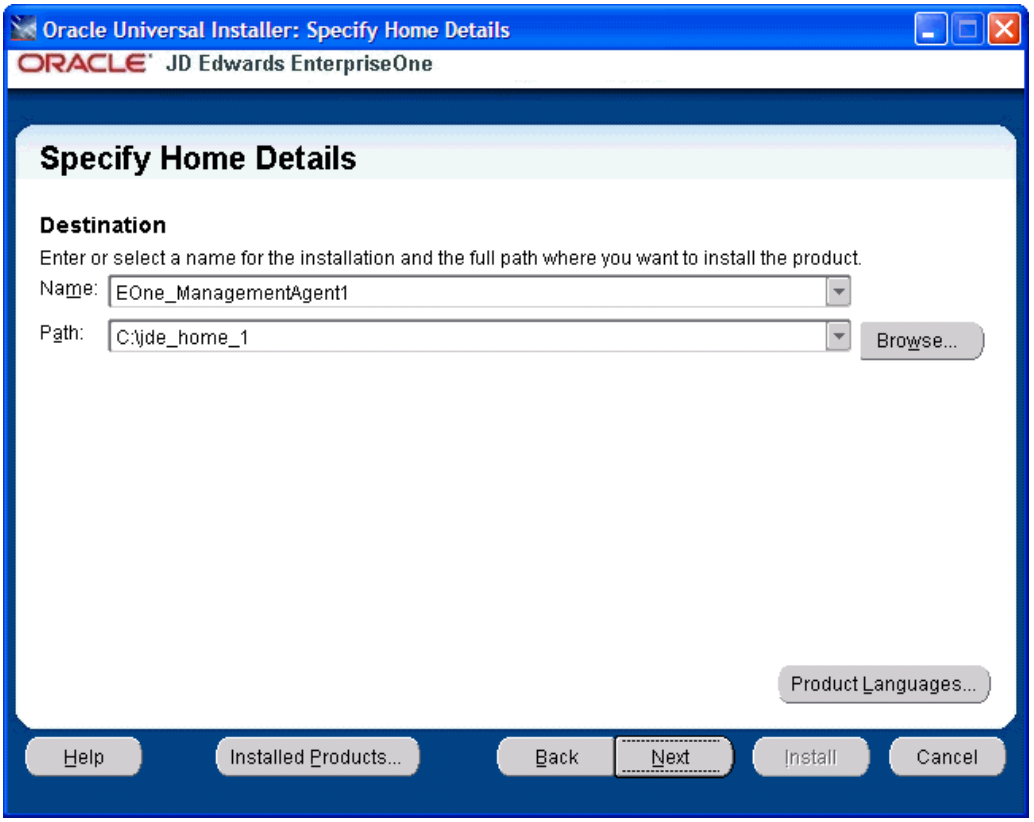
This process opens a Microsoft Windows command window as shown in the below example.



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:

- *Name:*

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

  EOne_Management_Agent

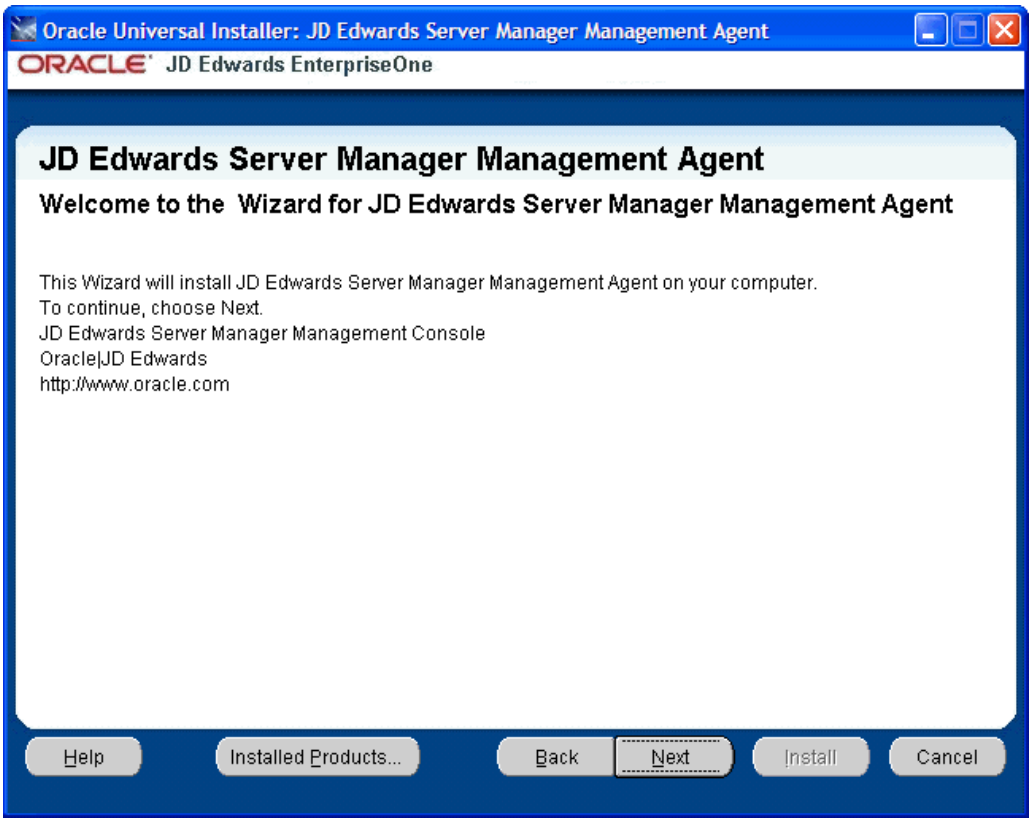
- *Path:*

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

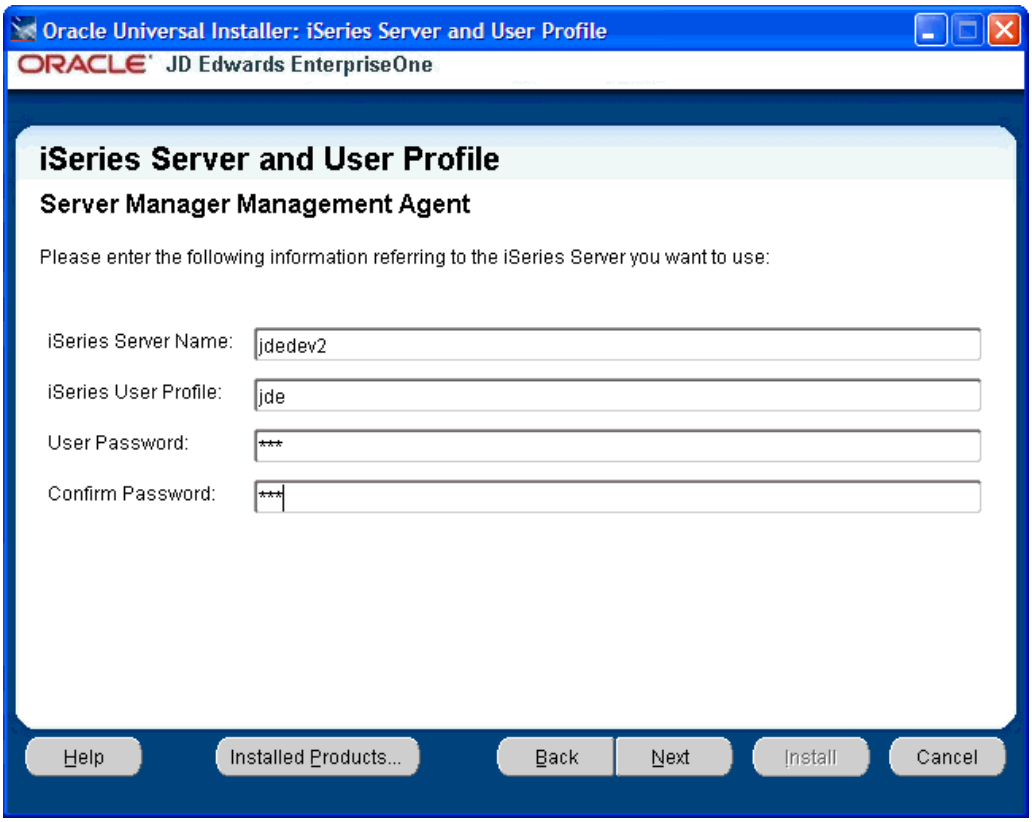
  `jde_home`

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.



5. On iSeries Server and User Profile, complete these fields:

   - *iSeries Server Name*

     Enter the name of your IBM i target server.

   - *iSeries User Profile*

     Enter the user profile for the IBM i target server on which the Management Agent will be installed.

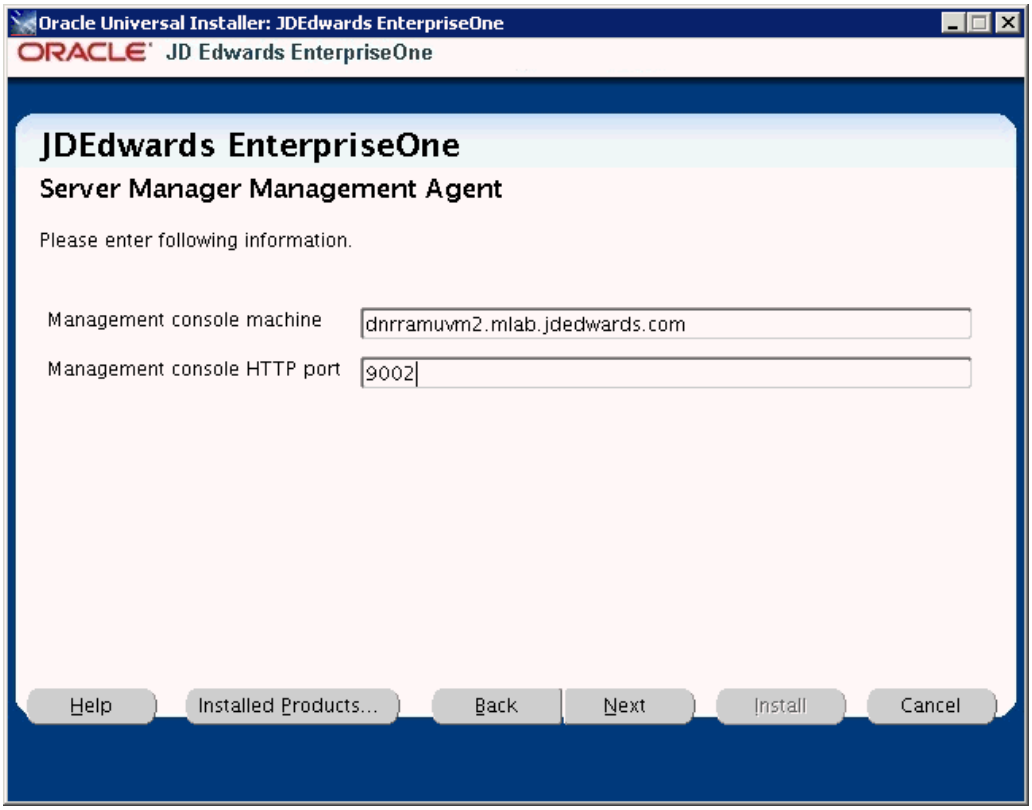
   - *User Password*

     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.

6. Click the **Next** button.



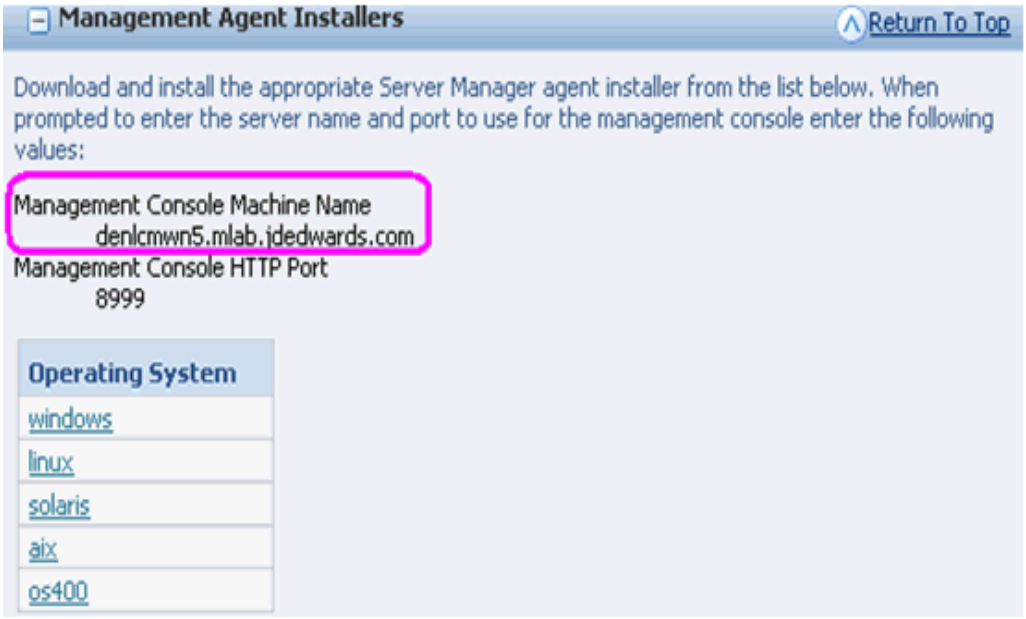
7. On Server Manager Management Agent, complete these fields:

- *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 `dnrramuvm2` you might need to specify`dnrramuvm2.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: Section 5.1, "Obtain the Management Agent Installer Application". You can also view the `readme.txt` file in the root directory of the Management Console.



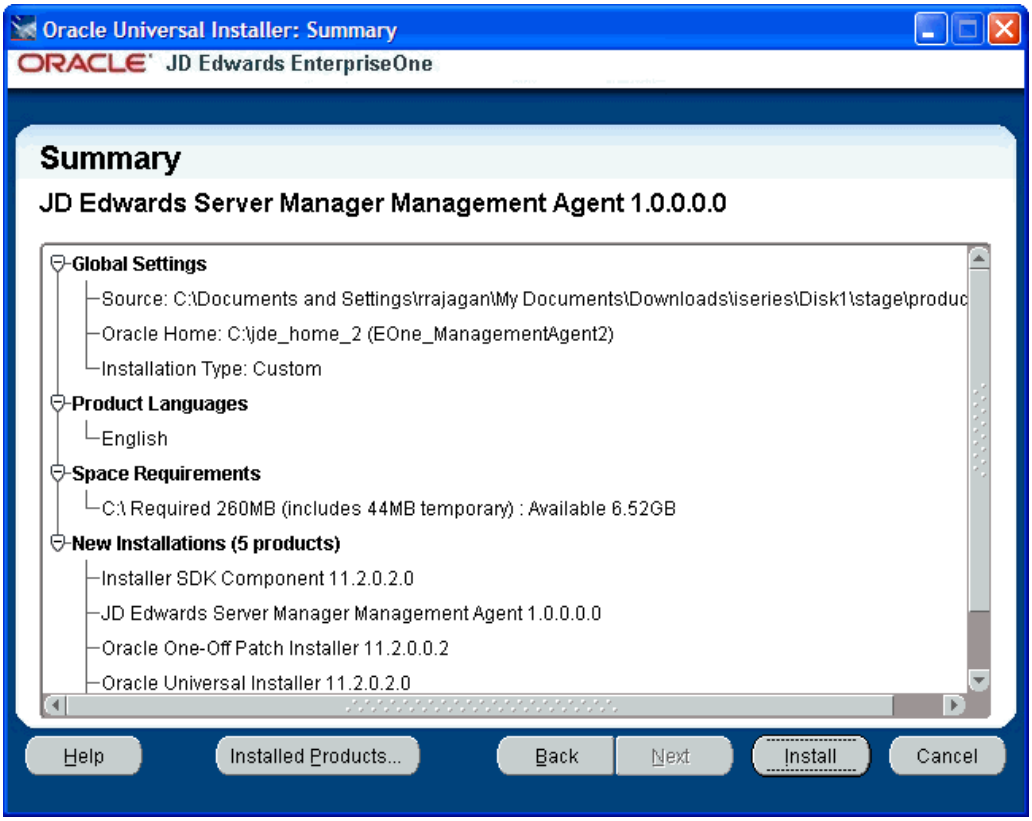
- *Management console HTTP port*

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

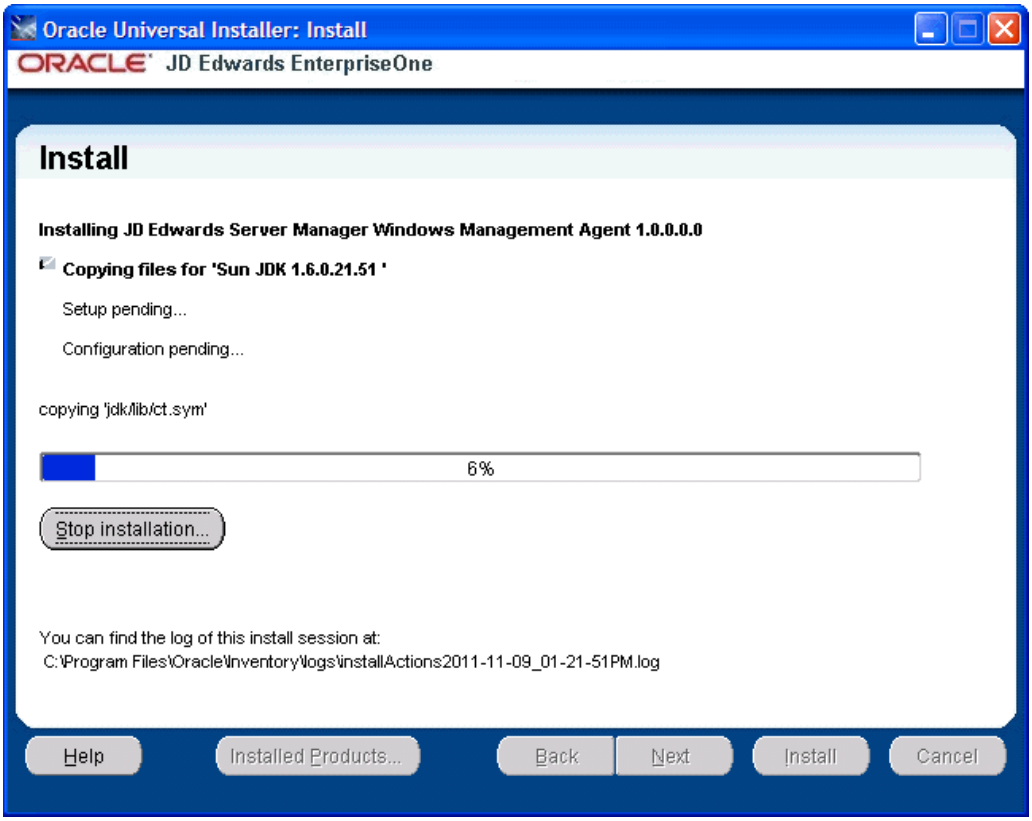
  The installer verifies the port connection to the Management Console. The machine must be started and the Management Console must be running in order to run the installer.

  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: Section 5.1, "Obtain the Management Agent Installer Application".

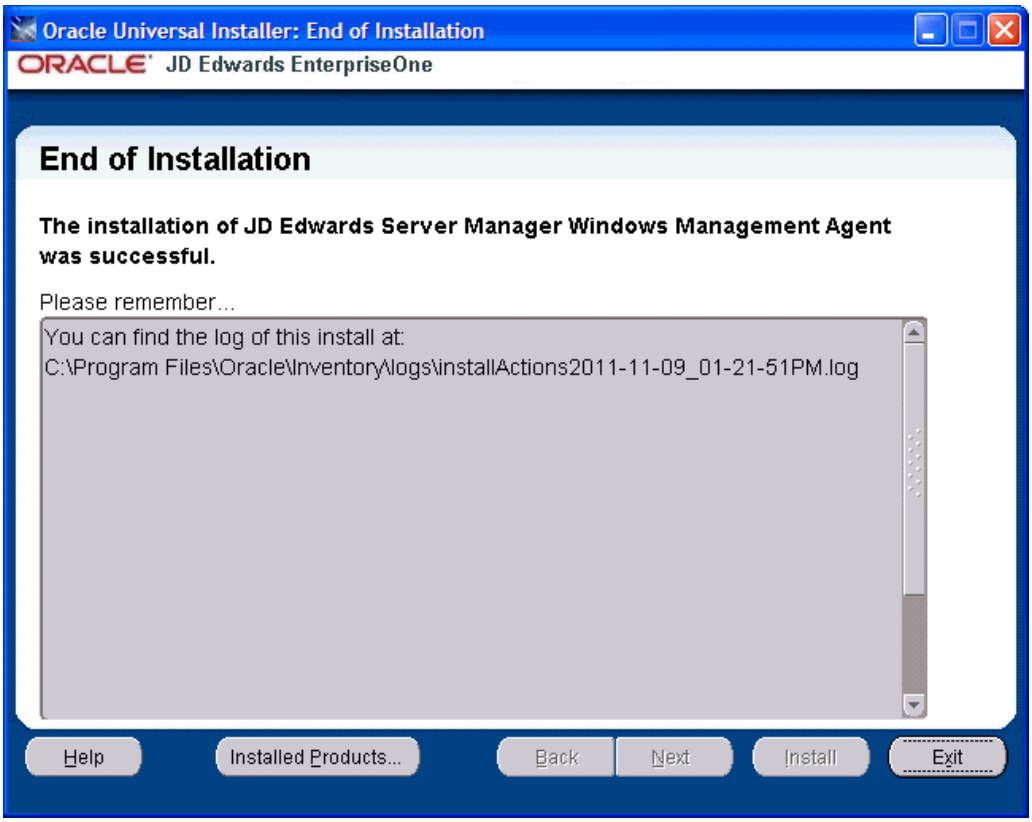
8. Click the **Next** button to verify the machine and port values.



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.



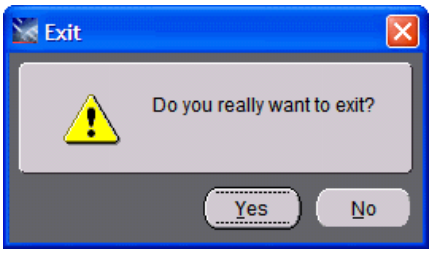
10. When the installation of the database finishes, the End of Installation screen is displayed.

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 you should always check the logs before you attempt to run the Deployment Server. The file is named log.txt and is located in the Deployment Server installation directory. For example:

```
C:\Program Files\Oracle\Inventory\logs\InstallActions\
installActionsyyyy-mm-dd_hh-mm-ssPM.log
```

---

11. Click the **Exit** button.



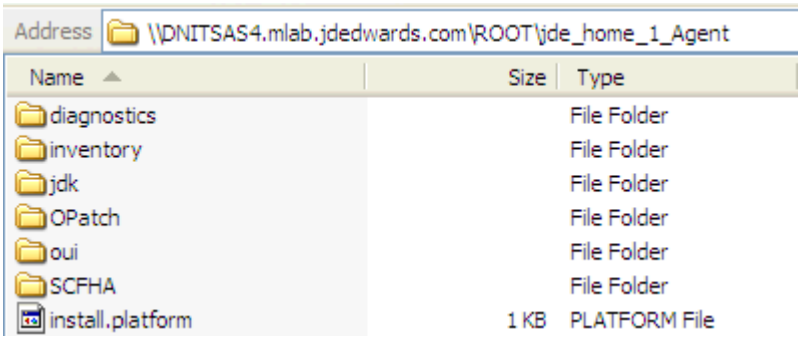
12. On the Exit dialog, click the **Yes** button to confirm you want to exit the Management Agent installer.

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:



5.4 Post Installation Steps for WebLogic 11g, WebLogic 12c, WebSphere 7.0, or WebSphere 8.5 Web Server Instances

If you are going to be managing either a WebLogic 11g web server or a WebSphere 7.0 or 8.5 web server instance, the Server Manager management agent must be modified to use the correct JVM.

This section describes post installation tasks for these application servers:

- Section 5.4.1, "WebLogic 11g"
- Section 5.4.2, "WebLogic 12c"
- Section 5.4.3, "WebSphere 7.0 and WebSphere 8.5"

5.4.1 WebLogic 11g

JD Edwards EnterpriseOne applications running under WebLogic web servers require that the WebLogic server uses a 64-bit JVM. In order to successfully manage a WebLogic server you must modify the Server Manager management agent to use a 64-bit, version 1.6 JVM.

This section describes post installation tasks for these platforms:

- Section 5.4.1.1, "Microsoft Windows"
- Section 5.4.1.2, "UNIX"

5.4.1.1 Microsoft Windows

Note: Microsoft Windows 2008 is the only Windows version currently supported with EnterpriseOne running under WebLogic.

WebLogic server is not supported on IBM i.

To configure WebLogic 11g web servers to support a 64-bit JVM on the Microsoft Windows platform:

1. Locate the `installAgentService.bat` batch file in the bin directory under the agent install location.
2. Edit the `installAgentService.bat` file to change the JAVA_HOME environment variable to point to an appropriate 64-bit, version 1.6 JDK or JRE directory.
3. Run the `updateAgentService.bat` batch file.

   This file stops, uninstalls, re-installs, and starts the agent service so that it will use the correct java program when it starts.

5.4.1.2 UNIX

To configure WebLogic 11g web servers to support a 64-bit JVM on any of the supported UNIX platforms:

1. Locate the `runAgent` script in the bin directory under the agent install location.
2. Edit the `runAgent` script to change the JAVA_HOME environment variable to point to an appropriate 64-bit, version 1.6 JDK or JRE directory.
3. Restart the Server Manager agent.

5.4.2 WebLogic 12c

JD Edwards EnterpriseOne applications running under WebLogic web servers require that the WebLogic server uses a 64-bit JVM. In order to successfully manage a WebLogic server you must modify the Server Manager management agent to use a 64-bit, version 1.7 JVM.

This section describes post installation tasks for these platforms:

- Section 5.4.2.1, "Microsoft Windows"
- Section 5.4.2.2, "UNIX"

5.4.2.1 Microsoft Windows

Note: Microsoft Windows 2008 is the only Windows version currently supported with EnterpriseOne running under WebLogic.

WebLogic server is not supported on IBM i.

To configure WebLogic 12c web servers to support a 64-bit JVM on the Microsoft Windows platform:

1. Locate the installAgentService.bat batch file in the bin directory under the agent install location.
2. Edit the installAgentService.bat file to change the JAVA_HOME environment variable to point to an appropriate 64-bit, version 1.7 JDK or JRE directory.
3. Run the updateAgentService.bat batch file.

   This file stops, uninstalls, re-installs, and starts the agent service so that it will use the correct java program when it starts.

5.4.2.2 UNIX

To configure WebLogic 11g web servers to support a 64-bit JVM on any of the supported UNIX platforms:

1. Locate the runAgent script in the bin directory under the agent install location.
2. Edit the runAgent script to change the JAVA_HOME environment variable to point to an appropriate 64-bit, version 1.7 JDK or JRE directory.
3. Restart the Server Manager agent.

5.4.3 WebSphere 7.0 and WebSphere 8.5

WebSphere 7.0 web servers use a version 1.6 JVM. In order to successfully manage a WebSphere 7.0 server you must modify the Server Manager management agent to use an appropriate version 1.6 JVM.

This section describes post installation tasks for these platforms:

- Section 5.4.3.1, "Microsoft Windows"
- Section 5.4.3.2, "UNIX or IBM i (OS400)"

5.4.3.1 Microsoft Windows

To configure WebSphere 7 web servers to support a 64-bit JVM on the Microsoft Windows platform:

1. Locate the `installAgentService.bat` batch file in the bin directory under the agent install location
2. Edit the `installAgentService.bat` script to change the JAVA_HOME environment variable to point to an appropriate version 1.6 JDK or JRE directory.

   Tools Release 9.1 Update 2.3. For IBM WebSphere 8.5, you must ensure that this points to the SDK 1.7 delivered by IBM WebSphere 8.5. For additional information on this JDK 1.7, refer to the *JD Edwards EnterpriseOne HTML Server Reference Guide for Microsoft Windows*.
3. Run the `updateAgentService.bat` batch file.

   This file stops, uninstalls, re-installs, and starts the agent service so that it will use the correct java program when it starts.

5.4.3.2 UNIX or IBM i (OS400)

To configure WebSphere 7 web servers to support a 64-bit JVM on any of the supported UNIX platforms or on IBM i:

1. Locate the `runAgent` script in the bin directory under the agent install location
2. Edit the `runAgent` script to change the JAVA_HOME environment variable to point to an appropriate version 1.6 JDK or JRE directory.

   Tools Release 9.1 Update 2.3. For IBM WebSphere 8.5 and non-IBM platforms, you must ensure that this points to the SDK 1.7 delivered by IBM WebSphere 8.5 or other platform-specific JDK. For additional information on the JDK 1.7 delivered by WebSphere, refer to the *JD Edwards EnterpriseOne HTML Server Reference Guide* for your platform.

   Tools Release 9.1 Update 2.3. For IBM i, the SDK 1.7 is part of the license program for Java option 14 and 15.
3. Restart the Server Manager agent.

5.5 Troubleshoot the Management Agent Installation

This section describes:

- Section 5.5.1, "Management Agent Installer Failed"
- Section 5.5.2, "Management Agent Does Not Start"
- Section 5.5.3, "Management Agent Dies on Unix or IBM i"
- Section 5.5.4, "Management Agent Cannot Manage Oracle Application Server on Unix"
- Section 5.5.5, "Management Agent Cannot Start or Stop a Unix Enterprise Server"
- Section 5.5.6, "Management Agent Cannot Manage Secure Servers on WebSphere Application Server on IBM i"

5.5.1 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
(x86)\Oracle\Inventory\logs\installActions2011-10-18-02-15-1
4PM.log
```

5.5.2 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
(x86)\Oracle\Inventory\logs\installActions2011-10-18-02-15-14PM.log
```

The log file should contain this message:

```
INFO: Starting the management agent listener on port 'xxxxx'
```

5.5.3 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.

5.5.4 Management Agent Cannot Manage Oracle Application Server on Unix

If you are using the Management Agent to manage an Oracle Application Server on a Unix platform, you must install the Management Agent with the same user and group as the Oracle 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@denlcmlx2 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 ccr
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@denlcmlx2 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
```

5.5.5 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@denlcmlx2 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 ccr
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
```

5.5.6 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
```

5.6 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 Chapter 19, "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:

- Section 5.6.1, "Microsoft Windows and UNIX"
- Section 5.6.2, "IBM i OS/400"

5.6.1 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 deinstall you will no longer be able to deinstall those components.

1. Launch Oracle Universal Installer:

   - **Microsoft Windows**

     `Disk1/install/setup.exe`

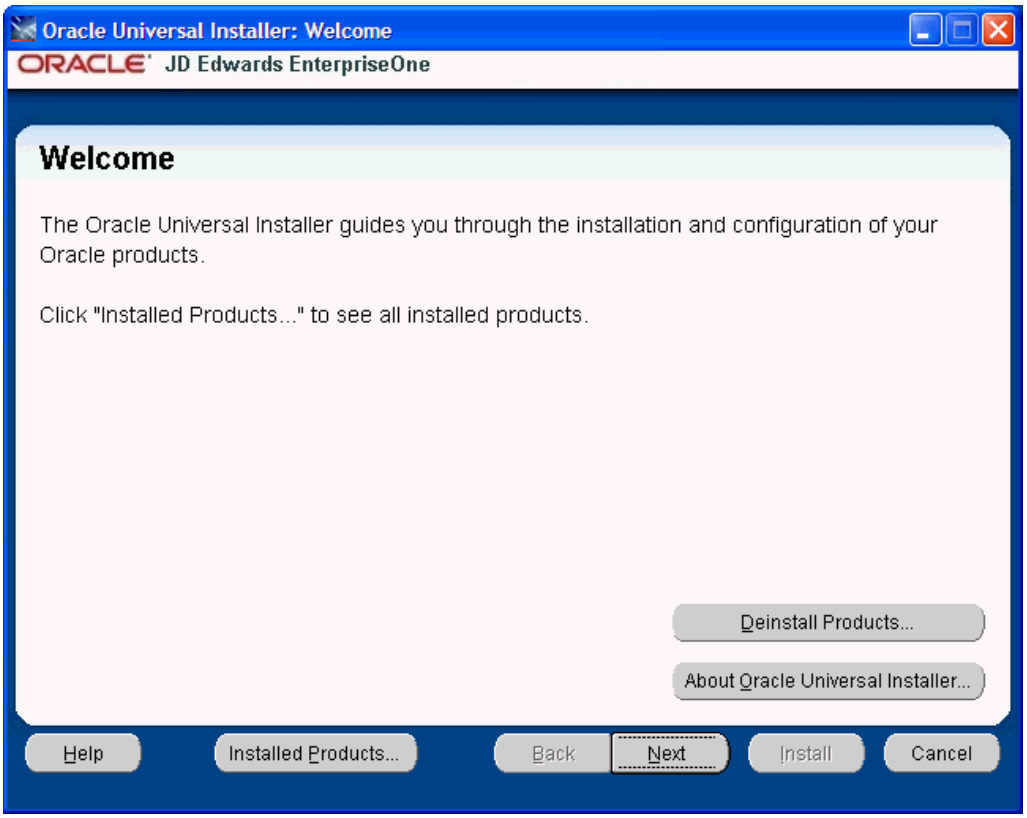
     Alternately, you can navigate Start > Oracle - E1_Management_Agent_x > Oracle Installation Products > Universal Installer

     where “x”, if it exists, is the numeric value of the Management Agent that you want to deinstall.

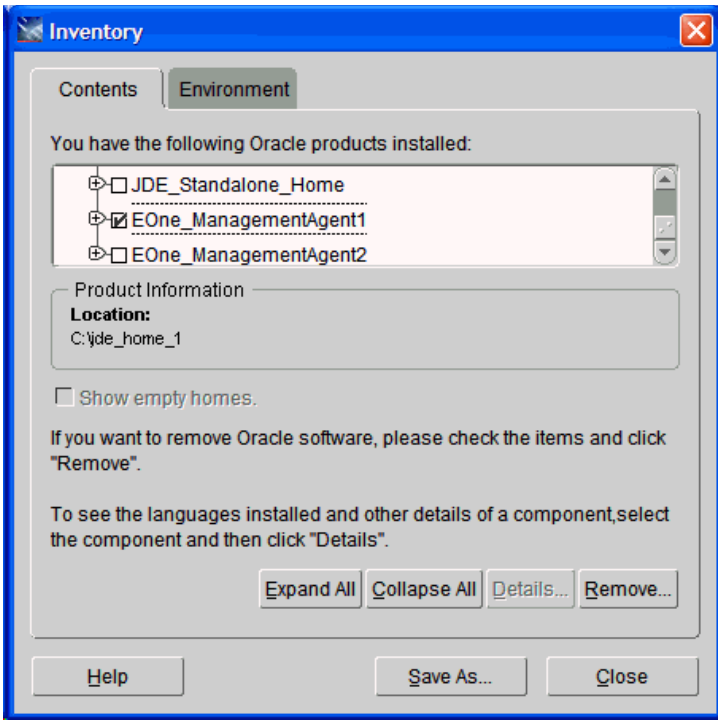
   - **UNIX**

     `/<installation_home>/oui/bin/runInstaller.sh`

   After the OUI installer is launched, the Welcome screen is displayed.



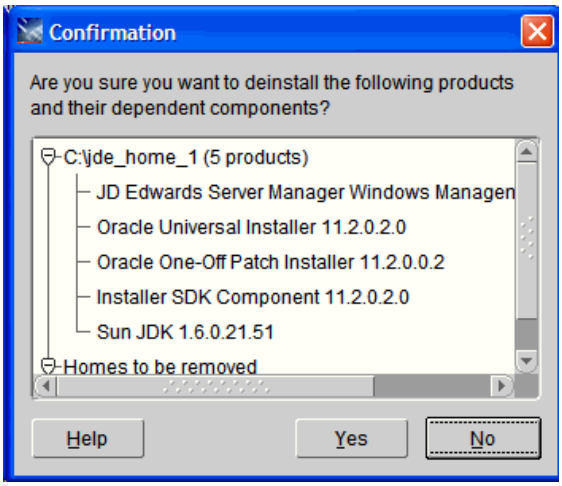
2. On Welcome, click the **Deinstall Products...** button.



3. On Inventory, with the Contents tab selected, select the check box for the Management Agent that you want to deinstall. For example:

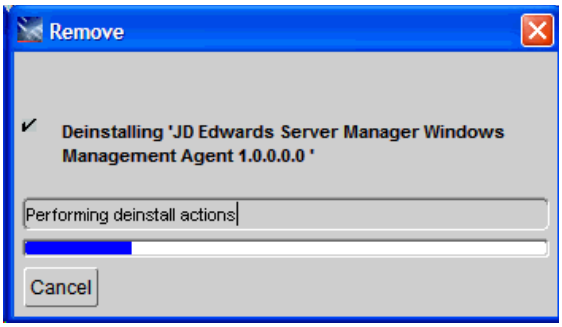
   EOne_ManagementAgent1

4. Click the **Remove** button.

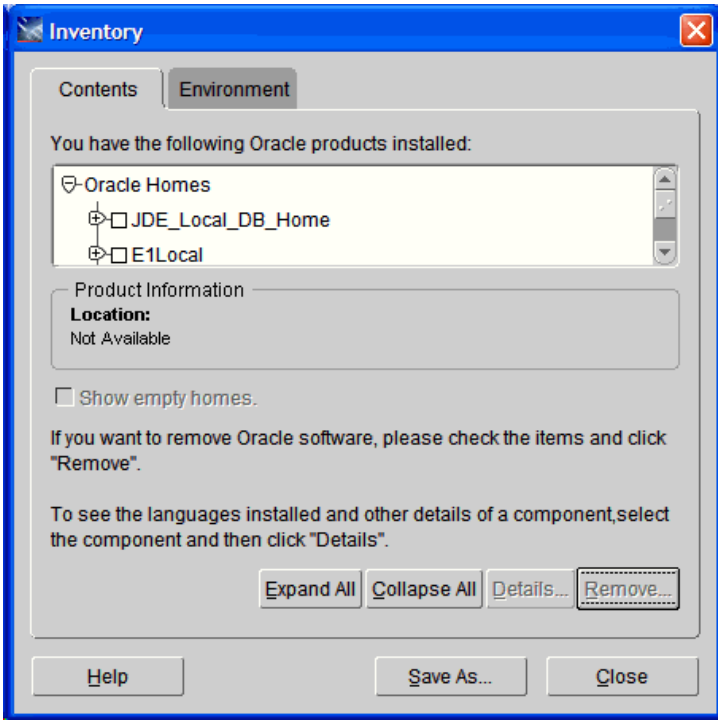


5. On Confirmation, ensure the selected **jde_home** on the target machine is that of the Management Agent that you want to install, and click the **Yes** button.

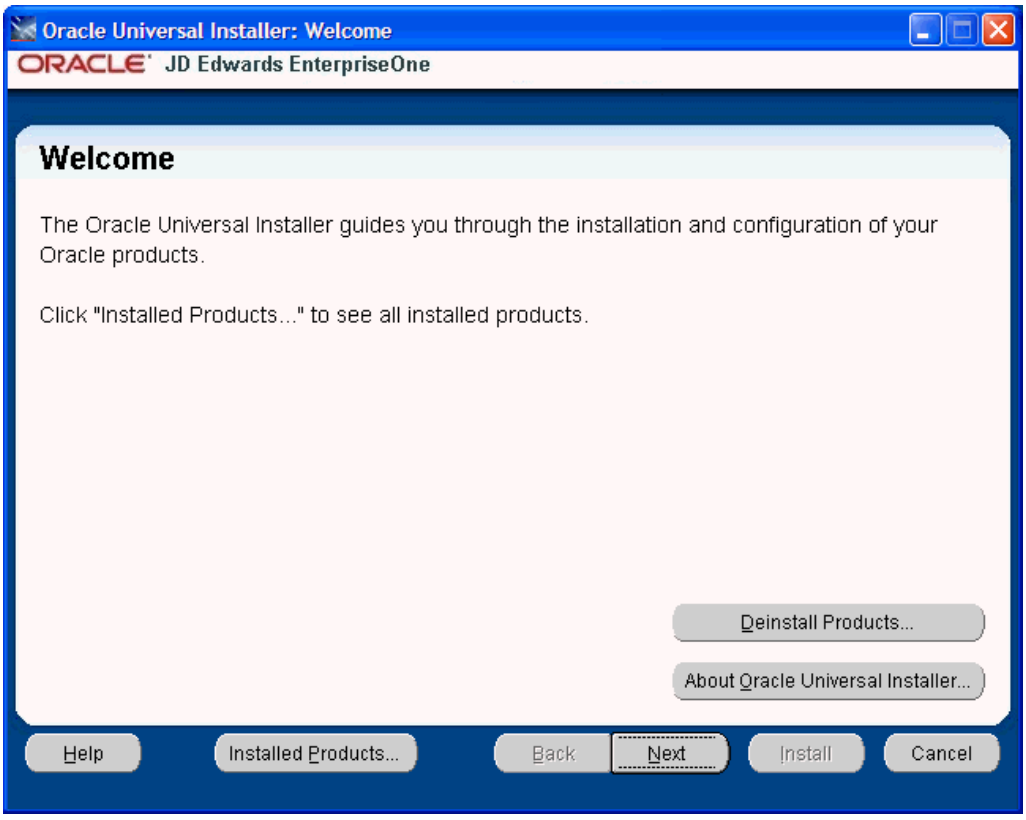
   A deinstallation progress panel is displayed:



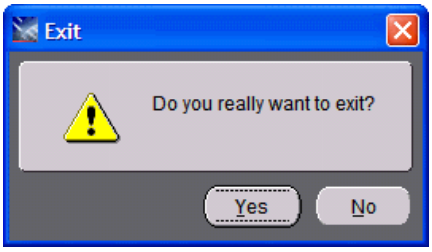
When the deinstallation complete, the Inventory screen is displayed.



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.

5.6.2 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.

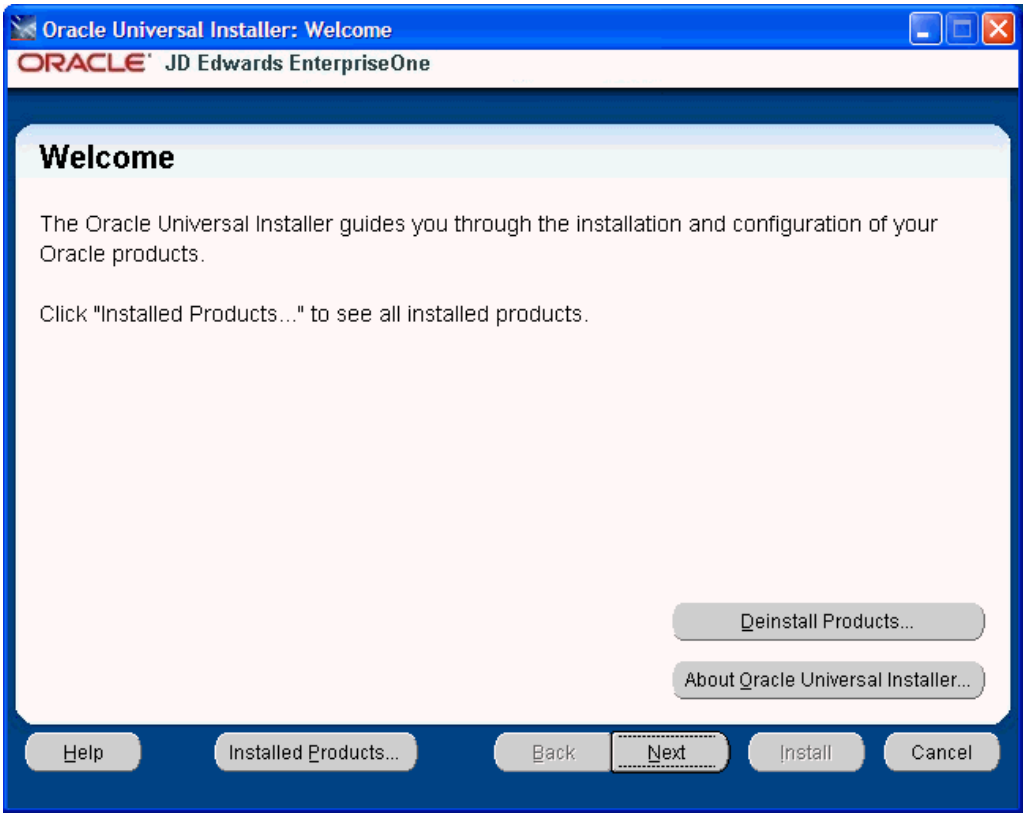
1. Launch Oracle Universal Installer from this location:

   `Disk1/install/setup.exe`

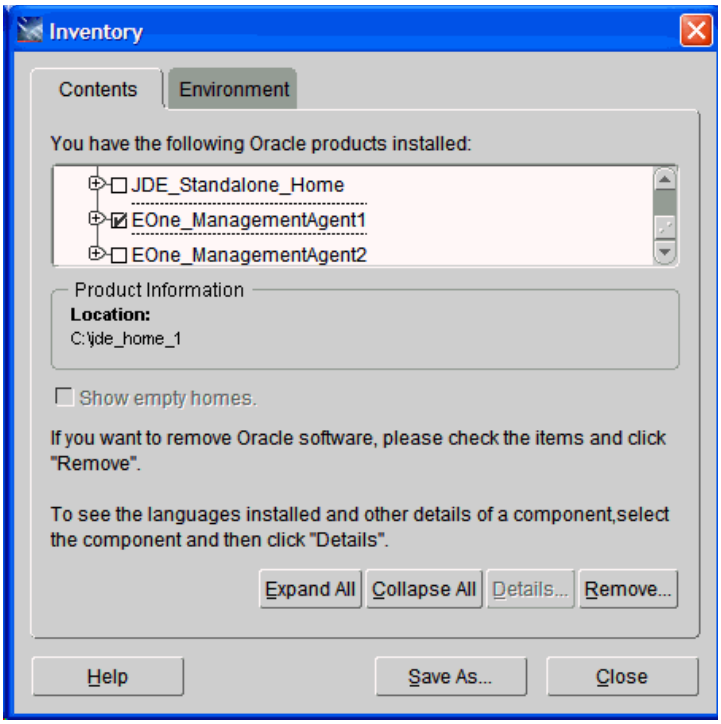
   Alternately, you can navigate Start > Oracle - E1_Management_Agent_x > Oracle Installation Products > Universal Installer

   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.



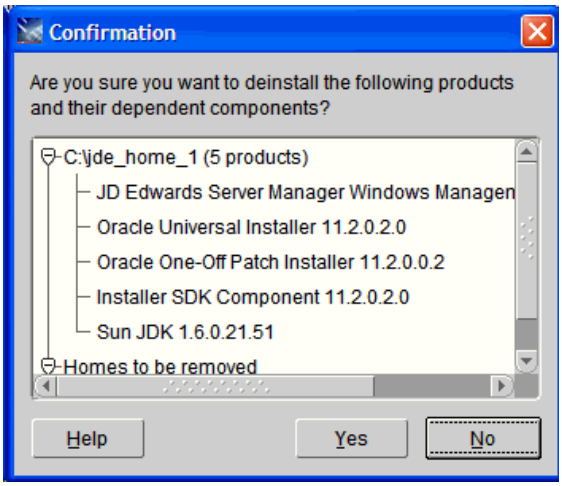
2. On Welcome, click the **Deinstall Products...** button.



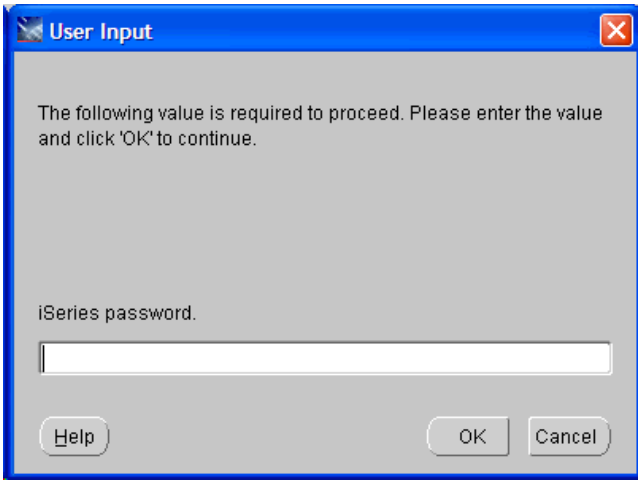
3. On Inventory, with the Contents tab selected, select the check box for the Management Agent that you want to deinstall. For example:

   EOne_ManagementAgent1

4. Click the **Remove** button.

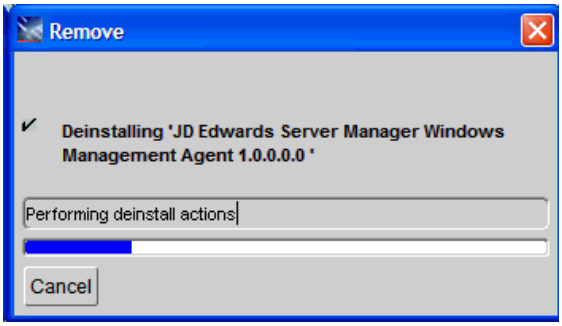


5. On Confirmation, ensure the selected **jde_home** on the target machine is that of the Management Agent that you want to install, and click the **Yes** button.

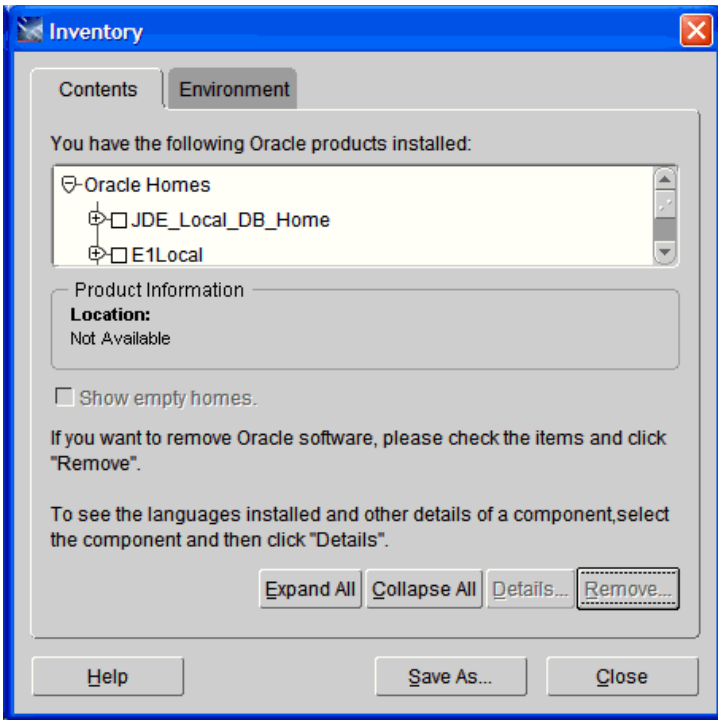


6. On the User Input dialog, enter the iSeries password.
7. Click the **OK** button.

   A deinstallation progress panel is displayed:

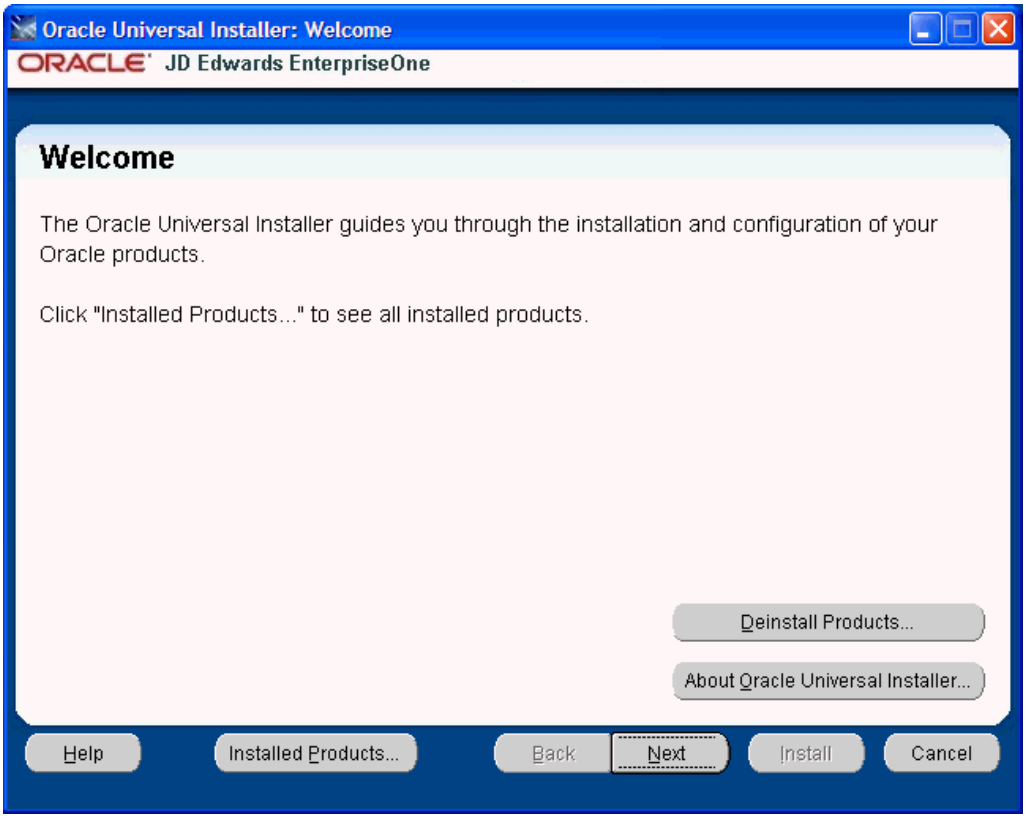


8. When the deinstallation complete, the Inventory screen is displayed.

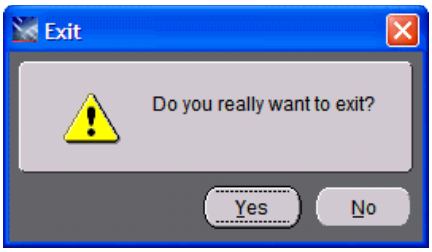


9. On Inventory, verify that the selected home for the Management Agent that you deinstalled is not displayed.

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.

6

Start, Stop, and Restart a Management Agent

This chapter discusses:

- Section 6.1, "Start a Management Agent"
- Section 6.2, "Stop a Management Agent"
- Section 6.3, "Restart a Management Agent"

6.1 Start a Management Agent

You can start the Management Agent by using a script that is delivered when the Management Agent is installed. The script resides on the machine on which you installed the Management Agent and is typically located in these platform-dependent directories:

- Section 6.1.1, "Microsoft Windows"
- Section 6.1.2, "UNIX"
- Section 6.1.3, "OS400 (IBM i)"

6.1.1 Microsoft Windows

You can use these methods to start the Management Agent:

- Section 6.1.1.1, "Start a Management Agent as a Service"
- Section 6.1.1.2, "Start a Management Agent from a Script"

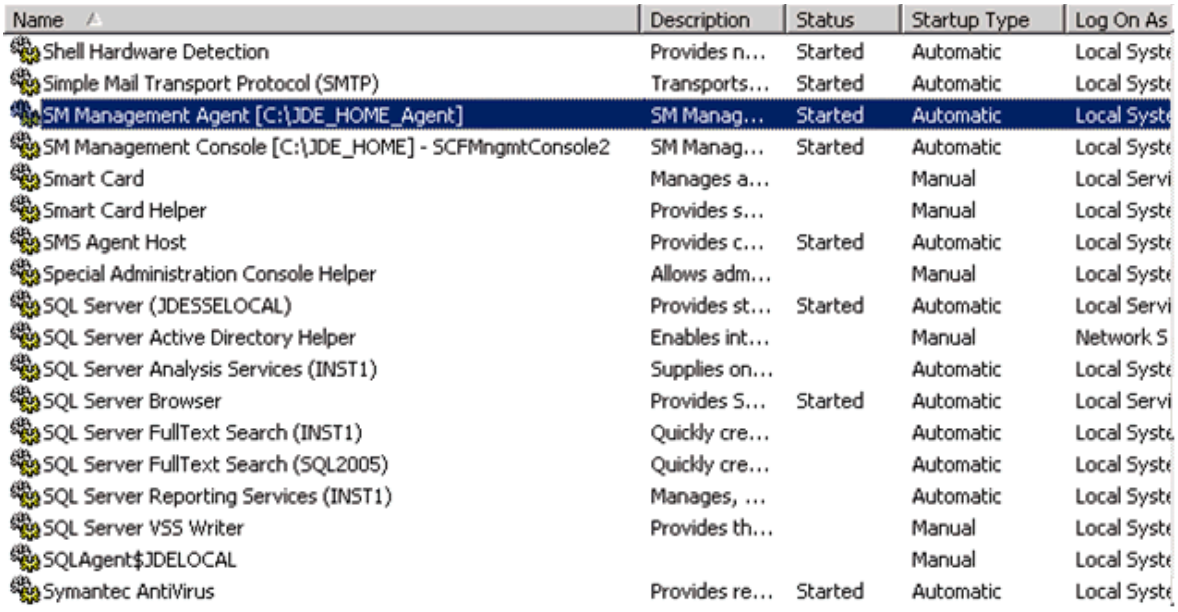
6.1.1.1 Start a Management Agent as a Service

The Management Agent installer creates a windows service that can be used to start, stop, or restart the Management Agent. This is the format of the service name:

SM Management Agent [install_location\JDE_HOME]

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

For example:



Name	Description	Status	Startup Type	Log On As
Shell Hardware Detection	Provides n...	Started	Automatic	Local Syste
Simple Mail Transport Protocol (SMTP)	Transports...	Started	Automatic	Local Syste
SM Management Agent [C:\JDE_HOME_Agent]	SM Manag...	Started	Automatic	Local Syste
SM Management Console [C:\JDE_HOME] - SCFMngmtConsole2	SM Manag...	Started	Automatic	Local Syste
Smart Card	Manages a...		Manual	Local Servi
Smart Card Helper	Provides s...		Manual	Local Syste
SMS Agent Host	Provides c...	Started	Automatic	Local Syste
Special Administration Console Helper	Allows adm...		Manual	Local Syste
SQL Server (JDESSELOCAL)	Provides st...	Started	Automatic	Local Servi
SQL Server Active Directory Helper	Enables int...		Manual	Network S
SQL Server Analysis Services (INST1)	Supplies on...		Automatic	Local Syste
SQL Server Browser	Provides S...	Started	Automatic	Local Servi
SQL Server FullText Search (INST1)	Quickly cre...		Automatic	Local Syste
SQL Server FullText Search (SQL2005)	Quickly cre...		Automatic	Local Syste
SQL Server Reporting Services (INST1)	Manages, ...		Automatic	Local Syste
SQL Server VSS Writer	Provides th...		Manual	Local Syste
SQLAgent$JDELOCAL			Manual	Local Syste
Symantec AntiVirus	Provides re...	Started	Automatic	Local Syste

6.1.1.2 Start a Management Agent from a Script

You can use this `.bat` file to start the Management Agent:

```
installation_directory\JDE_HOME\SCFHA\startAgent.bat
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

6.1.2 UNIX

You can use this script to start the Management Agent:

```
installation_directory/JDE_HOME/SCFHA/bin/startAgent
```

Note: The path `installation_directory/JDE_HOME` refers to the install location of the Management Agent.

6.1.3 OS400 (IBM i)

In order for the Management Agent to function, it is required that JDK 1.5 be installed on the IBM i machine.

Start the Management Agent as a Background Job

As shown below, you must use the "&" switch as a suffix for the command script in order to start the Management Agent as a background job. Launching the job in this manner means that when you leave the qshell the job will not die.

User Installing, Starting, or Restarting the Management Agent

The user who installs, starts or restarts the agent must have the minimum permissions of *ALLOBJ, *SAVSYS and *JOBCTL is *SECADM. After the Management Agent installation is complete, it will start. It is important to note that when starting the Management Agent the user that is signed onto the IBM i machine is the user that executes the functionality when the

Management Agent is performing Server Manager work. That user must not be a user that has a JD Edwards EnterpriseOne Enterprise Server library in its library list (for example: E900SYS).

Agent Commands

For the Management Agent running on the IBM i platform, you can run these commands from the default /JDEdwards/JDE_HOME/SCFHA folder:

restartAgent

runAgent

startAgent

stopAgent

To submit each command to batch:

1. To stop, start, or restart the Management Agent, log in to OS400 with a user profile which has sufficient privileges to operate these services.

   You should ensure that the job queue that the user belongs to is one that is not interrupted during processing. Because it is interruptible, a job queue such as QINTER might not be the best choice for the job queue in which to run the Management Agent. You should consider this warning when selecting the user with the correct permissions and configuration to run the Management Agent processing tasks.

2. To submit the Management Agent action (stop, start, or restart) to batch so it runs in a subsystem other than QINTER:

```
cmd: SBMJOB CMD (STRQSH CMD('cd
       /JDEdwards/JDE_HOME/bin;./startAgent &')) JOB(STARTAGENT)
       JOBQ(QTXSRCH)
```

   where in this example, the job queue is QTXTSRCH, which is a job queue that is delivered by IBM. This job queue has no thread limitation and runs in the QBATCH subsystem.

3. You can use the work with active jobs command to view the processes running under the QBATCH subsystem. For example:

```
cmd: SBMJOB CMD(STRQSH
       CMD('cd /JDEdwards/JDE_HOME/bin;./stopAgent &'))
       JOB(STOPAGENT) JOBQ(QTXTSRCH)
```

```
                         Work with Active Jobs                    ENTSRV1
                                                        08/14/08  12:23:27

CPU %:      .9    Elapsed time:  00:10:33    Active Jobs:    722
                        Current
Opt  Subsystem/Job  User      Type  CPU %  Function        Status
__   QBATCH         QSYS      SBS      .0                  DEQW
__     QPOZSPWP     QSECOFR   BCI      .0  PGM-QZSHSH      EVTW
__     QPOZSPWP     QSECOFR   BCI      .0  JVM-com.jdedwa  JVAW
__     STARTAGENT   QSECOFR   BCH      .0  CMD-STRQSH      TIMW
```

4. If you want to kill the initial `startAgent` job, you can issue this command:

   ```
   cmd: SBMJOB CMD(STRQSH CMD('cd /JDEdwards/JDE_HOME/SCFHA;./stopAgent
   &')) JOB(STOPAGENT) JOBQ(QTXTSRCH)
   ```

   where `QTXTSRCH` is the name of the job queue previously started.

5. To verify the job is killed, you can use this work with active jobs command to view the processes running under the QBATCH subsystem:

   ```
   cmd: WRKACTJOB SBS(QBATCH)
   ```

```
                         Work with Active Jobs                    ENTSRV1
                                                        08/14/08  12:29:22

CPU %:     2.2    Elapsed time:  01:55:35    Active Jobs:    725
                        Current
Opt  Subsystem/Job  User      Type  CPU %  Function        Status
__   QBATCH         QSYS      SBS      .0                  DEQW
```

6.2 Stop a Management Agent

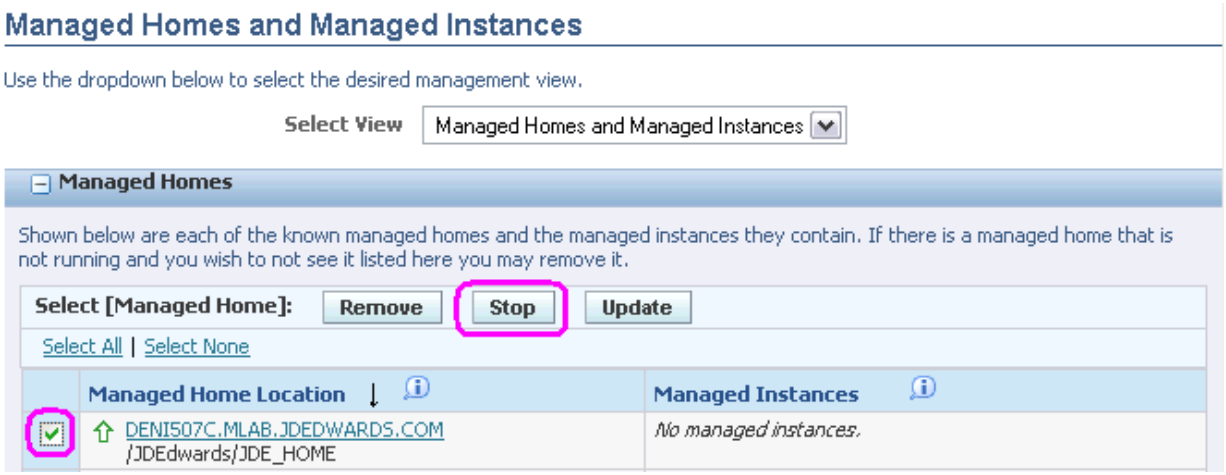
You can use these methods to stop a Management Agent:

- Section 6.2.1, "Stop a Management Agent from the Management Console"
- Section 6.2.2, "Stop a Management Agent Using a Script"
- Section 6.2.3, "Stop a Management Agent as a Service (Microsoft Windows only)"

6.2.1 Stop a Management Agent from the Management Console

Using the Management Console, Server Manager users with appropriate permissions (refer to Chapter 21, "Administer Management Console Users and User Groups") can stop a specific Management Agent, each of which is uniquely associated with a specific Managed Home. You can specify which Management Agent to stop by checking the check box of the associated Managed Home and then clicking the *Stop Agent* button on the Management Console.

Note: If a user does not have sufficient privileges to stop a Management Agent, the *Stop Agent* button on the Management Console is disabled (grayed out).



6.2.2 Stop a Management Agent Using a Script

You can stop a Management Agent using a script that resides on the machine on which you installed the Management Agent. Typically the `stopAgent` script is located in a platform-dependent directory:

- Microsoft Windows
- UNIX
- OS400 (IBM i)

6.2.2.1 Microsoft Windows

You can use this `.bat` file to stop the Management Agent:

```
installation_directory\JDE_HOME\SCFHA\stopAgent.bat
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

6.2.2.2 UNIX

You can use this script to stop the Management Agent:

```
installation_directory\JDE_HOME\SCFHA\stopAgent
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

6.2.2.3 OS400 (IBM i)

Use this command within qshell to stop the Management Agent:

```
JDE_HOME/SCFHA/stopAgent
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

6.2.3 Stop a Management Agent as a Service (Microsoft Windows only)

Refer to Start a Management Agent from a Script in this chapter.

6.3 Restart a Management Agent

You can restart (that is, “bounce”) a Management Agent that is currently running using a script that resides on the machine on which you installed the Management Agent. Typically the `restartAgent` script is located in a platform-dependent directory:

- Microsoft Windows
- UNIX
- OS400 (IBM i)

6.3.1 Microsoft Windows

You can use this `.bat` file to restart the Management Agent:

```
installation_directory\JDE_HOME\SCFHA\restartAgent.bat
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

6.3.2 UNIX

You can use this script to restart the Management Agent:

```
installation_directory\JDE_HOME\SCFHA\restartAgent
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

6.3.3 OS400 (IBM i)

User Installing, Starting, or Restarting the Management Agent. The user who installs, starts or restarts the agent must have the minimum permissions of *ALLOBJ, *SAVSYS and *JOBCTL is *SECADM. After the Management Agent installation is complete, it will start. It is important to note that when starting the Management Agent the user that is signed onto the IBM i machine is the user that executes the functionality when the Management Agent is performing Server Manager work. That user must not be a user that has a JD Edwards EnterpriseOne Enterprise Server library in its library list (for example: E900SYS).

Use this command within qshell to stop the Management Agent:

```
JDE_HOME/SCFHA/restartAgent
```

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Agent.

7

Start, Stop, and Restart the Management Console

This chapter discusses:

- Section 7.1, "Start, Stop, and Restart the Management Console as a Service"
- Section 7.2, "Start, Stop, and Restart the Management Console from a Script"

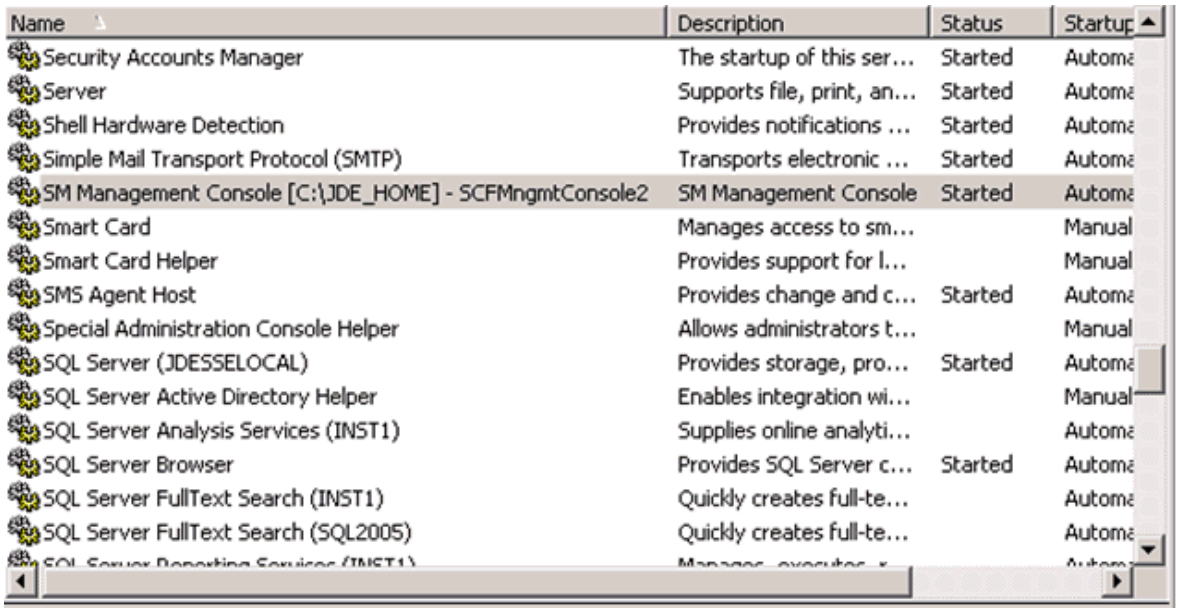
7.1 Start, Stop, and Restart the Management Console as a Service

The Management Console installer creates a Microsoft Windows service that can be used to start, stop, and restart the Management Console. This is the format of the service name:

SM Management Console [install_location\JDE_HOME]

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Console.

For example:



7.2 Start, Stop, and Restart the Management Console from a Script

In addition to installing the Management Console service, the Management Console installer also delivers scripts that you can used to start, stop, or restart (that is, bounce) the Management Console.

- *Start Script*

  If the Management Console is stopped, you can start it by using this `.bat` file

  `installation_directory\JDE_HOME\bin\startManagementConsole.bat`

- *Stop Script*

  If the Management Console is started, you can stop it by using this `.bat` file

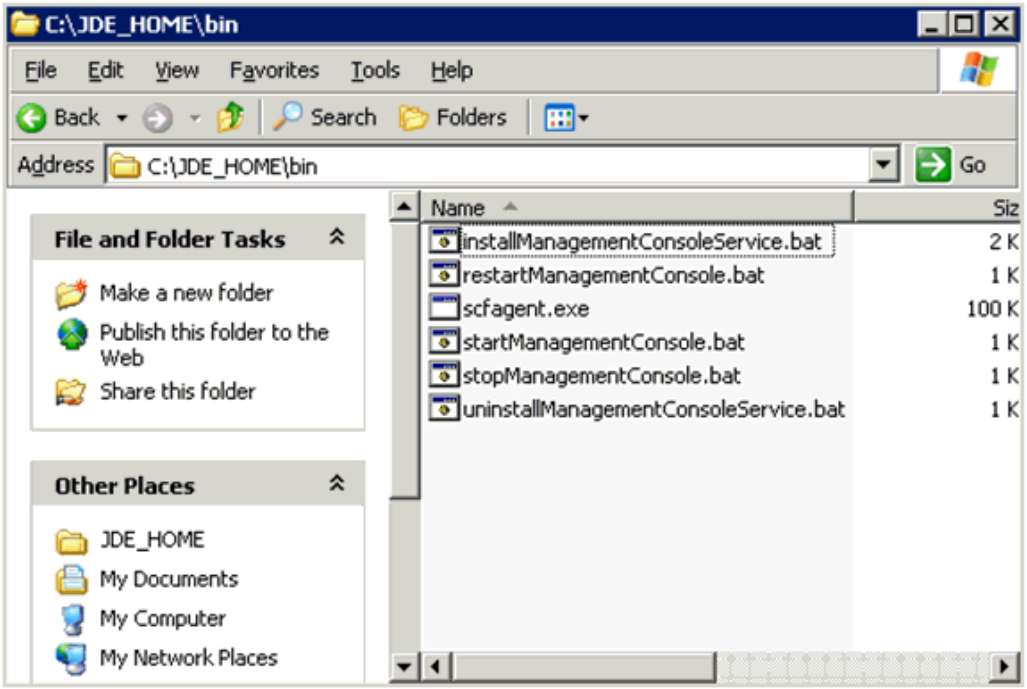
  `installation_directory\JDE_HOME\bin\stopManagementConsole.bat`

- *Restart Script*

  If the Management Console is running, you can stop and restart (that is, bounce) it by using this `.bat` file

  `installation_directory\JDE_HOME\bin\restartManagementConsole.bat`

Note: The path `installation_directory\JDE_HOME` refers to the install location of the Management Console.



8

User Interface for the Management Console

This chapter describes:

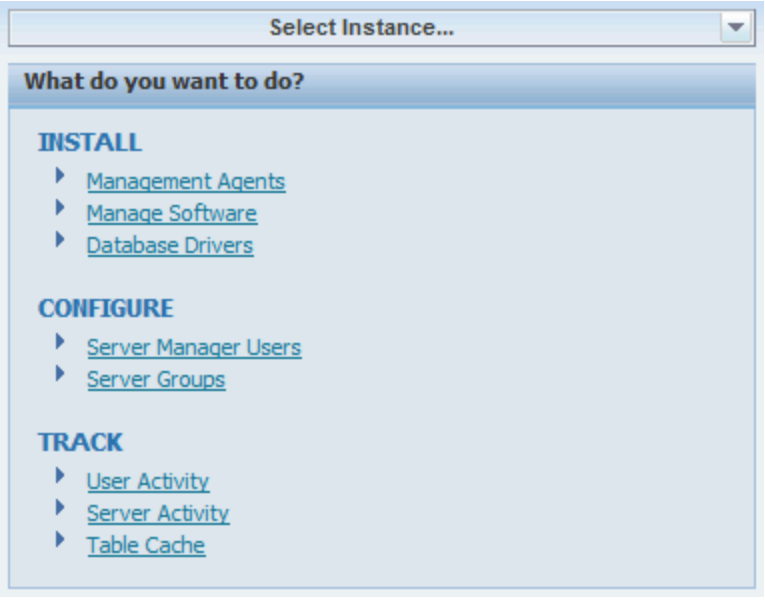
- Section 8.1, "User Interface Layout"
- Section 8.2, "User Interface Productivity Hints"

8.1 User Interface Layout

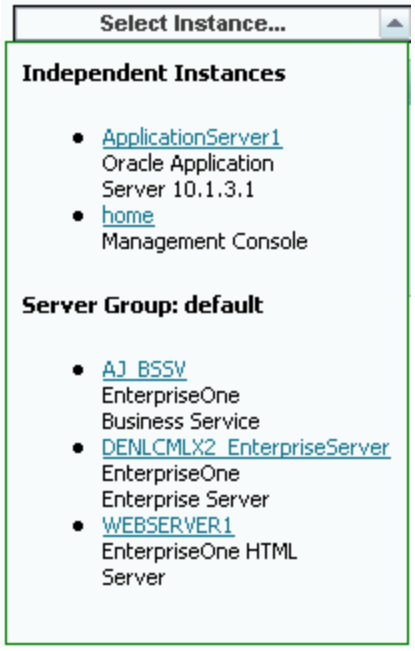
The user interface for the Management Console is comprised of these segments, starting from the top-left most portion of the page:

- Select Instance Dropdown
- Quick Links - What do you want to do?
- Views of the Management Console

8.1.1 Select Instance Dropdown



The *Select Instance dropdown* is available on every Management Console page. It is always located at the top-most portion of the left-hand pane, just above the *What do you want to do?* list.



When you click the *Select Instance... dropdown*, the Management Console displays a list of currently available instances registered with this Management Console. The list is organized by these groups:

- *Independent Instances*

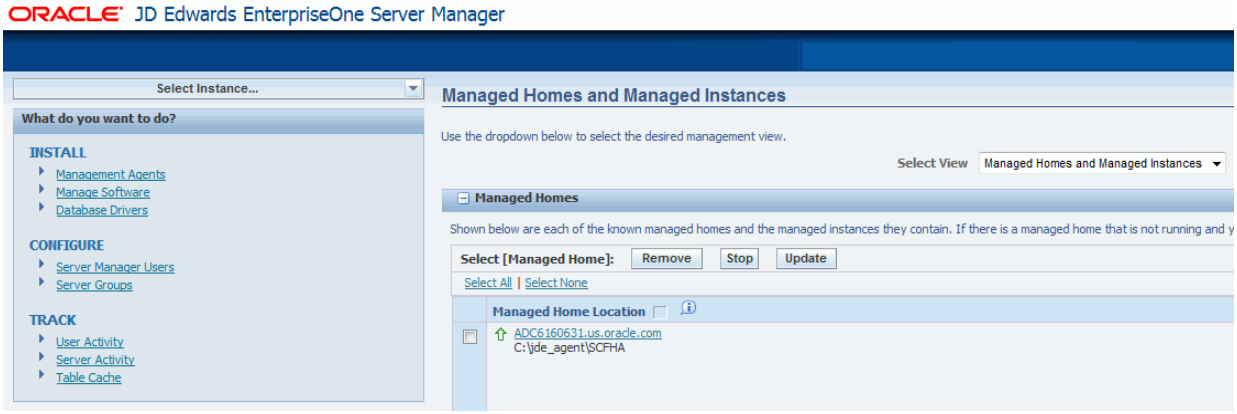
  These are instances not associated with a server group.

- *Server Group: name*

  Where *name* is the name of the server group. For example, *default*.

Each instance is listed by its name, which is a link to the instance, and a description of the instance. If you click the link for the instance, the Management Console displays the management page of the instance.

8.1.2 Quick Links - What do you want to do?



The Management Console displays a section in the left-hand pane of each web page called *What do you want to do?* that provides easy navigation to the Management Console functions for INSTALL, CONFIGURE, and TRACK:

INSTALL

- Management Agents

  Refer to Chapter 5, "Install a Management Agent" of this guide

- Managed Software

  Refer to Chapter 11, "Managed Software Components" of this guide

- Database Drivers

  Refer to Chapter 12, "Manage JDBC Drivers" of this guide

CONFIGURE

- Server Manager Users

  Refer to Chapter 10, "Configure Management Console Users" of this guide

- Server Groups

  Refer to Chapter 9, "Configure the Default Server Group Configuration Settings" and Administer Server Groups of this guide

TRACK

- User Activity

  Refer to "Search for User Resources" of this chapter

- Server Activity

  Refer to Chapter 22, "Monitor JD Edwards EnterpriseOne Servers" of this guide

- Clear Table Cache (Tools Release 9.1 Update 2)

  Refer to Chapter 32, "Clear Table Cache (Tools Release 9.1 Update 2)" of this guide

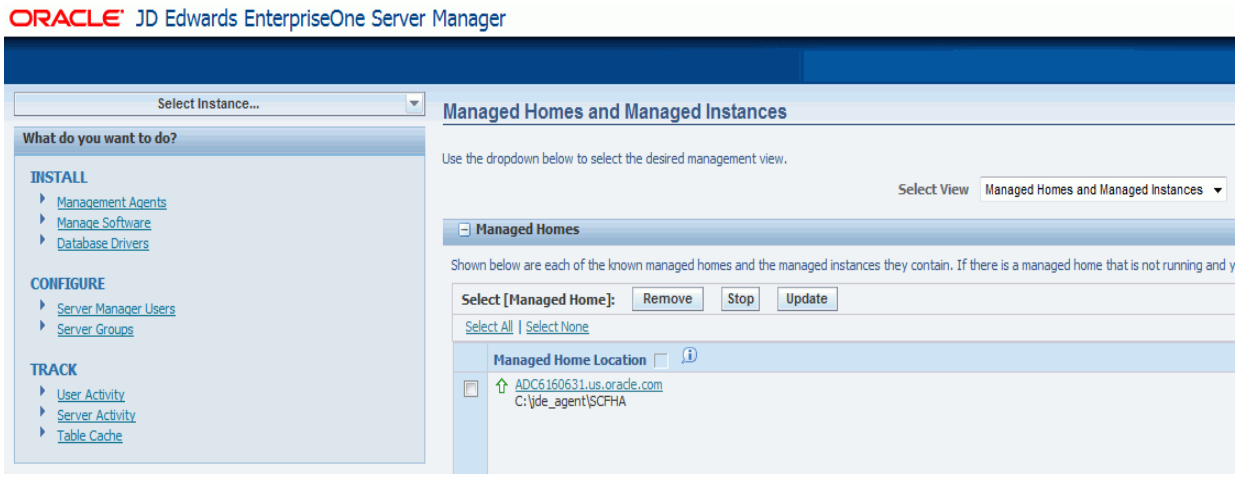
8.1.3 Views of the Management Console

The user interface for the Management Console supports these views:

- Management Dashboard
- EnterpriseOne Servers By Type
- EnterpriseOne Servers By Group
- Search for User Resources

8.1.3.1 Management Dashboard

The Management Dashboard is the entry point into the management application. The web page displays the status of all the Management Agents and Managed Instances. This view shows each of the known Managed Homes and the Managed Instances that they contain. Managed Homes and Managed Instances can be accessed by clicking their links.



To choose the Management Dashboard view of the Management Console, on the Home page, use the Select View dropdown to choose *Management Dashboard*.

Note: This is the default view whenever you start the Management Console.

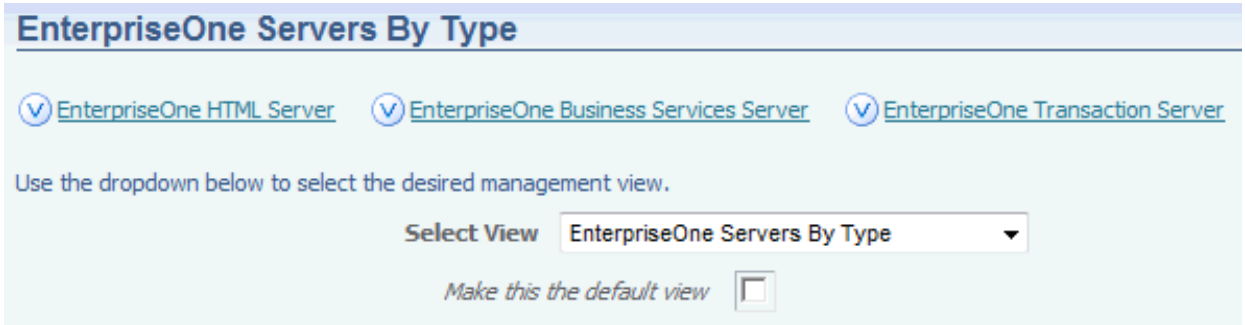
8.1.3.2 EnterpriseOne Servers By Type

The *EnterpriseOne Servers By Type* view of the Management Console lists each logical machine within the management domain of the Server Manager for JD Edwards EnterpriseOne. As such, this view also includes the Management Console itself. The complete list in this view includes:

- JD Edwards EnterpriseOne Management Console
- JD Edwards EnterpriseOne Enterprise Server
- JD Edwards EnterpriseOne HTML Server
- JD Edwards EnterpriseOne Transaction Server
- JD Edwards EnterpriseOne Collaborative Portal Server
- JD Edwards EnterpriseOne Business Services Server

To select the EnterpriseOne Servers view of the Management Console:

1. On the Home page, use the Select View dropdown to choose *EnterpriseOne Servers By Type*.



On the resulting page, the EnterpriseOne servers are organized by types.

2. The grids in this view show the operational status of each installed server and their associated Managed Instances. For any installed servers, you can click on the associated link to Instance Name to work with the instance. The grids lists these items:

   - *Instance Name*

     Identifies the unique name assigned to the Managed Instance at the time it was created or registered.

   - *Server Group*

     Specifies the name of the server group of which the Managed Instance is a member.

   - *State*

     Lists the operational state of the managed instance, where valid values are:

     – Running

     – Stopped

     – Starting

     – Stopping

     – Failed

     – Undetermined

   - *User Activity*

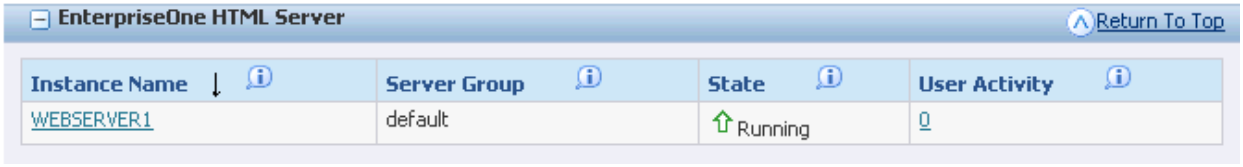
     Provides a summary of the current user activity on the instance.

     For an Enterprise Server, the display includes the number of active CallObject (kernel business function) user and the number of active security server kernel users.

     For an HTML Web Server, the display includes the number of active user sessions.

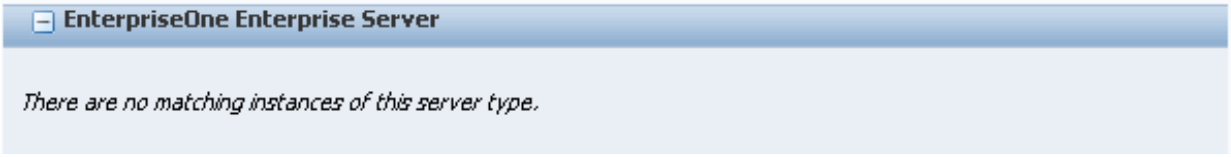
   This screen shot displays an example of the grid for an installed Enterprise Server.

   This screen shot displays an example of the grid for an installed HTML Web Server:



3. The view also lists server types that are available, but not installed.

   This screen shot displays an example of the Management Console if the Enterprise Server is not installed:



8.1.3.3 EnterpriseOne Servers By Group

In Server Manager, you manage servers by grouping similarly purposed servers into logical groupings called server groups. You determine how you want to group servers depending on your particular JD Edwards EnterpriseOne implementation. For example, you may want to put all production servers in one server group and manage development servers in another. Or, you may decide to place servers in separate server groups based on geographical location. How you organize and manage servers in server groups is up to you.

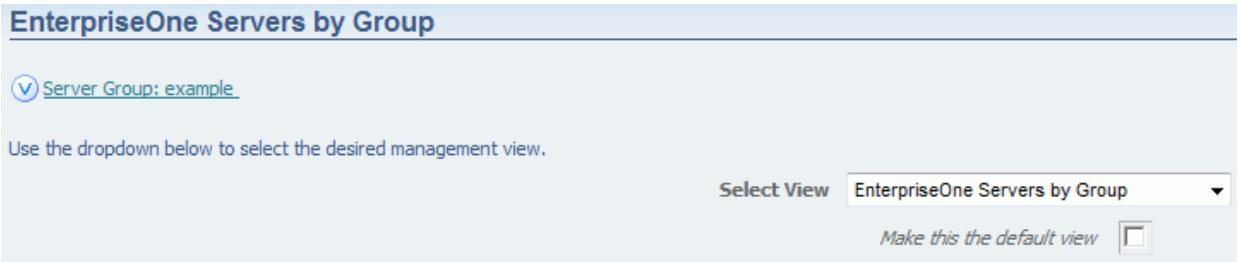
At a minimum, the *EnterpriseOne Servers By Group* view of the Management Console includes a default server group that you can use to initially manage servers. You can move any server from the default server group to a newly created server group. A server cannot belong to more than one server group, including the default server group.

You can include the following types of servers in a server group:

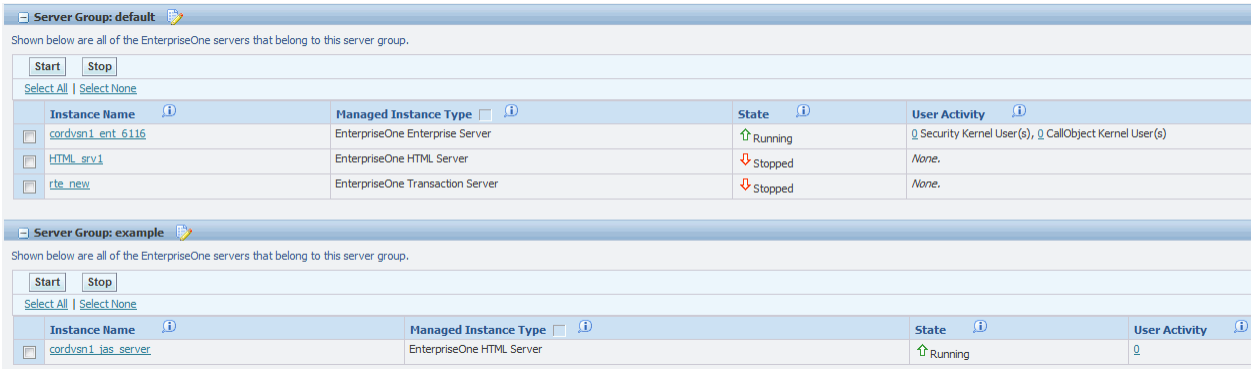
- JD Edwards EnterpriseOne Management Console
- JD Edwards EnterpriseOne Enterprise Server
- JD Edwards EnterpriseOne HTML Server
- JD Edwards EnterpriseOne Transaction Server
- JD Edwards EnterpriseOne Collaborative Portal Server
- JD Edwards EnterpriseOne Business Services Server

To select the *EnterpriseOne Servers By Group* view of the Management Console:

1. On the Home page, use the Select View dropdown to select *EnterpriseOne Servers by Group*.



2. The EnterpriseOne servers are organized by server groups, where every installation will have at least one server group called *default*. For example:



3. The grids in this view show the operational status of each installed server and their associated Managed Instances. You can click on the link in the Instance Name column to access the instance. The grids lists these items:

   - *Instance Name*

     Identifies the unique name assigned to the Managed Instance at the time is was created or registered.

   - *Managed Instance Type*

     Lists the type of server the Managed Instance represents.

   - *State*

     Lists the operational state of the managed instance, where values are:

     – Running

     – Stopped

     – Starting

     – Stopping

     – Failed

     – Undetermined

   - *User Activity*

     Provides a summary of the current user activity on the instance.

     For an Enterprise Server, the display includes the number of active CallObject (kernel business function) user and the number of active security server kernel users.

     For an HTML Web Server, the display includes the number of active user sessions.

4. Start and Stop buttons are available to start and stop individual or multiple servers in a group. (Release 9.1, Update 4).

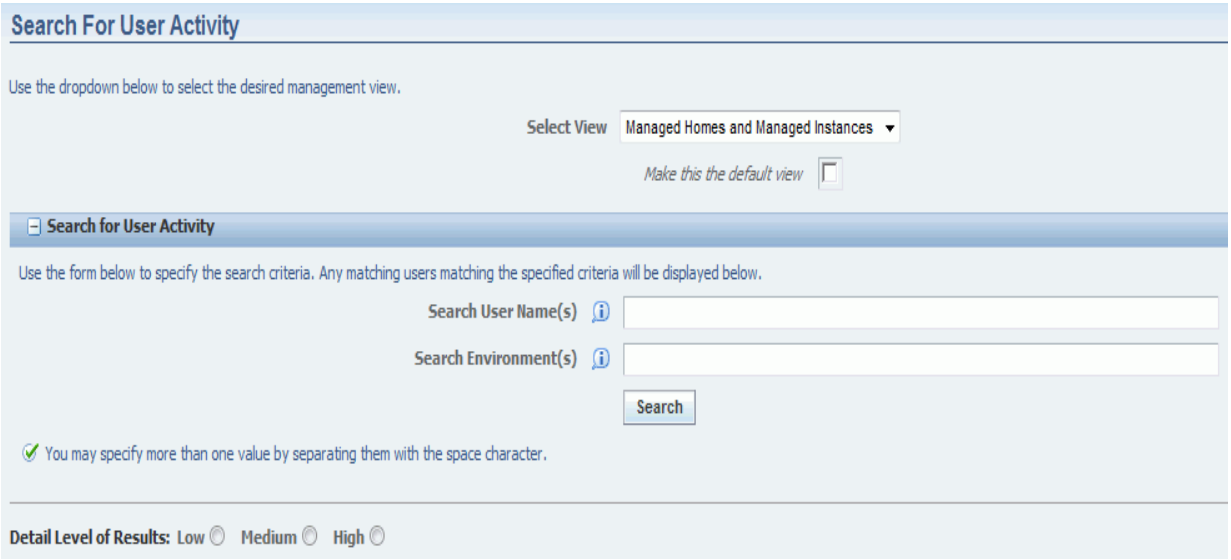
   This screen shot displays an example of the grid for the default server group:

8.1.3.4 Search for User Resources

You can use the Search for User Resources selection of the Management Console to view activity sorted by JD Edwards EnterpriseOne users.

To select the Search for User Resources view of the Management Console:

1. On the Home page, use the Select View dropdown to select *Search for User Resources*.



2. Complete these fields:

   - *Search User Name(s)*

     Enter one or more JD Edwards EnterpriseOne user names to filter the returned results. You should separate multiple names with spaces. Leave this field blank to search for all users.

   - *Search Environment(s)*

     Enter one or more environment names to filter the returned results. Server Manager will only display user resources that are associated with an environment for the environment that you specify. Leave this field blank to search for all environments.

   - *Detail Level of Results*

     Select a radio button for your desired level of results, where the choices are Low, Medium, or High.

3. Click the Search button.

8.2 User Interface Productivity Hints

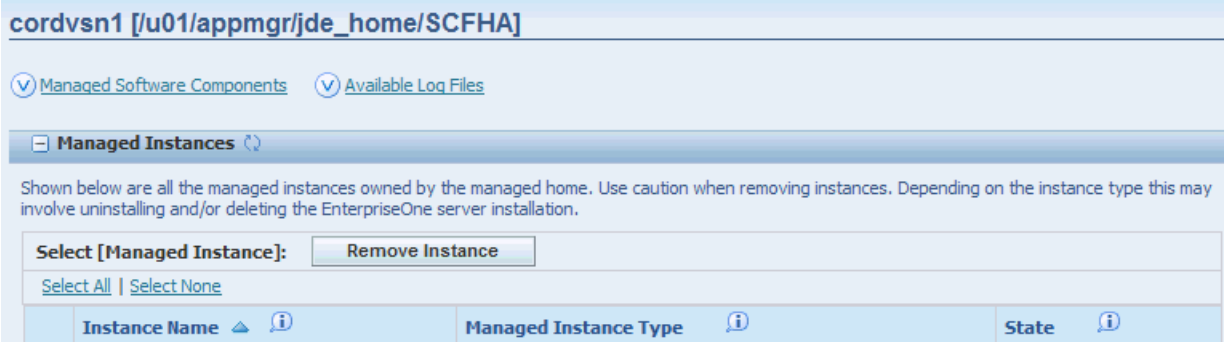
This section describes:

- Grid Multiple Item Selection
- Grid Column Alphanumeric Sorting
- State Column Settings - Managed Homes
- State Column Settings - Managed Instances

8.2.1 Grid Multiple Item Selection

For any grid displayed by the Management Console, the display includes these two links just above the heading of the grid:

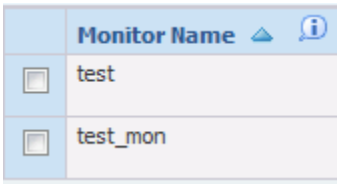
- *Select All*
- *Select None*



8.2.2 Grid Column Alphanumeric Sorting

For any grid displayed by the Management Console, you can alphanumerically sort the content of a column by clicking on the heading title. The first time you click on a heading, an icon appears indicating the column is sorted in ascending order, as indicated by a downward pointing arrow to the right of the heading text.

If you click the heading title again, the sort toggles to descending, as indicated by an upward point arrow to the right of the heading text. For example:



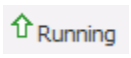
Note: The system keeps track of the sort using a browser cookie (Release 9.1, Update 4).

8.2.3 State Column Settings - Managed Homes

The state of a Managed Home is indicated by a graphical representation in the State column of the grid display. There are two possible states:

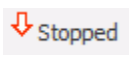
- Running

  A green up arrow indicates the Managed Home is running.



- Stopped

  A red down arrow indicates the Managed Home is stopped.



8.2.4 State Column Settings - Managed Instances

The state of a Managed Instance is indicated by description in State column of the grid display. There are three possible states:

- Running
- Stopped
- Undetermined

9

Configure the Default Server Group Configuration Settings

This chapter describes:

- Section 9.1, "Configuring Default Configuration Settings"
- Section 9.2, "Configuring Default Configuration Settings Based on Existing Instance (Release 9.1, Update 4)"

All server groups, including the default server group, contain default configuration settings that you can configure for each type of server that you manage in the Management Console. The default configuration settings allow you to provide the initial configuration settings for a particular server type. This allows you to configure the settings once for multiple servers before you create server instances.

When you create a new server instance, the Management Console applies the default configuration settings for that type of server to the newly created server. For example, in a server group, you can define the default configuration settings for a JD Edwards EnterpriseOne HTML Web Server. Each HTML Web Server that you create in that server group uses the server groups default configuration settings for HTML Web Servers.

You can modify the configuration settings for an individual server as needed. The changes are reflected only in the configuration settings of that particular server and do not affect the default configuration settings for that type of server in the server group. Conversely, modifying the default configuration settings for a server group does not affect the configuration of any servers that have already been created.

Note: When you create a server group, the Management Console copies default configuration settings from the default server group to the new server group. In the new server group, you can modify the default configuration settings as appropriate.

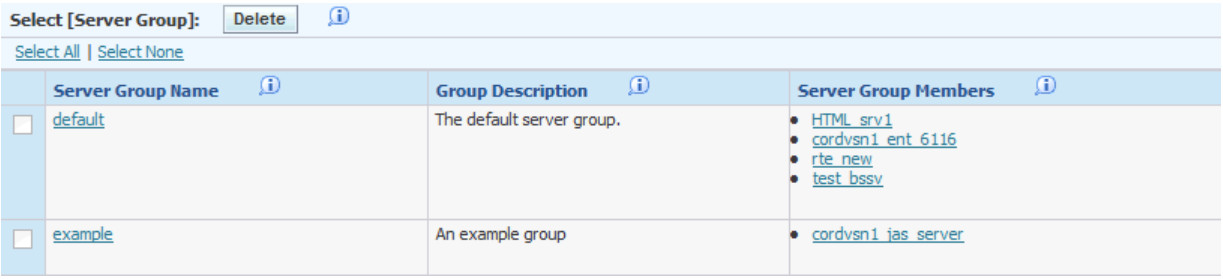
See Also

- Chapter 31, "Administer Server Groups"

9.1 Configuring Default Configuration Settings

To configure the default configuration settings for a server group:

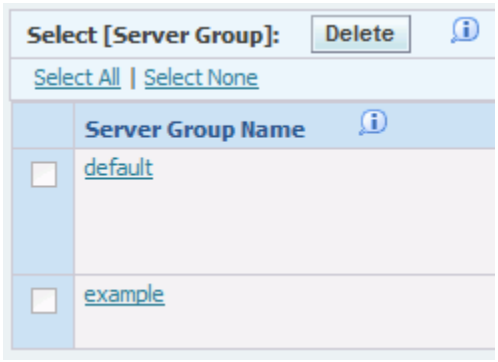
1. In the *What do you want to do now?* section of the Management Console, click the *Server Groups* link.



2. In the *Select [Server Group]* pane of the Server Groups page, click the Server Group Name hyperlink in the Server Group Name row.

Note: If prior to 9.1.4, click the *Configure* icon.

Figure 9–1 Server Group Name Hyperlink



In the Server Group Default Configuration pane, the Management Console lists each type of JD Edwards EnterpriseOne server that could belong to the group and the configuration categories for each.

3. Under the appropriate server type, click a configuration category link.

   Server Manager displays the parameters for that category.

4. Click the information icon next to each setting to view a definition of the parameter. The definition contains a description of the setting and if applicable, a set of valid values.

   If a set of valid values exists, the Management Console displays these values in a dropdown menu.

Note: There might be some configuration items that are installation-specific and therefore not displayed in the default configuration template. These settings are automatically configured for a new server when it is created.

For example:

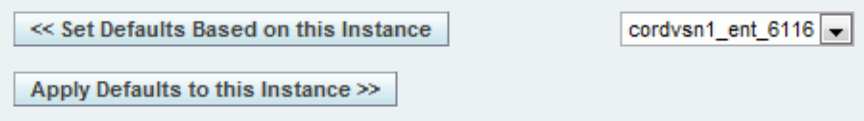
9.2 Configuring Default Configuration Settings Based on Existing Instance (Release 9.1, Update 4)

You can set server group defaults based on an existing instance. You may set the server group defaults based on an instance in the group, or apply the current server group default values to an instance in the group.

To configure the default configuration settings based on an existing instance:

1. In the Server Group Default Configuration section of the Configure Server Group default page; select the existing instance from the dropdown menu.

Figure 9–2 Server Group Default Configuration



2. Select the << *Set defaults Based on this Instance* button to set the server group defaults based on an existing instance.
3. Select the *Apply defaults to this Instance* >> button to apply the current server group default values to an instance group.

10

Configure Management Console Users

Management Console users are JD Edwards EnterpriseOne users that you import from JD Edwards EnterpriseOne. You determine which JD Edwards EnterpriseOne users should have access to the Management Console and assign each user to user groups, which are used to define the actions the users may perform.

An authorized user signs into the Management Console with JD Edwards EnterpriseOne credentials; a separate user ID and password are not required. The Management Console uses a JD Edwards EnterpriseOne security server for user authentication. The Management Console employs user groups as an efficient way to manage permissions and servers. Instead of administering these items at the user level, you can associate permissions with a user group.

For example, you might assign a set of users to a user group that allows the users to view the log files of a particular group of servers but not allow the users to start or stop the servers. You might also create a user group that enables its group members to completely administer the development servers but not to see the production servers within the Management Console application.

The Management Console user repository stores user group definitions, server group definitions, and authorization information.

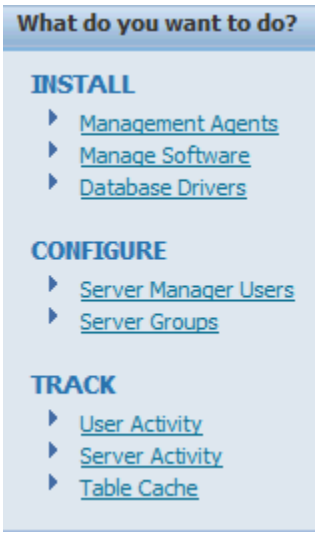
Refer to these applicable tasks in Advanced Console Administration part of this guide:

- Configure the Management Console for User Setup
- Manage Management Console Users
- Manage User Groups
- Assign Server Manager Permissions
- Run the User Access Report

11

Managed Software Components

You access *Managed Software Components* by clicking the *Manage Software* link within the *What do you want to do?* pane. Once you have uploaded the Managed Software Components, you can distribute them to Managed Home Locations where you plan to create new server instances. Or, if the software component is a new version of the Management Console you can use it to update the Management Console itself.

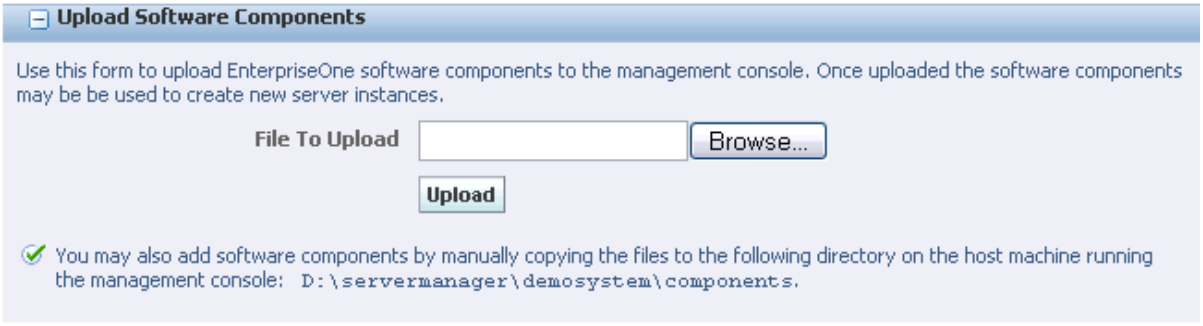


This chapter discusses:

- Section 11.1, "Upload Software Components"
- Section 11.2, "Distribute or Delete Managed EnterpriseOne Software Components"
- Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"
- Section 11.4, "Change a Managed EnterpriseOne Software Component"
- Section 11.5, "View the Software Release History for a Managed Instance"

11.1 Upload Software Components

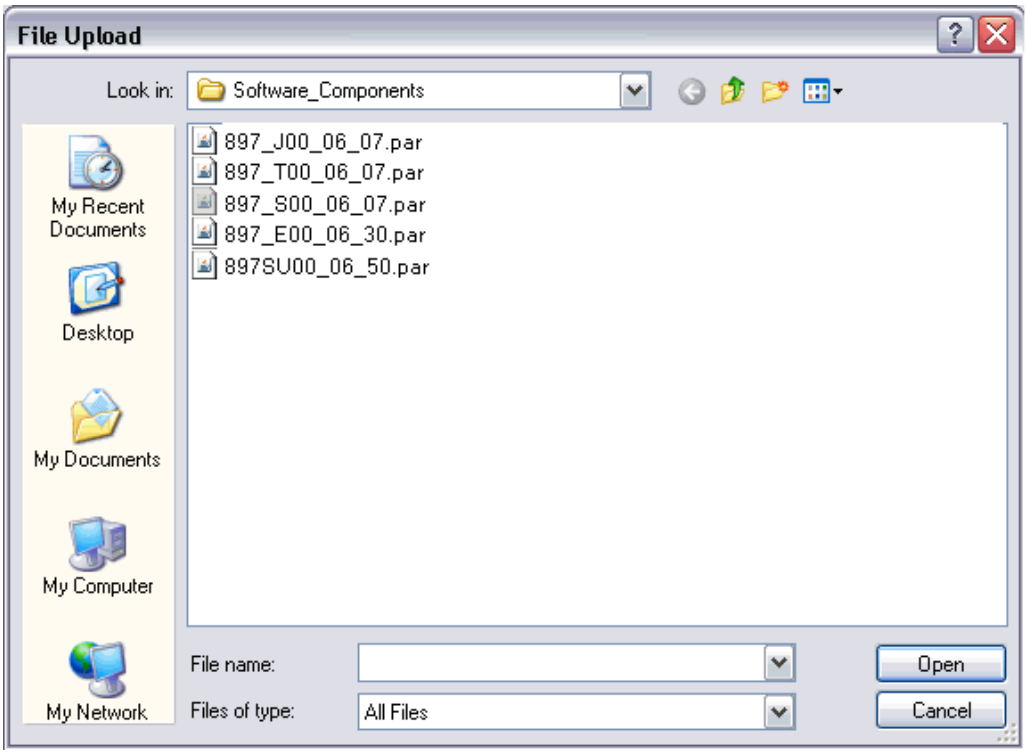
You use the Upload Software Components page to upload JD Edwards EnterpriseOne software components to the Management Console. Once you have uploaded and distributed the Managed Software Components to a Management Agent, you can use them to create new server instances.



To upload Managed Software Components:

1. On Upload Software Components, click the *Browse* button to locate the various .par files for each Managed Software Component. Typically you will obtain these files from Customer Connection using the Change Assistant, although they can also be on CD.

   For example:

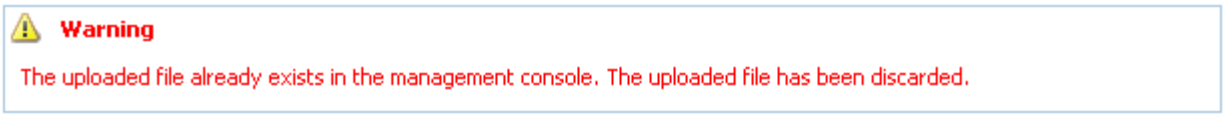


2. On File Upload, select the `.par` file(s) for the Managed Software Component that you wish to upload and click the *Open* button.

3. On Upload Software Components, click the *Upload* button to upload the selected file.

   As soon as the file is successfully uploaded, the Management Console updates the page to include the Managed Software Component.

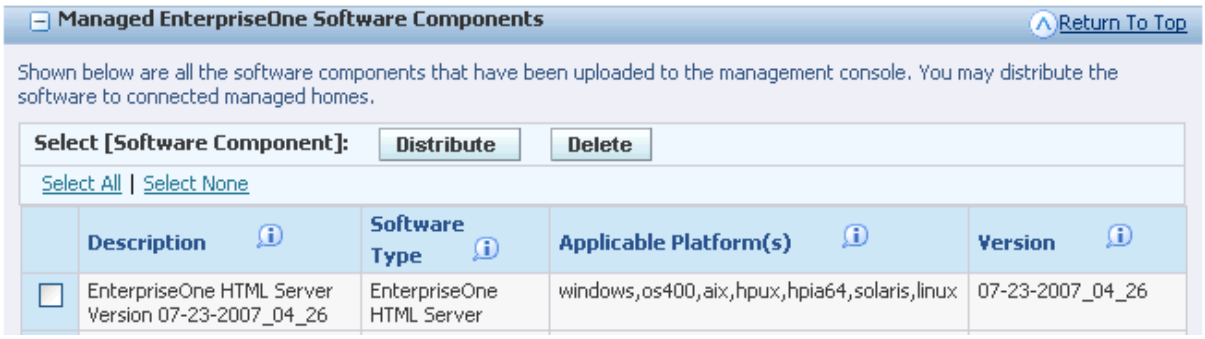
If you attempt to upload a Management Console that already exists with the identical file name, the Management Console displays this warning, discards the request, and does not overwrite the existing file:



Tip: You can also add Managed Software Components by manually copying the files to the `components` directory on the machine running the Management Console. This directory is auto-detected by Management Console and is displayed in the tip section of the Upload Software Components section. For example, in the preceding section, the directory is:

`D:\servermanager\demosystem\components`

11.2 Distribute or Delete Managed EnterpriseOne Software Components

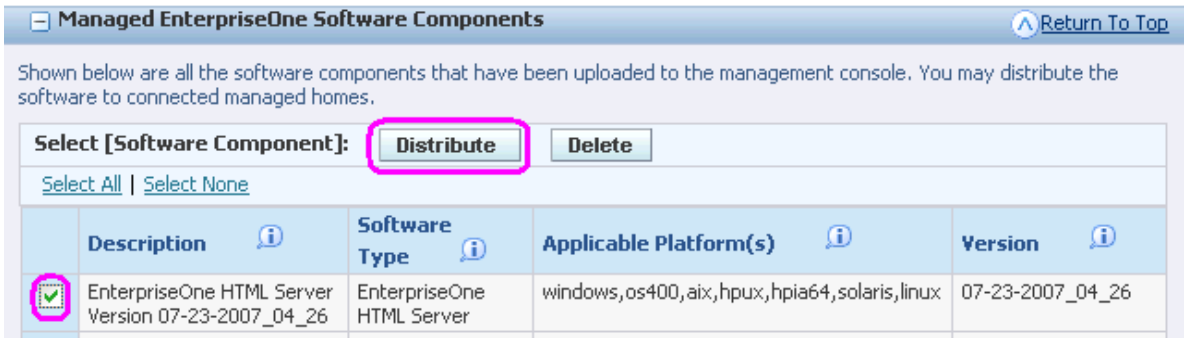


This section discusses these *Managed EnterpriseOne Software Components* functions:

- Distribute Software Components to Managed Homes
- Delete Managed Software Components from the Management Console
- Delete Managed Software Components known to the Management Console

11.2.1 Distribute Software Components to Managed Homes

Once you have uploaded them, the *Managed EnterpriseOne Software Components* page displays all the Managed Software Components that have been uploaded to the Management Console.



To distribute Management Consoles to Managed Homes:

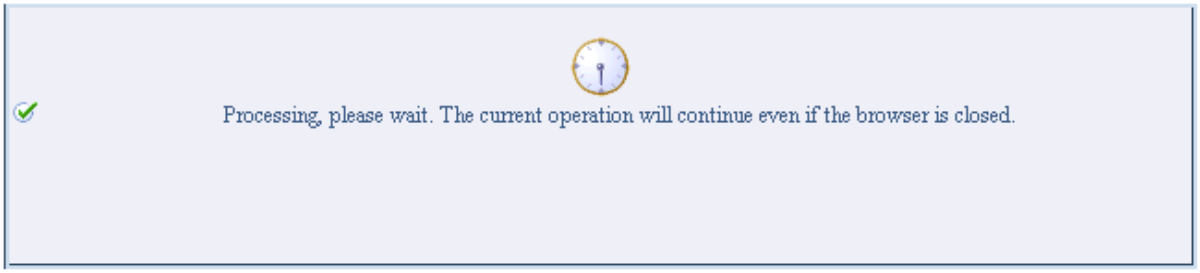
1. On Managed EnterpriseOne Software Components, select one or more available Software Components that you want to distribute to a connect Managed Home.

2. Click the *Distribute* button.

The Management Console displays a page of connected Managed Homes to which you can distribute the selected Software Component.

3. On the list of available Managed Homes to which you can distribute the selected Software Component, select one or more Managed Homes.

4. Click the *Distribute Software* button.



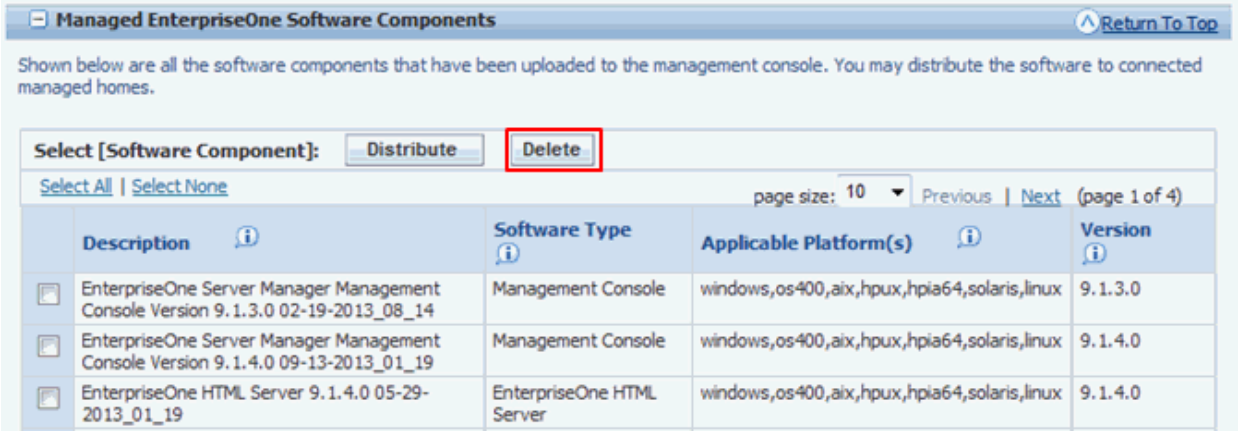
The Management Console displays a progress panel and performs the requested operation.

5. To verify that the selected Software Component is distributed, you can navigate to the Managed Home to which you distributed the Software Component and check the list of software components in Managed Software Components.Management Consoles.

11.2.2 Delete Managed Software Components from the Management Console

To delete Managed Software Components from the Management Console:

1. In the *What do you want to do?* section, click on the link for *Manage Software*.



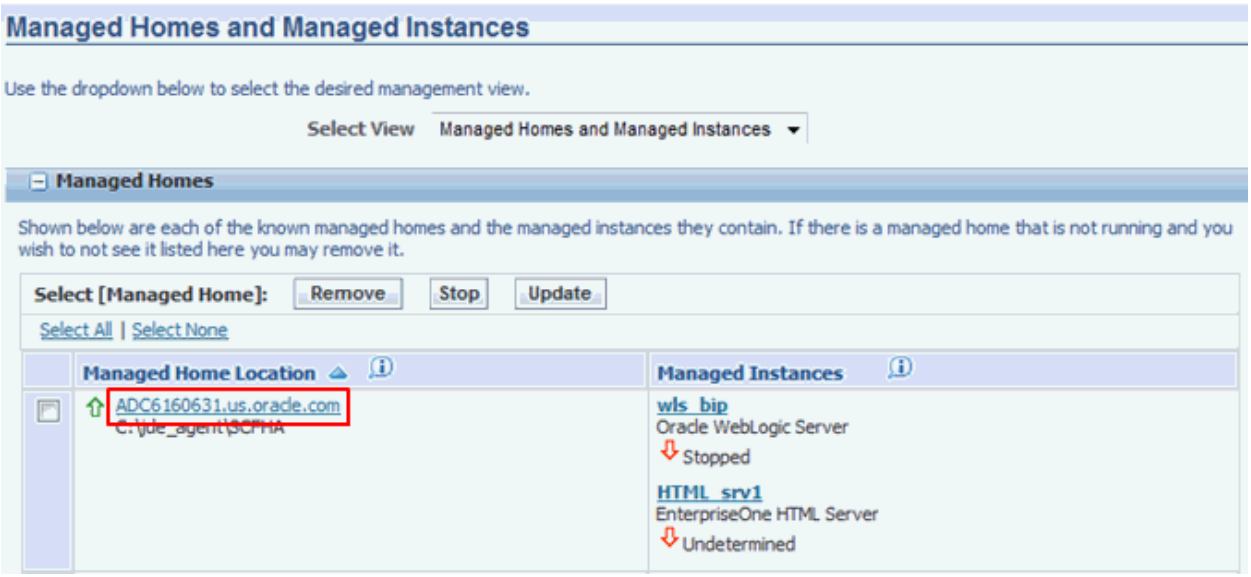
2. On the Managed Software Components section, use the check box to select one or more Managed Software Components to delete.
3. Click the *Delete* button.

4. On the confirmation dialog, click OK to perform the requested deletion.

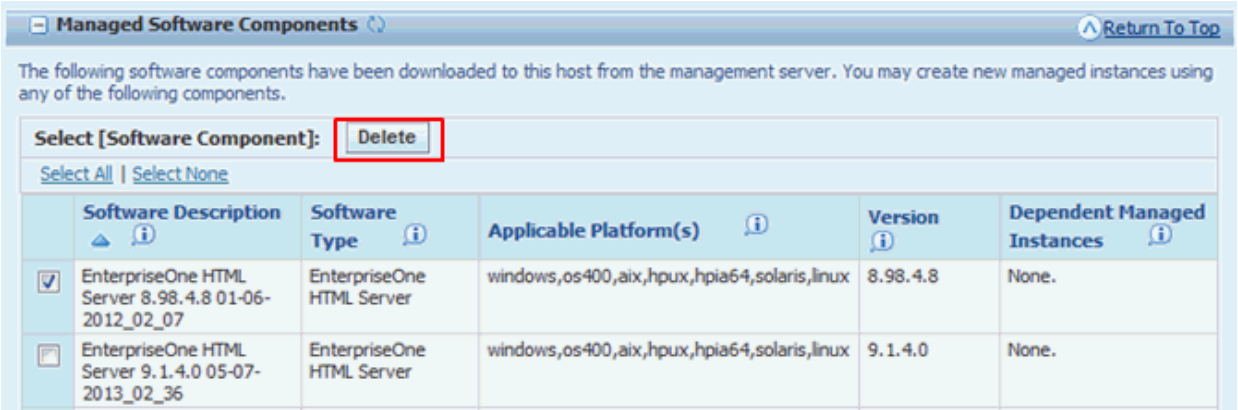
You cannot delete a Software Component that has a Dependent Managed Instance. Such instances are displayed in the last column of the Managed Software Components grid.

11.2.3 Delete Managed Software Components known to the Management Console

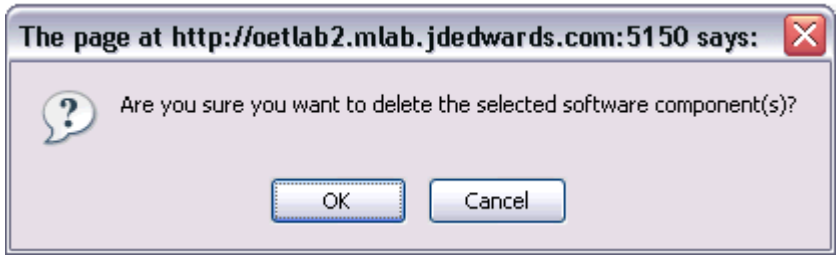
To delete Managed Software Components known to the Management Agent:



1. On the Managed Homes and Managed Instances page, click on the link to a Managed Home.



2. On the Managed Software Components section, use the check box to select one or more Managed Software Components to delete.
3. Click the *Delete* button.



4. On the confirmation dialog, click OK to perform the requested deletion.

You cannot delete a Software Component that has a Dependent Managed Instance. Such instances are displayed in the last column of the Managed Software Components grid.

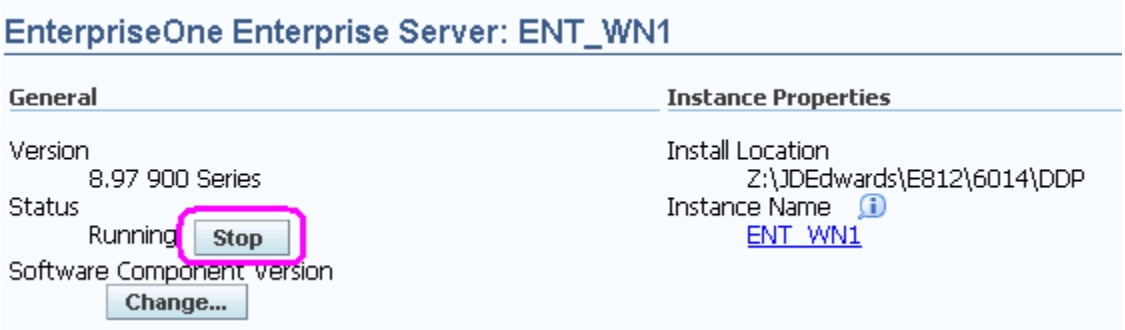
11.3 Start or Stop a Managed EnterpriseOne Software Component

When you click the link for a Managed Instance, the Instance Name page displays information in two categories:

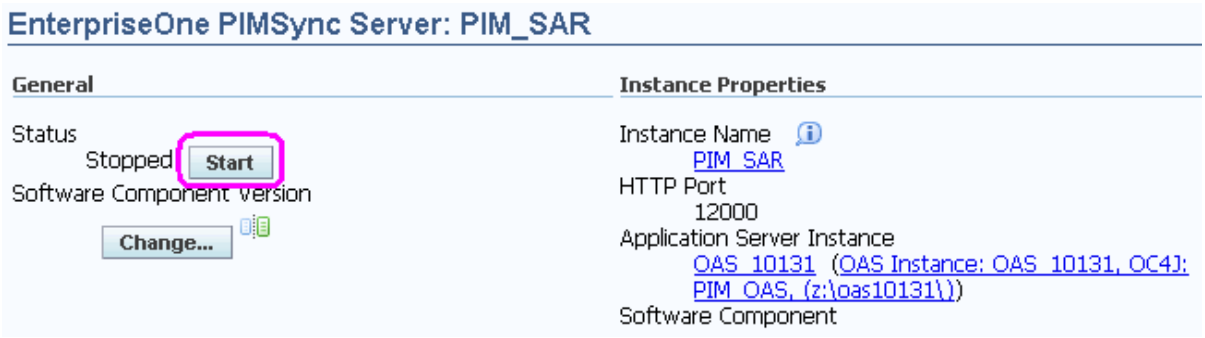
- General
- Instance Properties

The General section of the page shows the status of the Managed Instance. If the status is either *Started* or *Stopped*, the page contains either the *Stop* or *Start* button, as appropriate. If the status of the Managed Instance is undetermined, the page does not contain either button.

For example, if the status is Running, you can stop the instance by pressing the Stop button as shown below:



Also for example, if the status is Stopped, you can start the instance by pressing the Start button as shown below:

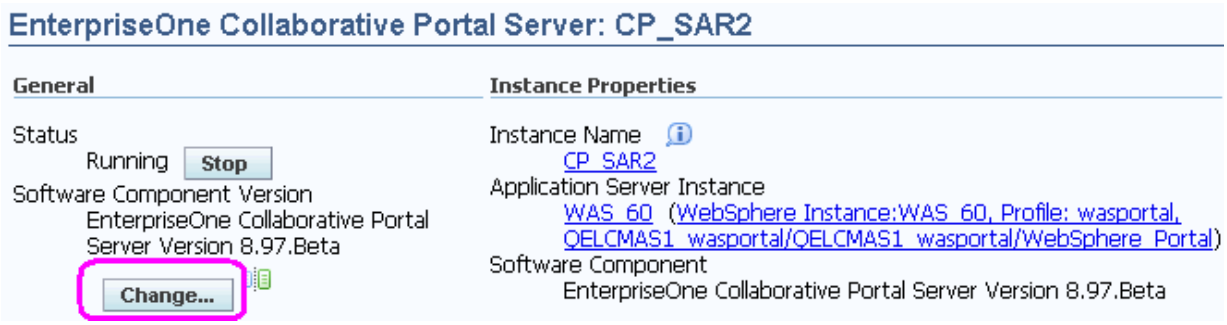


11.4 Change a Managed EnterpriseOne Software Component

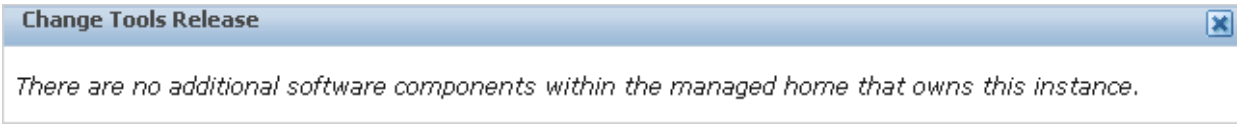
When you click the link for a Managed Instance, the Instance Name page displays information in two categories:

- General
- Instance Properties

In the General section of the page contains a section for *Software Component Version*, under which is a *Change* button.



If there is only a single version of the Software Component associated with this Managed Instance, clicking the *Change* button displays this *Change Tools Release* dialog that indicates there is no component available to which to change:



If multiple versions of the Software Component are available to the Management Console, clicking the *Change* button displays the *Change Tools Release* dialog that lists each available Software Component. For example:

To change a Software Component:

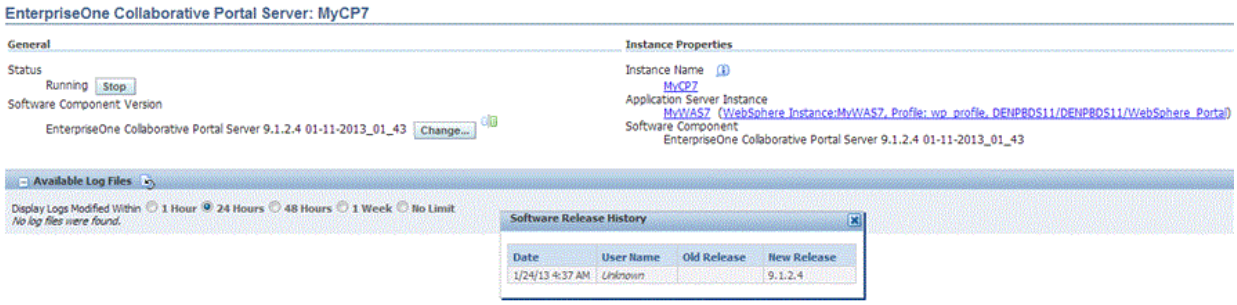
1. Select the radio button associated with the Management Console to which you wish to change.
2. Click the *Change Component* button.

   There is no confirmation dialog for this action. As soon as you click the *Change Component* button, the Management Console begins the work. You can always revert to your previous version assuming you have a copy of the Software Component for the Management Console to which you want to change.

Note: If you are using WebSphere Application Server and running JD Edwards EnterpriseOne as part of a federated (or clustered) web server, you may need to regenerate the WebSphere global plugin configuration after deploying the newest tools release. This is required when new servlets have been added to the tools release you are deploying.

11.5 View the Software Release History for a Managed Instance

If more than more version of a Software Component has been installed to a Managed Instance the *Software Release History* icon is displayed in the *General* section of the page. For example:



To view the Software Release History for a Managed Instance:

1. Select a Managed Instance for which you wish to view the Software Release History.
2. In the *General* section of the page, click the *Software Release History* icon (refer to preceding graphic).

   The *Software Release History* popup displays these grid items:

   - *Date*
   - *User Name*
   - *Old Release*
   - *New Release*

12

Manage JDBC Drivers

Tip: *Web-Based Servers.* Although not absolutely required, the sequence of installing JDBC drivers on your Management Console machines should precede the installation of any JD Edwards EnterpriseOne web-based server. This sequence is recommended because the process of installing JD Edwards EnterpriseOne web-based servers includes starting the server after the installation is complete. If the requisite JDBC driver is not installed, the JD Edwards EnterpriseOne web-based server cannot communicate with the JD Edwards EnterpriseOne Security Server thus the server cannot start.

Server Manager allows you to centrally manage JDBC drivers that are required to enable the various web-based servers to access their respective databases. Using Server Manager you can upload and install any of these JDBC drivers supported by the JD Edwards EnterpriseOne web-based servers:

- Oracle Database
- MicroSoft SQL Server
- IBM DB2 for Windows or Unix
- IBM DB2 for IBM i

This chapter discusses:

- Section 12.1, "Obtain JDBC Drivers"
- Section 12.2, "Upload JDBC Drivers to the Management Console"
- Section 12.3, "Install JDBC Drivers to J2EE Servers"
- Section 12.4, "Uninstall the JDBC Driver from J2EE Servers"
- Section 12.5, "Install JDBC Drivers to JD Edwards EnterpriseOne Data Access Servers"
- Section 12.6, "Uninstall JDBC Drivers from JD Edwards EnterpriseOne Data Access Servers"

12.1 Obtain JDBC Drivers

You should obtain the required driver files from the database vendor. Once all the required files have been obtained they can be uploaded to the management console. This table lists the requisite JDBC drivers.

Database	JDBC Driver Files
Oracle 9i	classes12.jar

Database	JDBC Driver Files
Oracle 10g (JDK 1.4)	ojdbc4.jar
Oracle 11g (JDK 1.5)	ojdbc5.jar
Oracle 11g (JDK 1.6)	ojdbc6.jar
SQL Server (JDK 1.4/JDK 1.5)	sqljdbc.jar
SQL Server (JDK 1.6)	sqljdbc4.jar
IBM DB2 UDB Type-2 (JDK 1.4/JDK 1.5)	db2java.zip
IBM DB2 UDB Type-4 (JDK 1.4/JDK 1.5)	db2jcc.jar db2jcc_license_cu.jar
IBM DB2 UDB (JDK 1.6)	db2jcc4.jar
IBM DB2 for IBMi (IBM i)	jt400.jar

Beginning with WebLogic 12.1.3, WebLogic is pre-configured to use a bundled Oracle 12c database JDBC driver. This JDBC driver comes pre-installed with the WebLogic Server installation, and no additional steps are required to connect to an Oracle 12c database.

For the Oracle database, you can locate the driver file in these locations:

- Oracle Database

  Your installation of an Oracle database product includes the JDBC Thin driver for use with JDK 1.2 and JDK 1.3.

- Oracle Technology Network (OTN)

  `http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc101040.html`

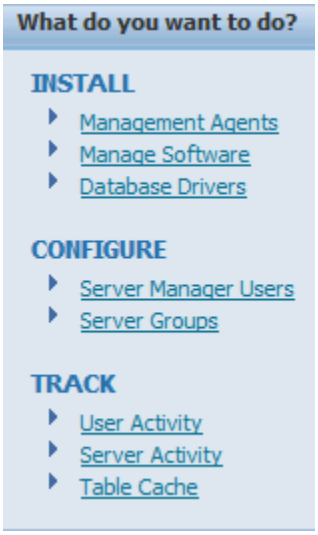
- JD Edwards Update Center

  Search for `classes12.jar` at this link:

  `https://support.oracle.com`

12.2 Upload JDBC Drivers to the Management Console

To upload JDBC drivers to the Management Console:



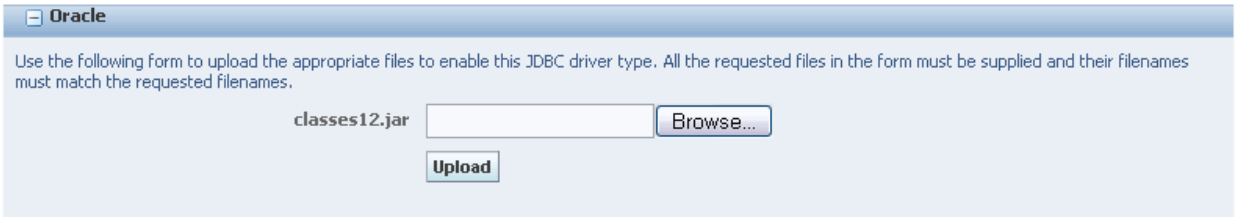
1. Navigate to the JDBC driver management page using this quick link in the *What do you want to do?* section:

   Database Drivers

2. Locate the section corresponding to the type of driver you wish to install.

   The Management Console displays this JDBC Driver Upload form only if you have not previously uploaded the JDBC driver.

   For example, if you have not previously uploaded the Oracle driver, the form looks like this:



3. For each of the required files use the `Browse` button to select the corresponding file previously obtained.

   For example, if you were uploading the driver for Oracle, you would browse to the location of the `classes12.jar file`.

4. Click the Upload button.

   The selected driver file(s) are uploaded to this directory, which contains the Management Console software repository.

   `x:\JDE_HOME\components`

   where *x:* is the drive on which you installed the Management Console, and

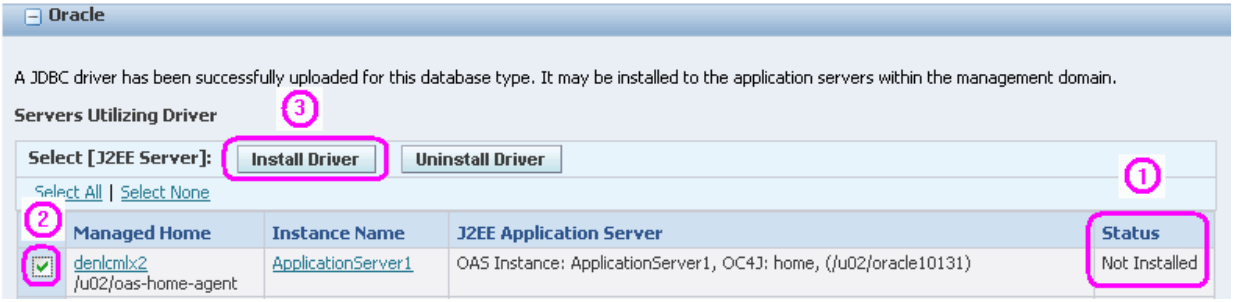
   where `JDE_HOME` is the name that you defined as the home for the Management Console.

   Tip: External to the Management Console, the functional equivalent of using this form to upload the driver is to place it in the specified directory by other means. Once you have placed the driver files in the appropriate directory, refreshing the JDBC Drivers page displays the available application servers on which the drivers are not already installed, but on which they can be installed. Server Manager will not display bundled JDBC drivers that come already installed with Oracle WebLogic Server. The bundled JDBC driver does not need to be uploaded or installed through Server Manager.

12.3 Install JDBC Drivers to J2EE Servers

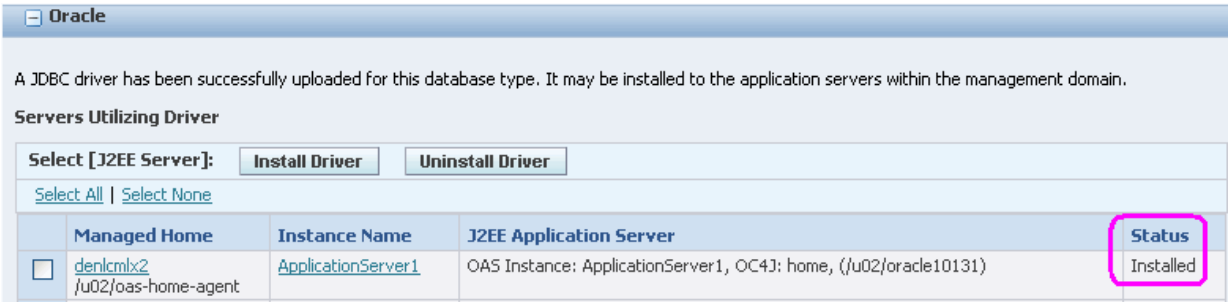
Once the JDBC driver file(s) are successfully uploaded for the chosen database type, they can be installed on the application servers within the management domain.

Management Console installs JDBC drivers in a web container within an Application Server installation. This installation corresponds to an OC4Jinstance within Oracle Application Server and to a J2EE server in IBM WebSphere.



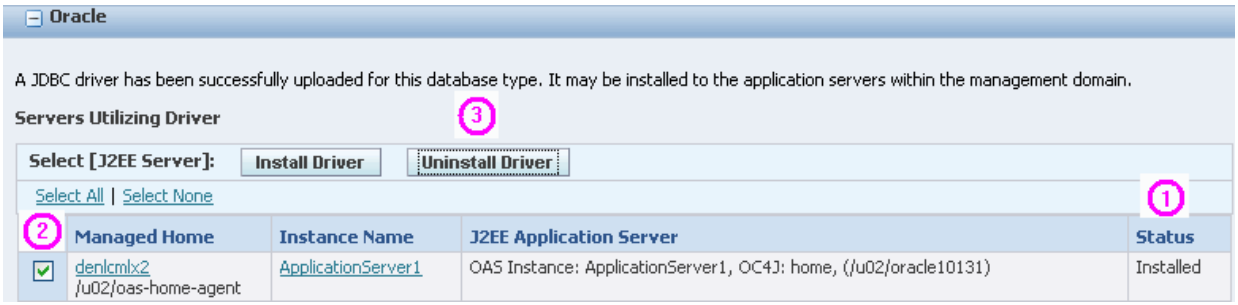
To install a driver on an Application Server:

1. Verify that the Status of the target application server for the installation is *Not Installed*.
2. Select the check box for the application server on which you want to install the driver.
3. Click the *Install Driver* button.
4. Refresh the JDBC Driver page and verify the status is changed to *Installed*.



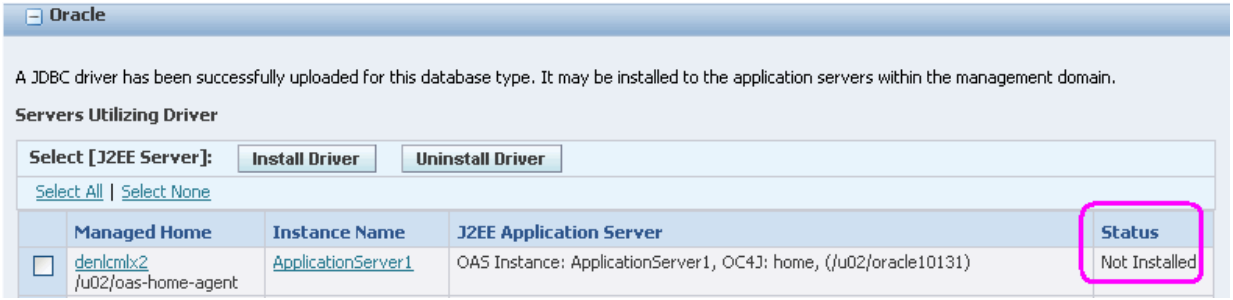
12.4 Uninstall the JDBC Driver from J2EE Servers

To uninstall the JDBC Driver from J2EE Servers:



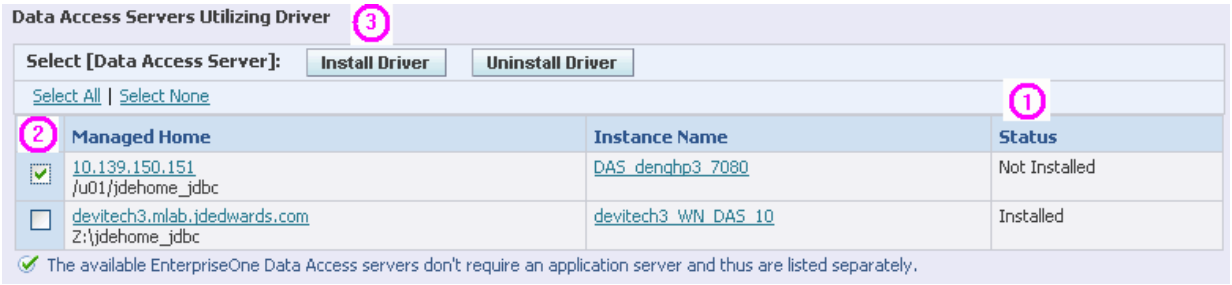
1. Verify that the status of the J2EE server on which you wish to uninstall the JDBC Driver is *Installed*.
2. Enable the check box for the application server on which you want to uninstall the driver.
3. Click the *Uninstall Driver* button.

4. On the resulting confirmation dialog, click the *OK* button to confirm that you want to delete the JDBC driver from the selected server.
5. Refresh the JDBC Driver page and verify that the status is changed to *Not Installed*.



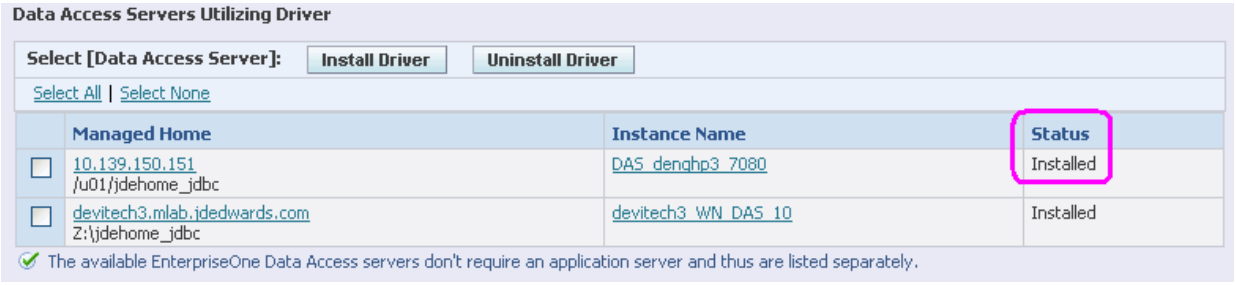
12.5 Install JDBC Drivers to JD Edwards EnterpriseOne Data Access Servers

After you have uploaded the JDBC driver file(s) for the chosen database type, and after you have installed your Data Access Server, you can use Server Manager to install the JDBC driver file(s) to the Data Access Servers within the management domain.



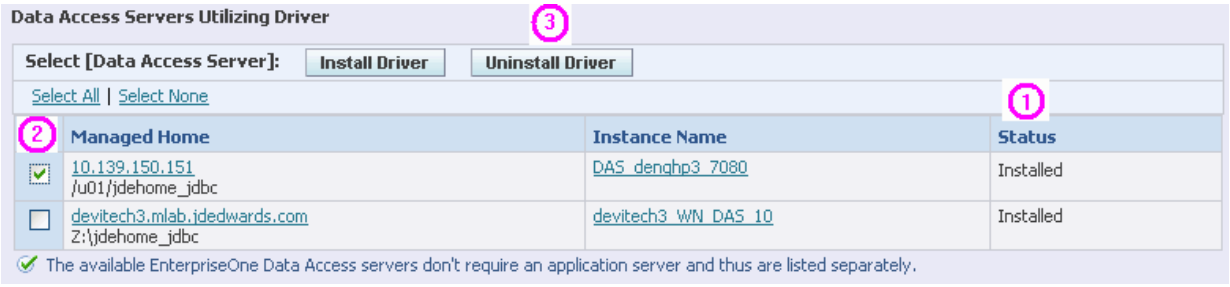
To install a driver on a Data Access Server:

1. Verify that the Status of the target Data Access Server for the installation is *Not Installed*.
2. Select the check box for the Data Access Server on which you want to install the driver.
3. Click the *Install Driver* button.
4. Refresh the JDBC Driver page and verify the status is changed to *Installed*.

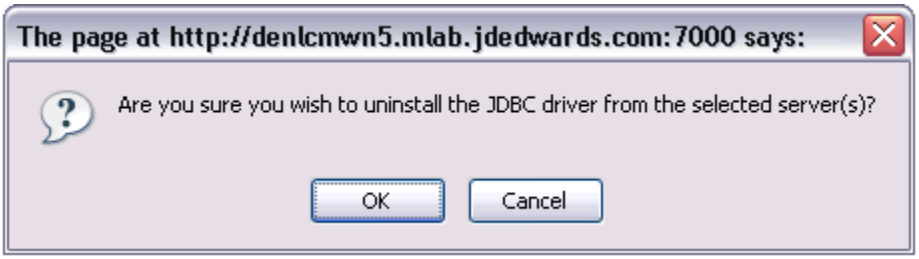


12.6 Uninstall JDBC Drivers from JD Edwards EnterpriseOne Data Access Servers

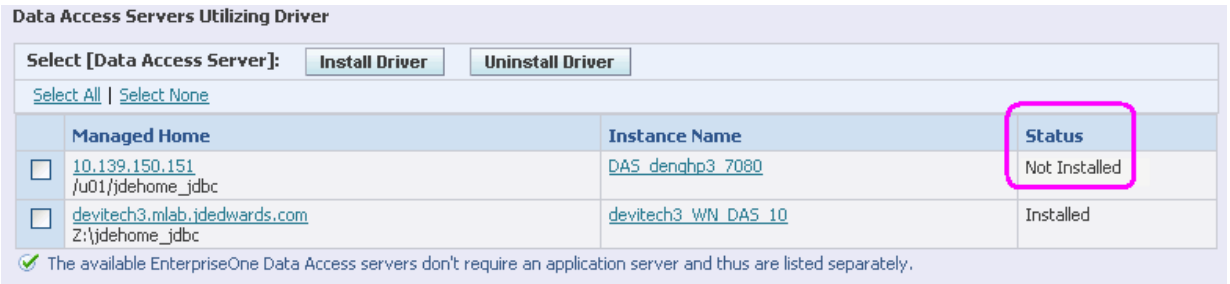
To uninstall the JDBC Driver from JD Edwards EnterpriseOne Data Access Servers:



1. Verify that the status of the Data Access Server on which you wish to uninstall the JDBC Driver is *Installed*.
2. Enable the check box for the Data Access Server on which you want to uninstall the driver.
3. Click the *Uninstall Driver* button.



4. On the resulting confirmation dialog, click the *OK* button to confirm that you want to delete the JDBC driver from the selected server.
5. Refresh the JDBC Driver page and verify that the status is changed to *Not Installed*.



13

Register an Application Server

This chapter discusses:

- Section 13.1, "Register an Oracle Application Server, Version 10.1.3.1"
- Section 13.2, "Register a WebSphere Application Server, Version 7.0"
- Section 13.3, "Register a WebSphere Application Server, Version 8.5 (Tools Release 9.1 Update 2.3)"
- Section 13.4, "Register an Oracle WebLogic Server 11g"
- Section 13.5, "Register an Oracle WebLogic Server 12c"

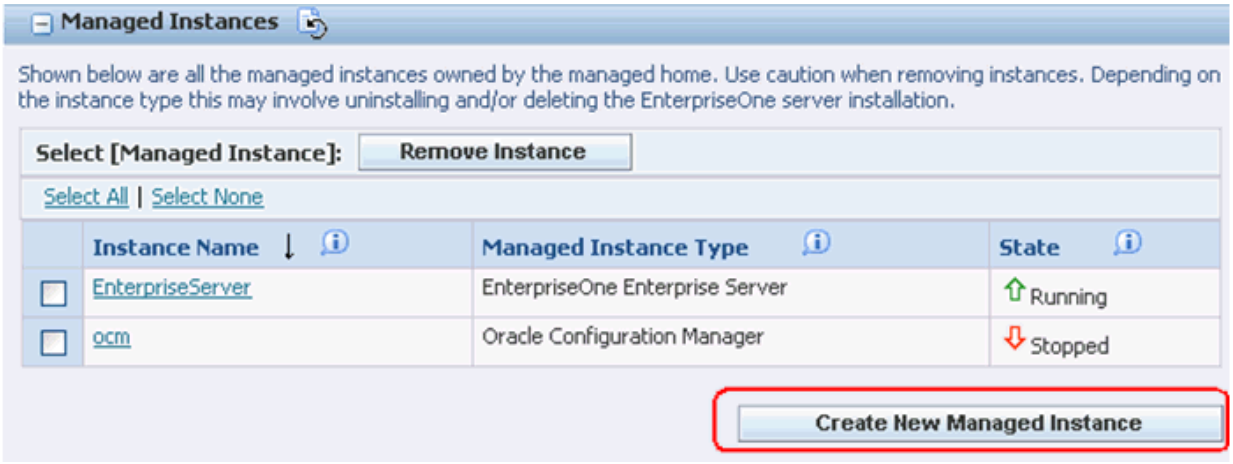
13.1 Register an Oracle Application Server, Version 10.1.3.1

Only Oracle Application Servers that are registered with the Management Console can be managed by the Management Console. The Oracle Application Server must be installed outside of Server Manager. You should always verify that your OAS versions are fix-current per Oracle directives. You should also verify that your version of OAS is compatible with JD Edwards EnterpriseOne servers (for details refer toSection 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide).

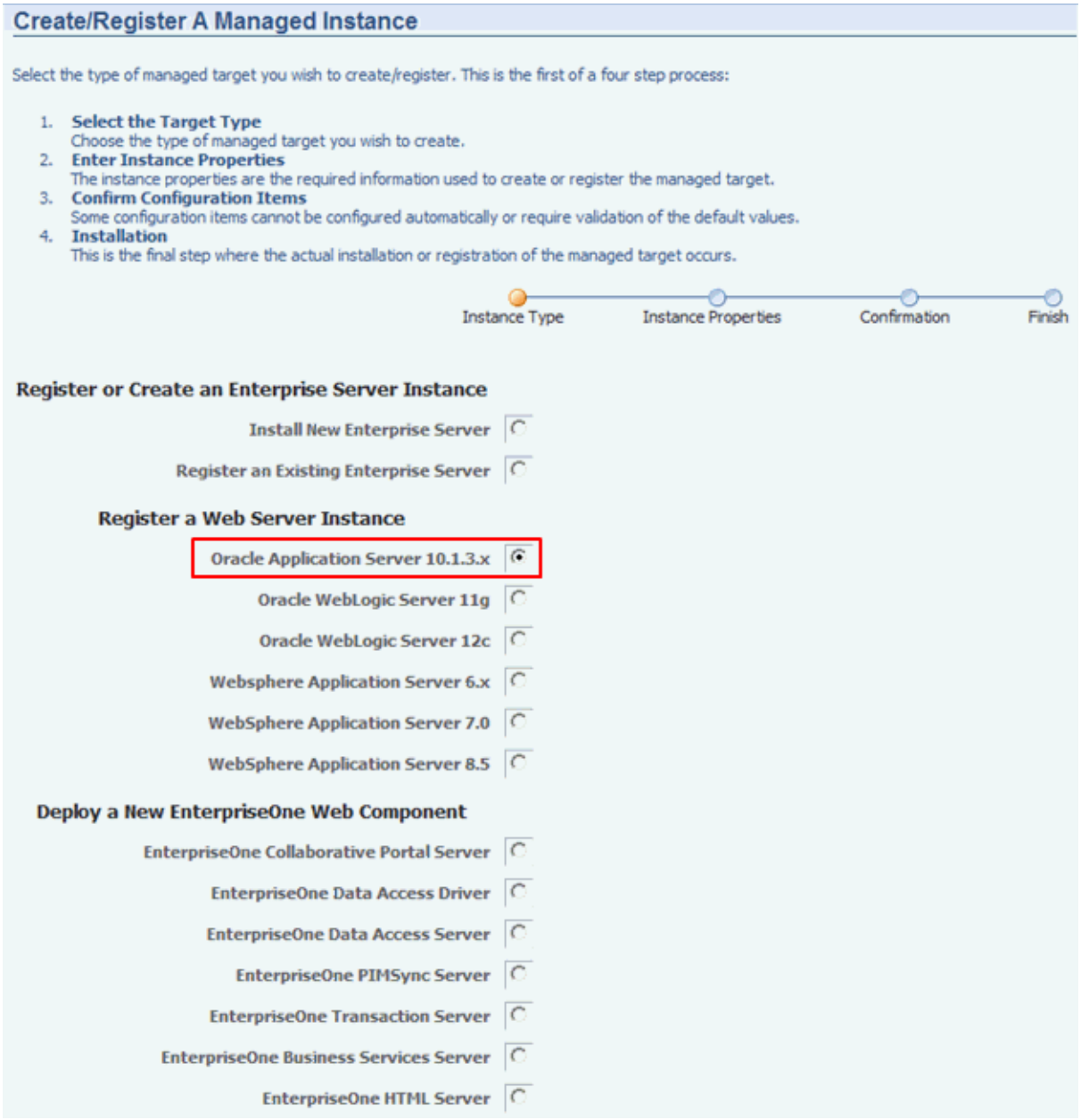
Note: Registration of an Oracle Application Server requires that a Management Agent first be installed on the Oracle Application Server. This server must be installed with the correct user and also started with the correct user. Refer to Chapter 5, "Install a Management Agent".

To register an existing Oracle Application Server:

1. Select the Managed Home which resides on the machine on which your Oracle Application Server resides.



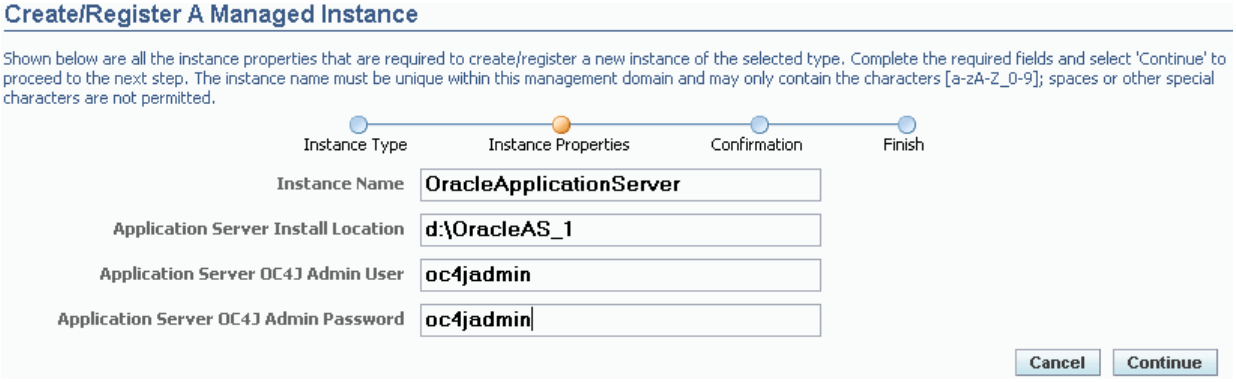
2. Click the **Create a New Managed Instance** button to create the Managed Instance within the Managed Home.



3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   Oracle Application Server 10.1.3.x

4. Click Continue.



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Instance Name*

     Enter a unique name for the instance name.

   - *Application Server Install Location*

     Enter the installation location for the existing Oracle Application Server.

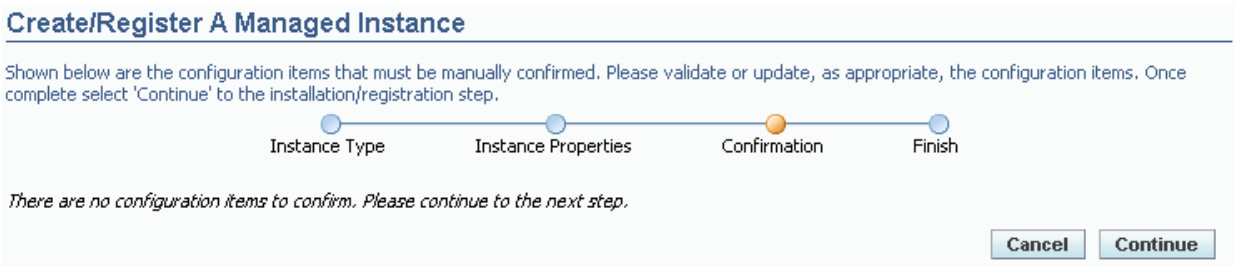
   - *Application Server OC4J Admin User*

     Enter the administrative user for the Oracle Application Server on which this OC4J will be created.

   - *Application Server OC4J Admin Password*

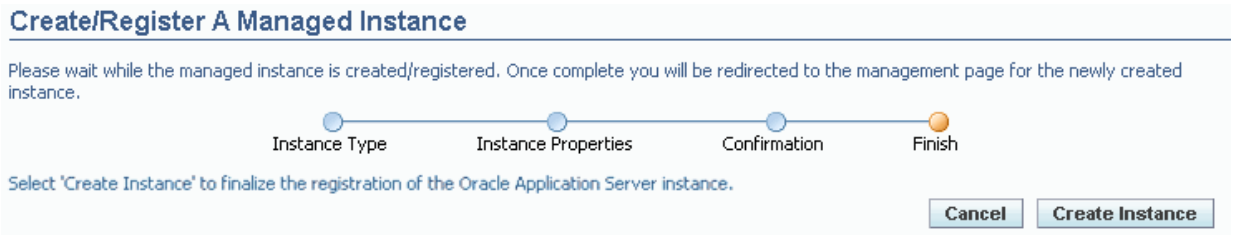
     Enter the password for the administrative user for the Oracle Application Server on which this OC4J will be created.

6. Click Continue.

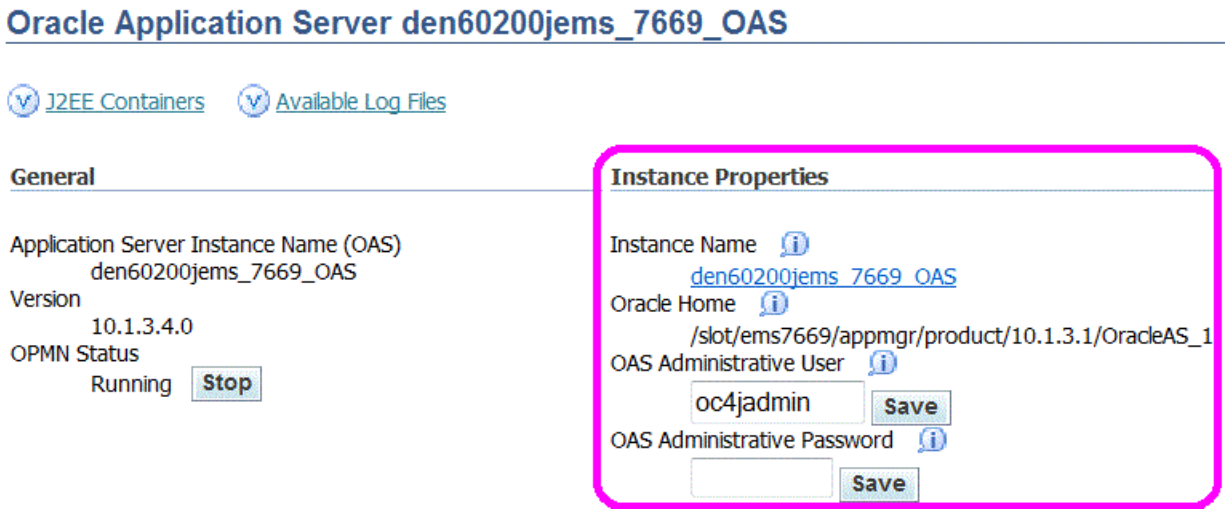


7. On Create/Register a Managed Instance, Confirmation, there are no configuration items to confirm.

8. Click Continue.



9. On Create/Register a Managed Instance, Finish, click the **Create Instance** button to complete the registration of the Oracle Application Server.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Oracle Application Server. This server also appears as a Managed Instance within the corresponding Managed Home.

For each registered Oracle Application Server Managed Instance, the Management Console displays appropriate information at the top of the web page:

- *General*
  - Application Server Instance Name (OAS)

    Displays the name of this Oracle Application Server.
  - Version

    Displays the version of this Oracle Application Server Managed Instance.
  - OPMN Status

    Displays either Stopped with the Start button, or Started with the Stop button.
- *Instance Properties*
  - Instance Name

    Displays a clickable link for the unique name assigned to the Oracle Application Server Managed Instance at the time is was created or registered.
  - Oracle Home

    Displays the complete path to the Oracle home where this Oracle Application Server instance was installed.
  - Oracle Administrative User

    Displays the administrative user credential that is used by Server Manager to perform administrative tasks on the oracle application server instance. This is typically the oc4jadmin administrative account.
  - Oracle Administrative Password

    The administrative password credential that is used by Server Manager to perform administrative tasks on the oracle application server instance. This is typically the oc4jadmin administrative account.

13.2 Register a WebSphere Application Server, Version 7.0

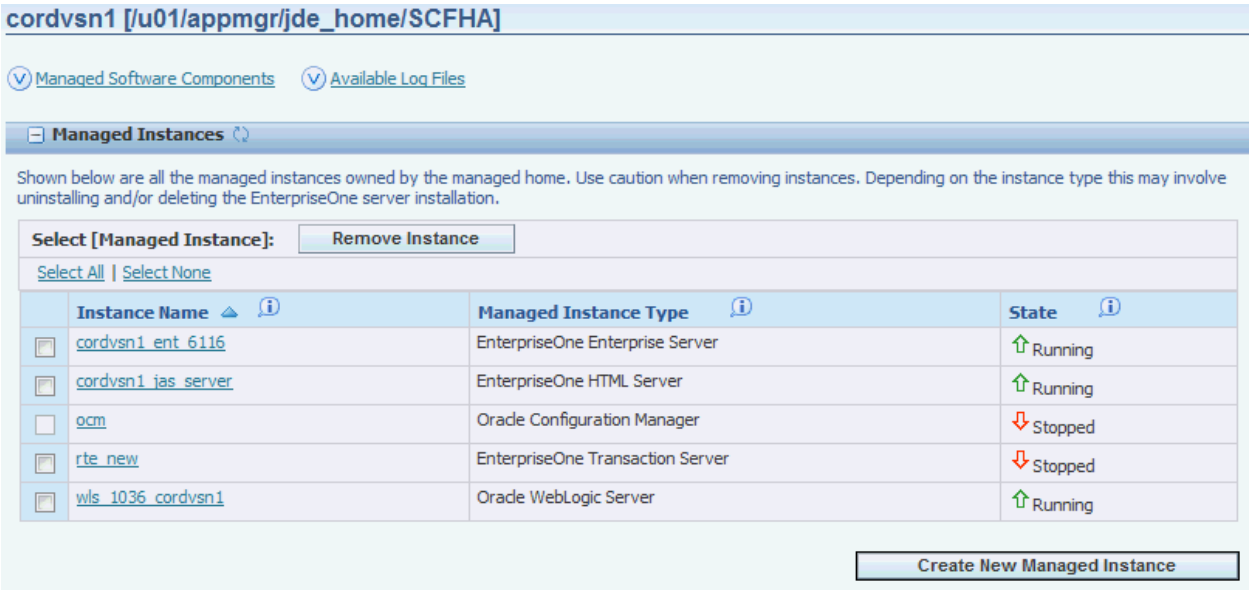
Only WebSphere Application Servers, version 7.0 that are registered with the Management Console can be managed by the Management Console. The WebSphere Application Server must be installed outside of Server Manager. You should always verify that your WAS versions are fix-current per IBM directives. You should also verify that your version of WAS is compatible with JD Edwards EnterpriseOne servers (for details refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide).

Note: Registration of a WebSphere Application Server requires that a Management Agent first be installed on the WebSphere Application Server. This server must be installed with the correct user and also started with the correct user. Refer to Chapter 5, "Install a Management Agent".

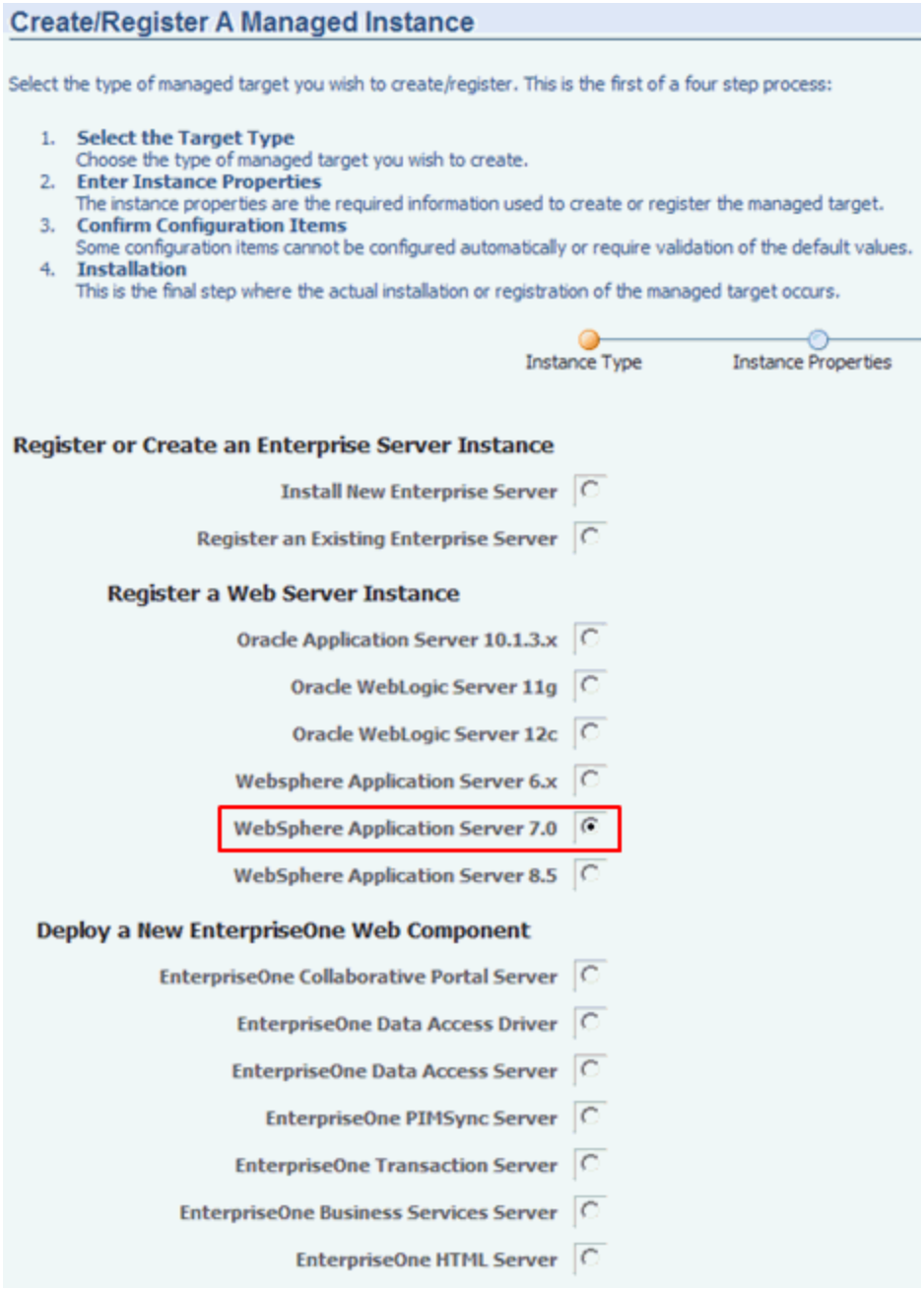
If you have enabled administrative security in a WebSphere Application Server profile, refer to Section 13.2.1, "Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled" in this chapter.

To register an existing WebSphere Application Server:

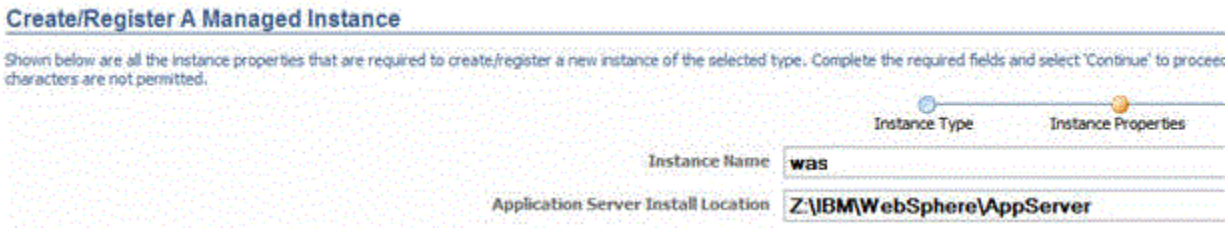
1. Select the Managed Home with which you wish to register the WebSphere Application Server.



2. Click the **Create a New Managed Instance** button to create the Managed Instance within the Managed Home.



3. On Create/Register a Managed Instance, Instance Type, select the **WebSphere Application Server 7.0** radio button.



4. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Instance Name*

Enter a unique name for the instance name.

- *Install Location*

  Enter the installation location for the existing WebSphere Application Server. This location should include the path up to the parent folder of the `profiles` folder.

  For example:

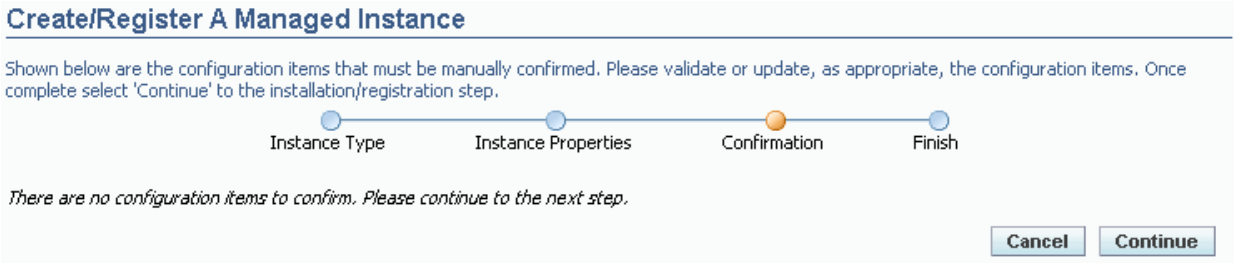
  OS400 (IBMi / IBM i)

  `/QIBM/ProdData/WebSphere/AppServer/V7/ND`

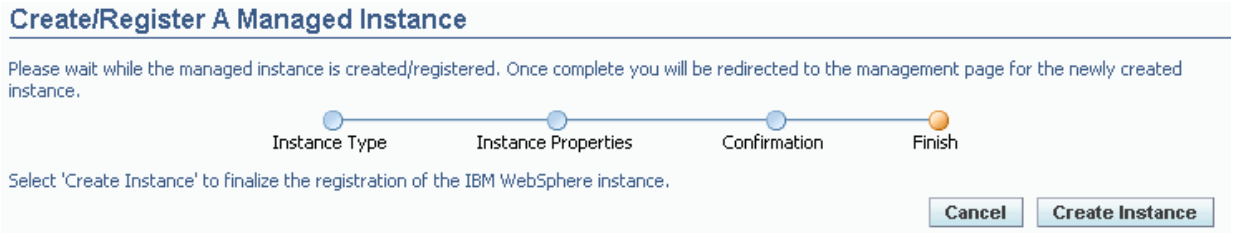
  Unix

  `/u01/WebSphere7/AppServer`

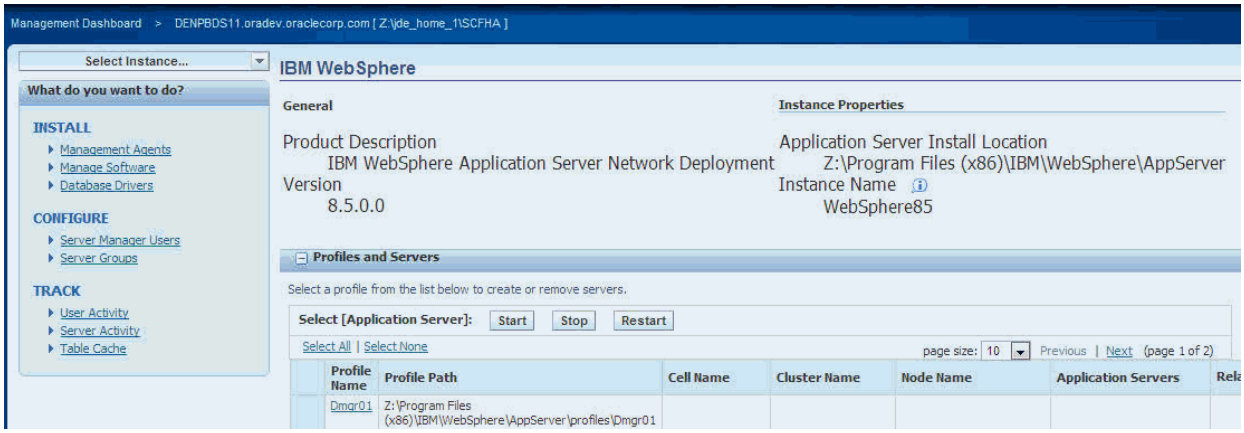
5. Click Continue.



6. On Create/Register a Managed Instance, Confirmation, there are no configuration items to confirm.
7. Click Continue.



8. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the registration of the WebSphere Application Server.



After you have completed the installation the browser is redirected to the Management Console page for the newly registered WebSphere Application Server. This server also appears as a Managed Instance within the corresponding Managed Home.

For each registered WebSphere Application Server Managed Instance, the Management Console displays appropriate information at the top of the web page:

- *Product Description*

  Displays the description for this WebSphere Application Server Managed Instance.

- *General*

  - Version

    Displays the version of this WebSphere Application Server Managed Instance.

- *Instance Properties*

  - Application Server Install Location

    Displays the full path for the install location of the selected WebSphere Application Server Managed Instance.

  - Instance Name

    Displays a clickable link for the unique name assigned to the WebSphere Application Server Managed Instance at the time is was created or registered.

13.2.1 Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled

To configure WebSphere Application Server to work with Server Manager when Administrative Security is enabled:

1. Locate the `soap.client.props` file associated with the security profile.

   Typically the file is found at this location:

   ```
   WAS_Install_Location\profiles\Profile_Name\properties\soap.client.props
   ```

2. Modify these settings in the `soap.client.props` file:

   ```
   com.ibm.SOAP.securityEnabled=true

   com.ibm.SOAP.loginUserid=admin_user

   com.ibm.SOAP.loginPassword=admin_password
   ```

   where *admin_user* and *admin_password* are values appropriate to your environment.

3. In order for the security changes to take effect, you must restart the Management Agent to which the WebSphere Application Server is registered. For instructions, refer to Section 6.3, "Restart a Management Agent".

13.3 Register a WebSphere Application Server, Version 8.5 (Tools Release 9.1 Update 2.3)

Note: Tools Release 9.1 Update 2.3. Beginning with this release, WebSphere Application Server Version 8.5 is supported with JD Edwards EnterpriseOne.

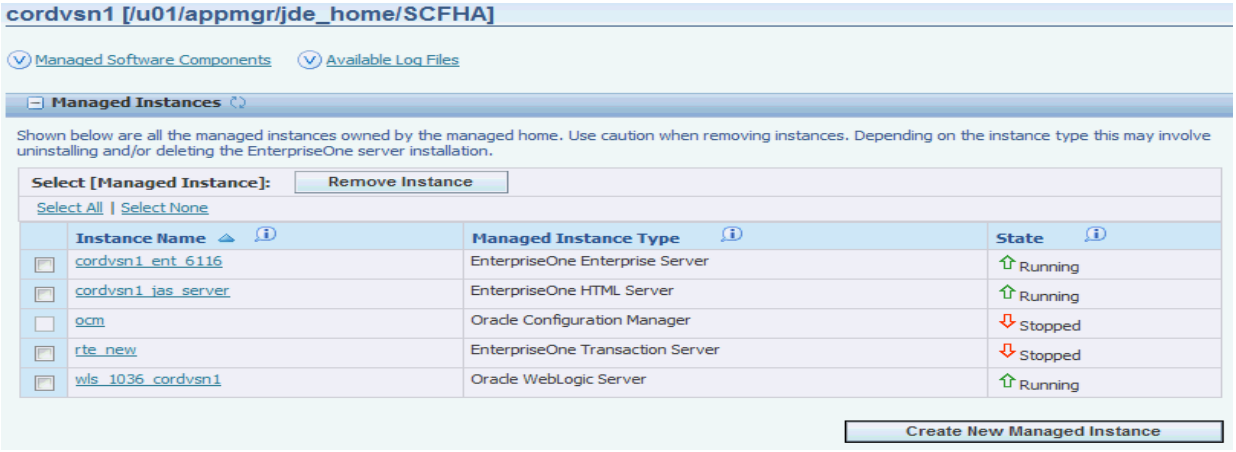
Only WebSphere Application Servers, version 8.5 that are registered with the Management Console can be managed by the Management Console. The WebSphere Application Server must be installed outside of Server Manager. You should always verify that your WAS versions are fix-current per IBM directives. You should also verify that your version of WAS is compatible with JD Edwards EnterpriseOne servers (for details refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide).

Note: Registration of a WebSphere Application Server requires that a Management Agent first be installed on the WebSphere Application Server. This server must be installed with the correct user and also started with the correct user. Refer to Chapter 5, "Install a Management Agent".

If you have enabled administrative security in a WebSphere Application Server profile, refer to Section 13.3.1, "Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled" in this section.

To register an existing WebSphere Application Server:

1. Select the Managed Home with which you wish to register the WebSphere Application Server.



2. Click the **Create a New Managed Instance** button to create the Managed Instance within the Managed Home.

3. On Create/Register a Managed Instance, Instance Type, select the **WebSphere Application Server 8.5** radio button.

4. On Create/Register a Managed Instance, Instance Properties, complete these fields:

- *Instance Name*

Enter a unique name for the instance name.

- *Install Location*

  Enter the installation location for the existing WebSphere Application Server. This location should include the path up to the parent folder of the `profiles` folder.

  For example:

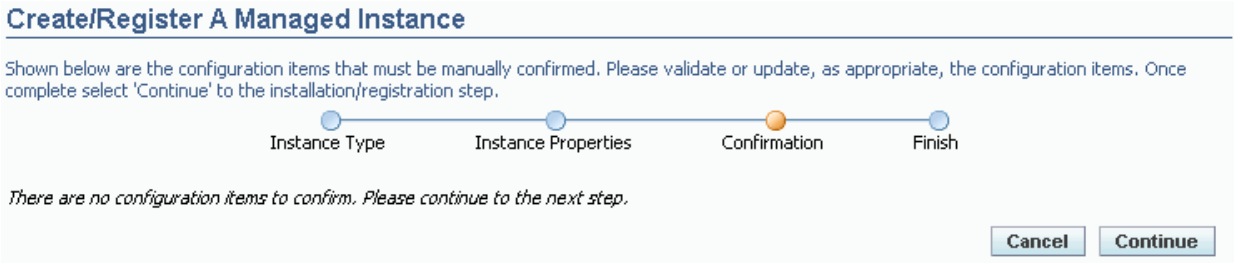
  OS400 (IBM i)

  `/QIBM/ProdData/WebSphere/AppServer/V85/ND`

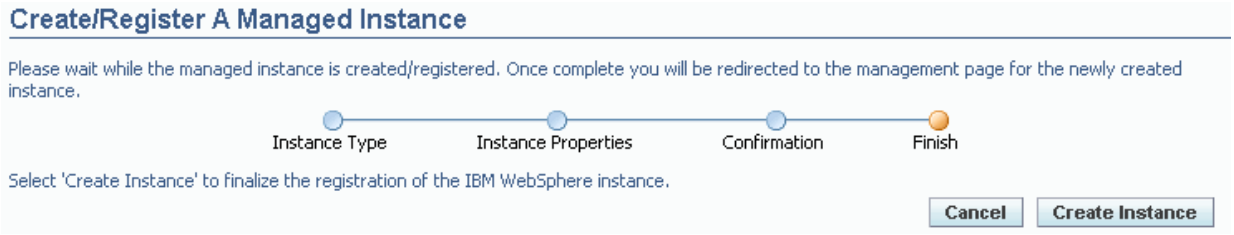
  Unix

  `/u01/WebSphere85/AppServer`

5. Click Continue.



6. On Create/Register a Managed Instance, Confirmation, there are no configuration items to confirm.
7. Click Continue.



8. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the registration of the WebSphere Application Server.

After you have completed the installation the browser is redirected to the Management Console page for the newly registered WebSphere Application Server. This server also appears as a Managed Instance within the corresponding Managed Home.

For each registered WebSphere Application Server Managed Instance, the Management Console displays appropriate information at the top of the web page:

- *Product Description*

  Displays the description for this WebSphere Application Server Managed Instance.

- *General*

  – Version

    Displays the version of this WebSphere Application Server Managed Instance.

- *Instance Properties*
  - Application Server Install Location

    Displays the full path for the install location of the selected WebSphere Application Server Managed Instance.
  - Instance Name

    Displays a clickable link for the unique name assigned to the WebSphere Application Server Managed Instance at the time is was created or registered.

13.3.1 Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled

To configure WebSphere Application Server to work with Server Manager when Administrative Security is enabled:

1. Locate the `soap.client.props` file associated with the security profile.

   Typically the file is found at this location:

   `WAS_Install_Location\profiles\Profile_Name\properties\soap.client.props`
2. Modify these settings in the `soap.client.props` file:

   `com.ibm.SOAP.securityEnabled=true`

   `com.ibm.SOAP.loginUserid=admin_user`

   `com.ibm.SOAP.loginPassword=admin_password`

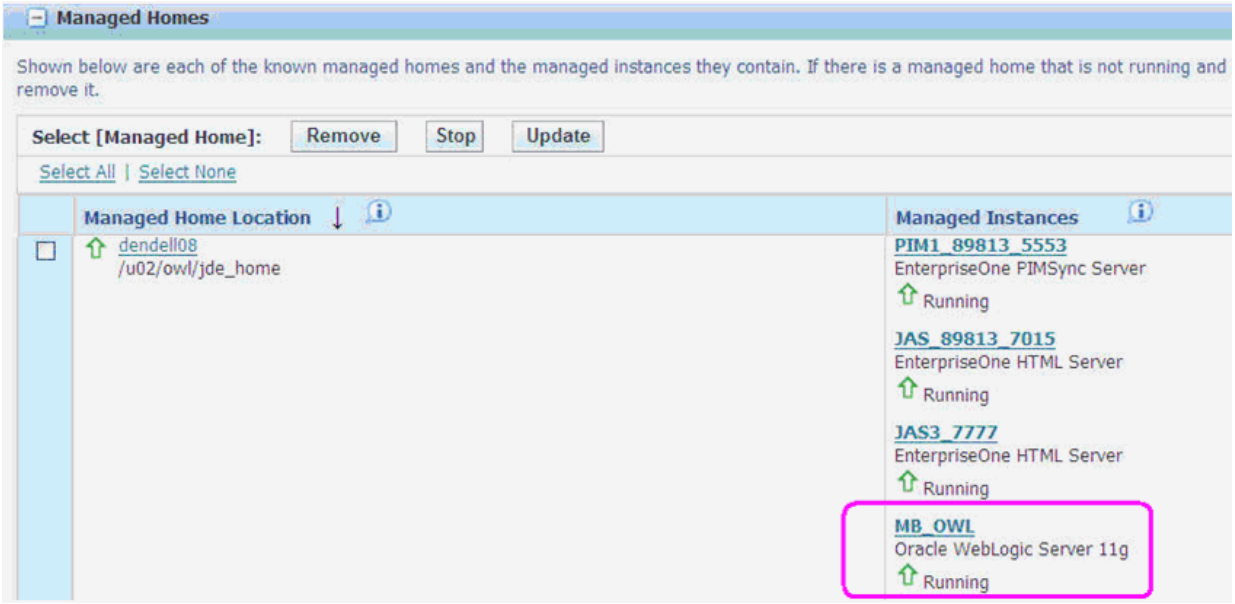
   where *admin_user* and *admin_password* are values appropriate to your environment.
3. In order for the security changes to take effect, you must restart the Management Agent to which the WebSphere Application Server is registered. For instructions, refer to Section 6.3, "Restart a Management Agent".

13.4 Register an Oracle WebLogic Server 11g

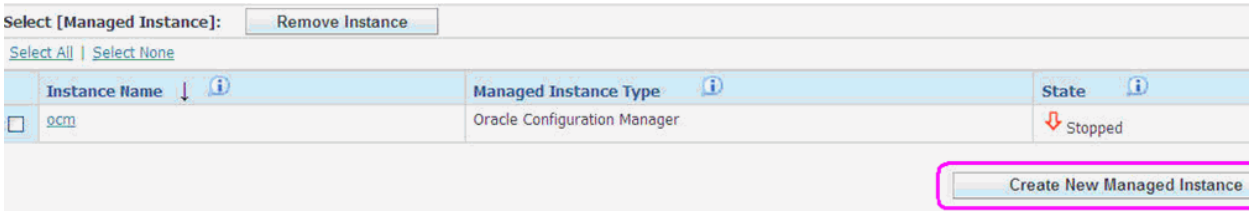
Only Oracle WebLogic Servers that are registered with the Management Console can be managed by the Management Console. The Oracle WebLogic Server must be installed outside of Server Manager. You should always verify that your Oracle WebLogic Server versions are fix-current per Oracle directives. You should also verify that your version of Oracle WebLogic Server is compatible with JD Edwards EnterpriseOne servers (for details refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide).

Note: Registration of an Oracle WebLogic Server requires that a Management Agent first be installed on the Oracle WebLogic Server. This server must be installed with the correct user and also started with the correct user. Refer to Chapter 5, "Install a Management Agent".

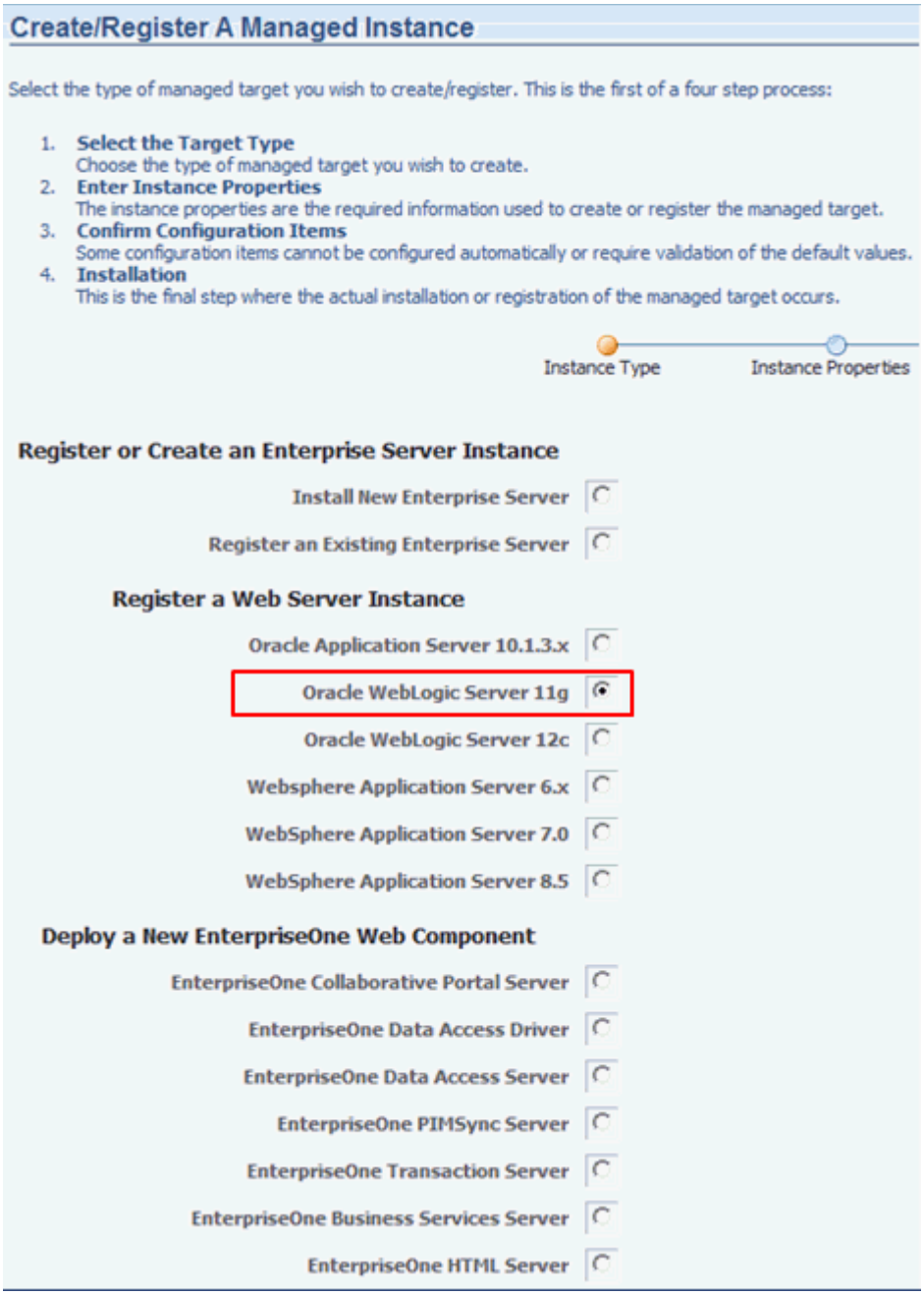
To register an existing Oracle WebLogic Server:



1. Select the Managed Home with which you wish to register an Oracle WebLogic Server.



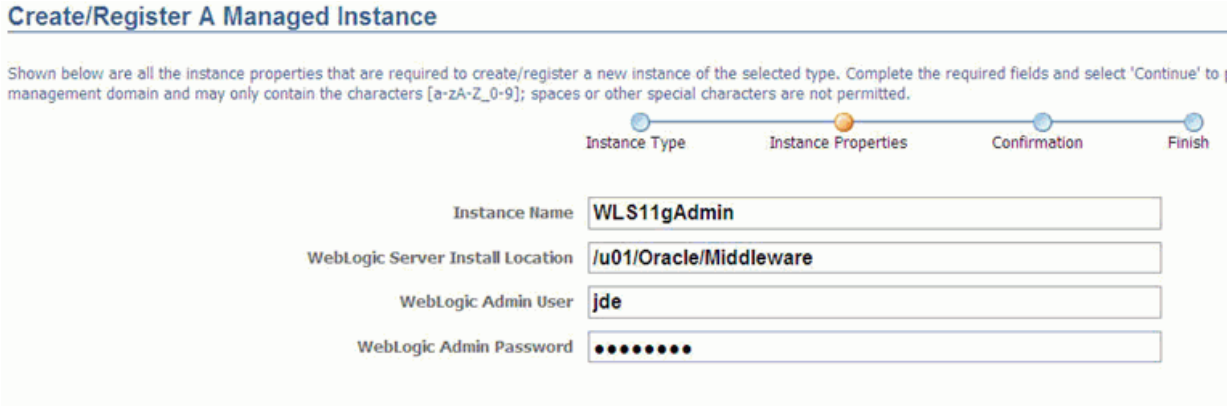
2. On Managed Instances, click the **Create New Managed Instance** button.



3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   Oracle WebLogic Server 11g

4. Click the **Continue** button.



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Instance Name*

     Enter a unique name for the instance name.

   - *Oracle WebLogic Server Install Location*

     Enter the installation location for the existing Oracle WebLogic Server. This is the Oracle WebLogic Home, where the default value is:

     `/u01/Oracle/Middleware`

   - *Oracle WebLogic Admin User*

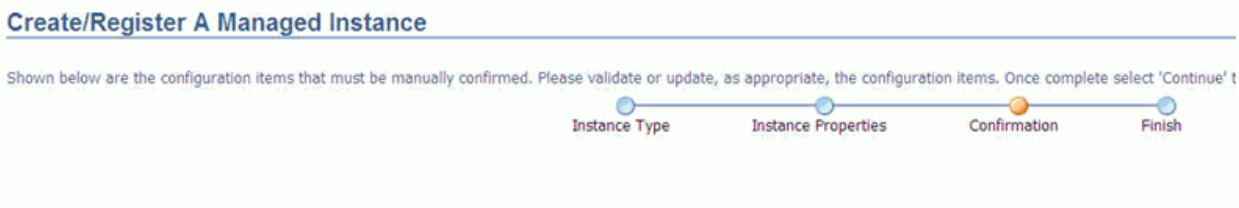
     Enter the administrative user for the Oracle WebLogic Administrative Console on which this Managed Instance will be created. The default admin user is:

     `Oracle WebLogic`

   - *Oracle WebLogic Admin Password*

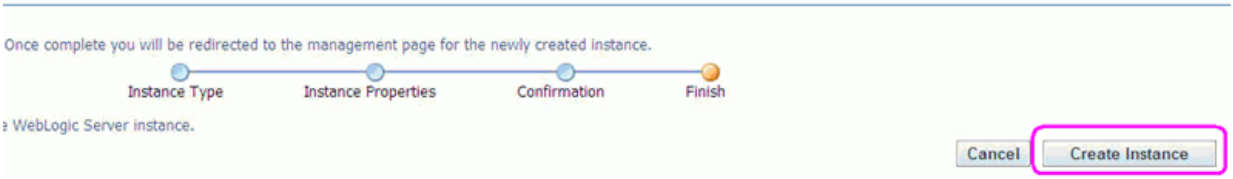
     Enter the administrative user for the Oracle WebLogic Administrative Console on which this Managed Instance will be created. For the default password refer to the `/u01/Oracle/Middleware/utils/quickstart/quickstart.sh` program. Access the **Start Administration Console** option.

6. Click the **Continue** button.

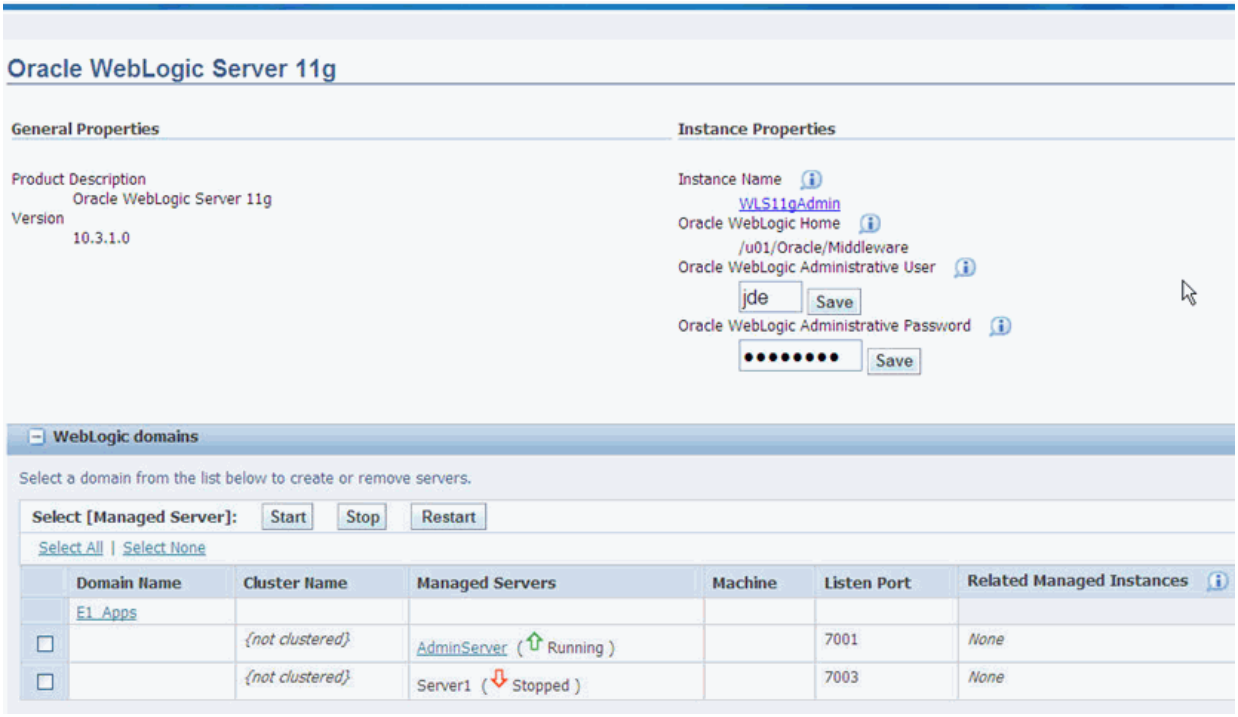


7. On Create/Register a Managed Instance, Confirmation, there are no configuration items to confirm.

8. Click the **Continue** button.



9. On Create/Register a Managed Instance, Finish, click the **Create Instance** button to complete the registration of the Oracle WebLogic Server.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Oracle WebLogic Server. This server also appears as a Managed Instance within the corresponding Managed Home.

For each registered Oracle WebLogic Server Managed Instance, the Management Console displays appropriate information at the top of the web page:

- *General Properties*
  - *Product Description*

    Oracle WebLogic Server 11g
  - *Version*

    10.3.1.0
- *Instance Properties*
  - *Instance Name*

    Displays a clickable link for the unique name assigned to the Oracle WebLogic Server Managed Instance at the time is was created or registered.
  - *Oracle WebLogic Home*

    Displays the complete path to the Oracle WebLogic Server Home where this Oracle WebLogic Server instance was installed.
  - *Oracle WebLogic Administrative User*

    Displays the administrative user credential that is used by Server Manager to perform administrative tasks on the Oracle WebLogic Server instance.
  - *Oracle WebLogic Administrative Password*

Displays the administrative password credential that is used by Server Manager to perform administrative tasks on the Oracle WebLogic Server instance.

13.5 Register an Oracle WebLogic Server 12c

Only Oracle WebLogic Servers that are registered with the Management Console can be managed by the Management Console. The Oracle WebLogic Server must be installed outside of Server Manager. You should always verify that your Oracle WebLogic Server versions are fix-current per Oracle directives. You should also verify that your version of Oracle WebLogic Server is compatible with JD Edwards EnterpriseOne servers (for details refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide).

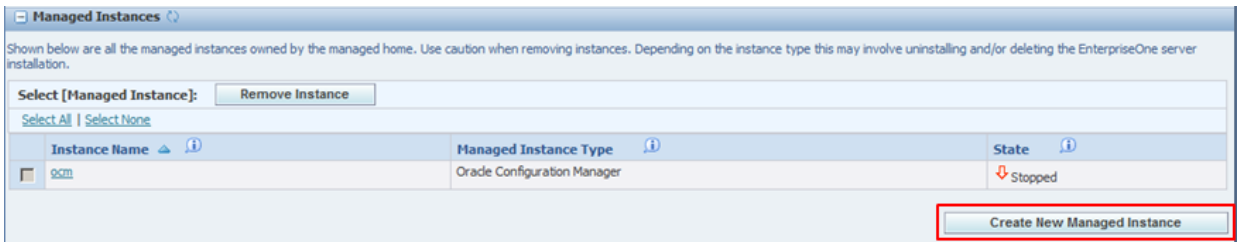
Note: Registration of an Oracle WebLogic Server requires that a Management Agent first be installed on the Oracle WebLogic Server. This server must be installed with the correct user and also started with the correct user. Refer to Section 5, "Install a Management Agent".

To register an existing Oracle WebLogic Server:

Figure 13–1 Managed Homes

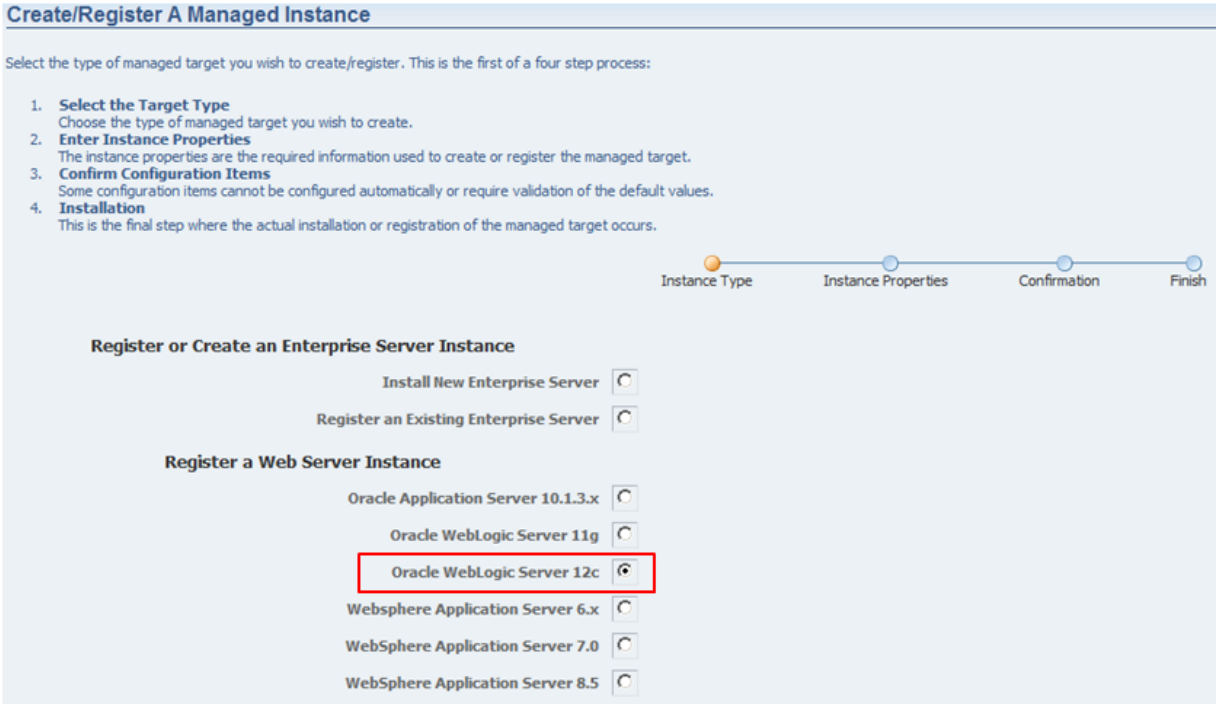
1. Select the Managed Home where you want to register an Oracle WebLogic Server.

Figure 13–2 Managed Instances



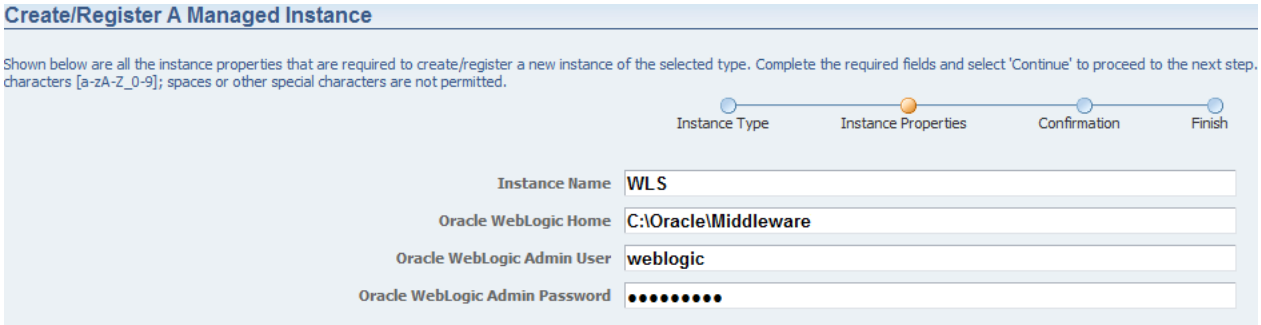
2. On Managed Instances, click the *Create New Managed Instance* button.

Figure 13–3 Oracle WebLogic Server 12c Selection



3. On Create/Register a Managed Instance, Instance Type, select the *Oracle WebLogic Server 12c* radio button.
4. Click the Continue button.

Figure 13–4 Instance Properties



5. On the Create/Register a Managed Instance screen for Instance Properties, complete these fields:

   - Instance Name

     Enter a unique name for the instance name.

   - Oracle WebLogic Server Install Location

     Enter the installation location for the existing Oracle WebLogic Server. This is the Oracle WebLogic Home, where the default value is:

     C:\Oracle\Middleware

   - Oracle WebLogic Admin User

Enter the administrative user for the Oracle WebLogic Administrative Console on which this Managed Instance will be created. The default admin user is:

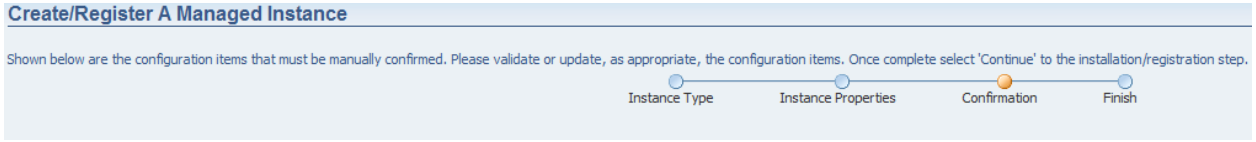
Oracle WebLogic

? Oracle WebLogic Admin Password

Enter the administrative user for the Oracle WebLogic Administrative Console on which this Managed Instance will be created.

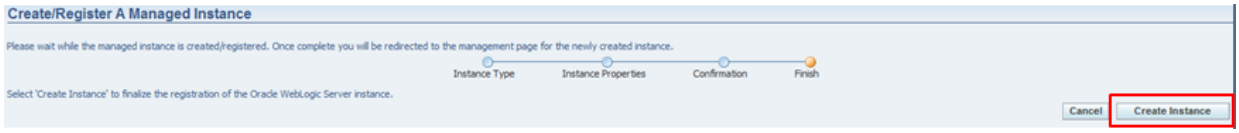
6. Click the Continue button.

Figure 13–5 Confirmation



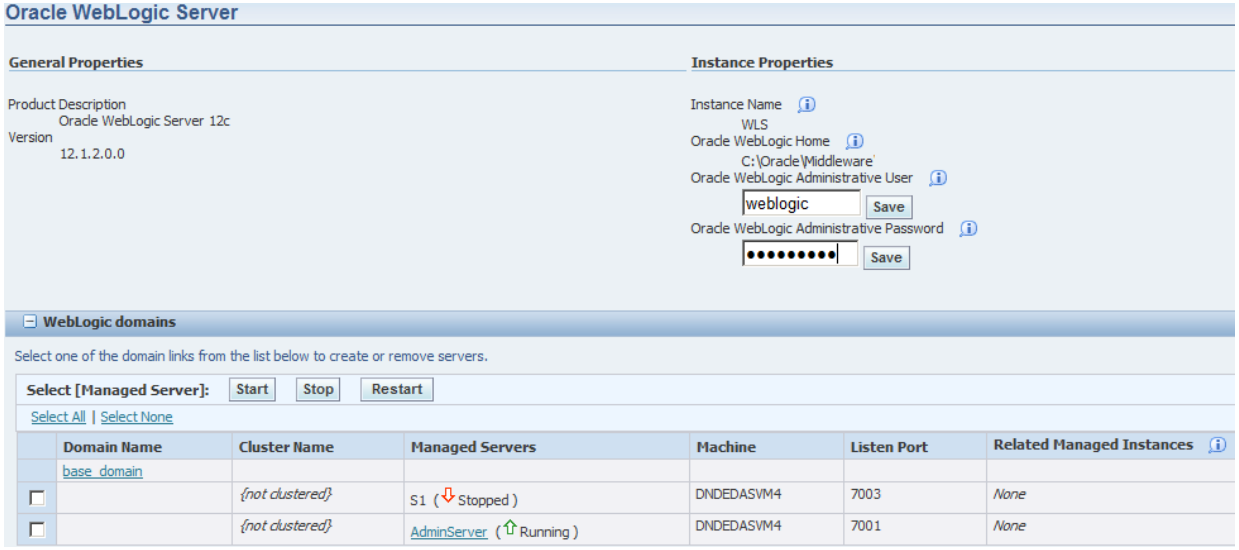
7. On the Create/Register a Managed Instance screen for Confirmation, there are no configuration items to confirm.
8. Click the Continue button.

Figure 13–6 Finish



9. On the Create/Register a Managed Instance screen for Finish, click the *Create Instance* button to complete the registration of the Oracle WebLogic Server.

Figure 13–7 WLS Domains



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Oracle WebLogic Server. This server also appears as a Managed Instance within the corresponding Managed Home.

For each registered Oracle WebLogic Server Managed Instance, the Management Console displays appropriate information at the top of the web page:

General Properties

- Product Description

  Oracle WebLogic Server 12c

- Version

  12.1.2.0.0

Instance Properties

- Instance Name

  Displays a clickable link for the unique name assigned to the Oracle WebLogic Server Managed Instance at the time is was created or registered.

- Oracle WebLogic Home

  Displays the complete path to the Oracle WebLogic Server Home where this Oracle WebLogic Server instance was installed.

- Oracle WebLogic Administrative User

  Displays the administrative user credential that is used by Server Manager to perform administrative tasks on the Oracle WebLogic Server instance.

- Oracle WebLogic Administrative Password

  Displays the administrative password credential that is used by Server Manager to perform administrative tasks on the Oracle WebLogic Server instance.

14

Create a J2EE Server Container

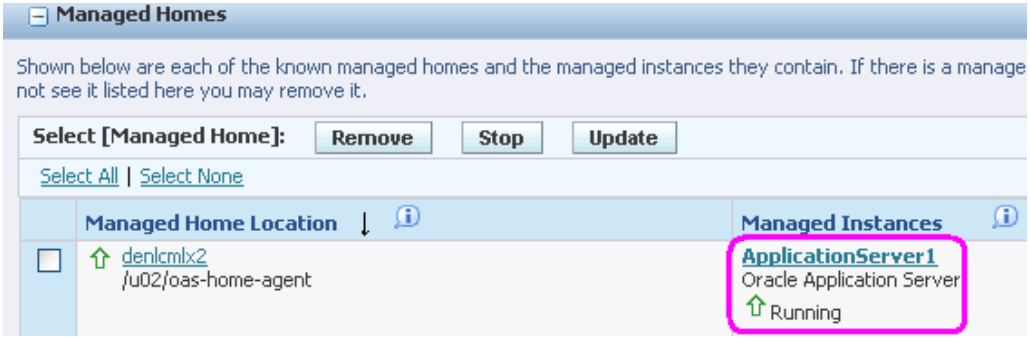
This chapter discusses:

- Section 14.1, "Create a J2EE Server Container for the Oracle Application Server (OAS)"
- Section 14.2, "Create a J2EE Server Container for the WebSphere Application Server (WAS)"
- Section 14.3, "Create a J2EE Server for an Oracle WebLogic Server Domain"
- Section 14.4, "Install or Uninstall JDBC Drivers to the J2EE Server (WLS or WAS)"

14.1 Create a J2EE Server Container for the Oracle Application Server (OAS)

> **Note:** There is a one-to-one relationship between a web-based server and a J2EE Server Container. You cannot install more than one web-based server in each J2EE Server Container.

To create a J2EE Server Container:



1. Select the existing Managed Instance for a running Oracle Application Server Managed Instance with which you wish to create a new J2EE Server Container.

2. In the *J2EE Containers* section of the page, use the form below to create a new OC4J instance within the OAS installation by completing these fields:

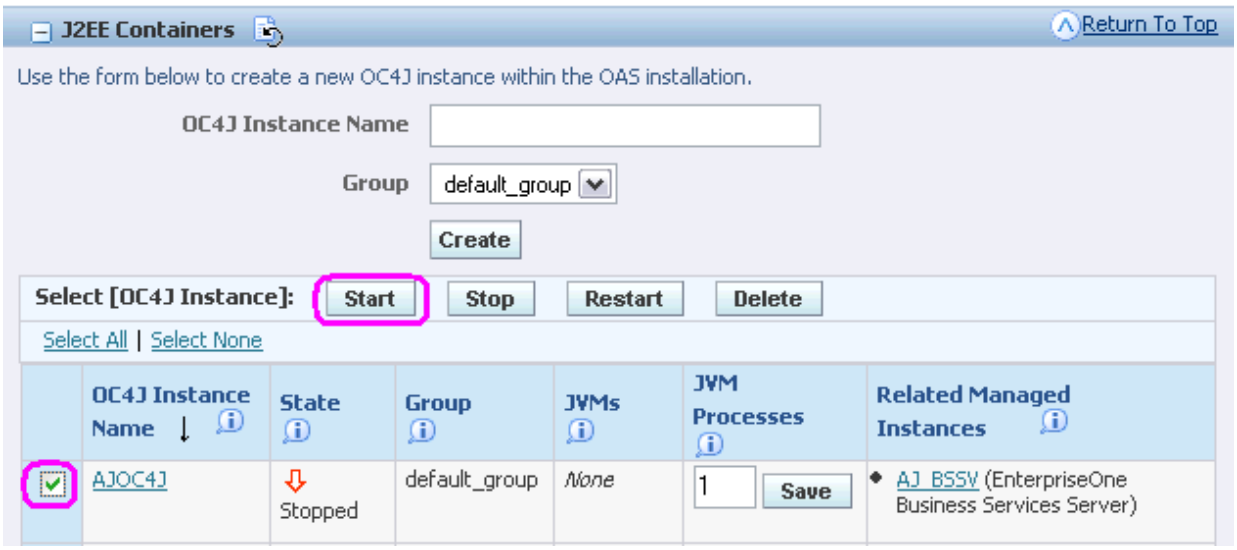
   - *OC4J Instance Name*

     Enter a unique name for this OC4J instance.

   - *Group*

     Select the Oracle Application Server defined group in which to create the new OC4J instance.

3. Click the *Create* button.



4. On J2EE Server Containers, select the J2EE Server Container that you just created and click the *Start* button.

Note: While technically you are not required to start the J2EE Server Container, it is good practice to ensure that it is properly created and able to start. Otherwise, it might not start as expected during the installation process for a JD Edwards EnterpriseOne web-based server.

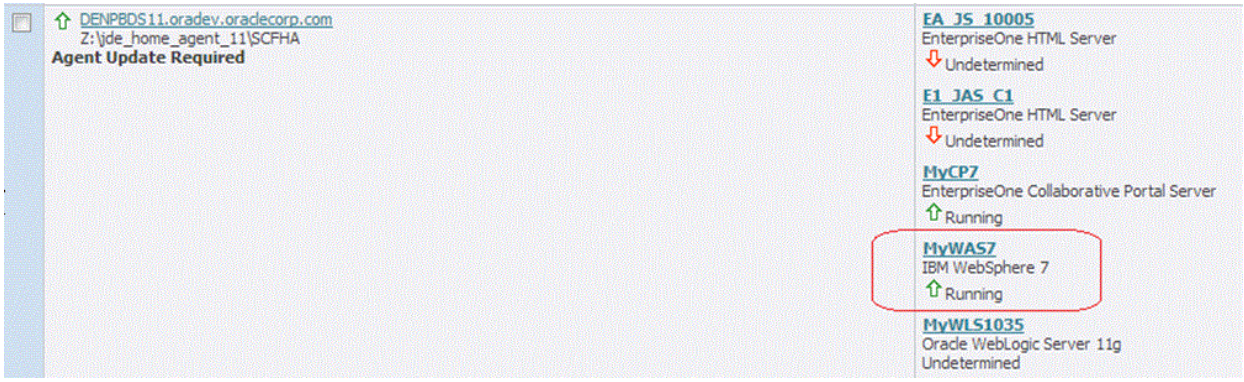
Tip: The Server Manager displays a progress monitor indicating that the Start operation is in progress and will continue even if you close the browser. After the progress monitor is no longer displayed, you can refresh the Management Console page to verify that the newly-created J2EE Server Container starts as expected.

Note: If you do not install the JDBC drivers before installing the Web-Based Server Instance, the Web-Based Server Instance will not be able to start as expected at the end of the installation. Refer to Section 14.4, "Install or Uninstall JDBC Drivers to the J2EE Server (WLS or WAS)"

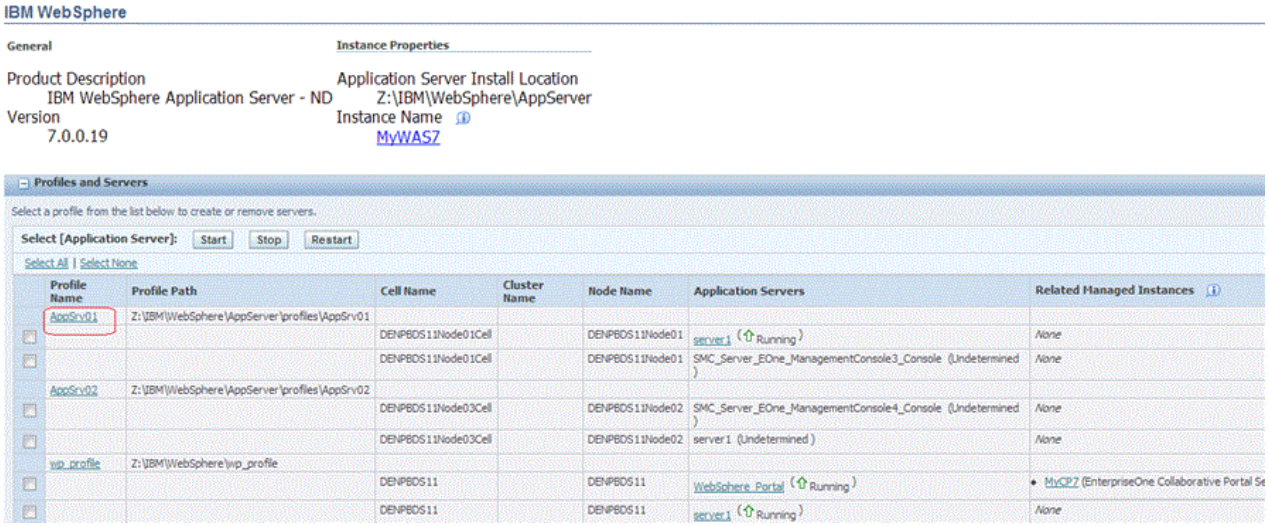
14.2 Create a J2EE Server Container for the WebSphere Application Server (WAS)

Note: There is a one-to-one relationship between a web-based server and a J2EE Server Container. You cannot install more than one web-based server in each J2EE Server.

To create a J2EE Server Container:

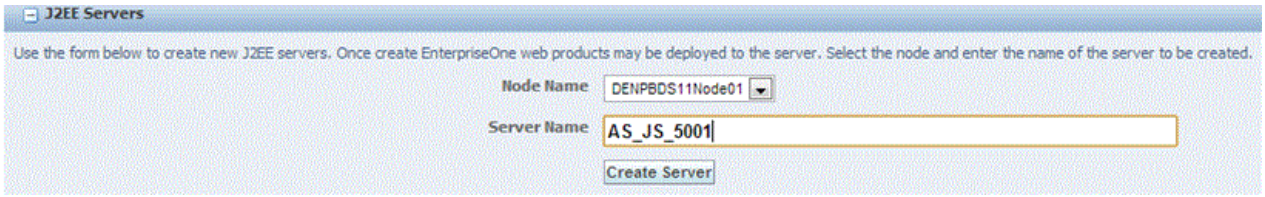


1. Select the existing Managed Instance for a running WebSphere Application Server with which you wish to create a new J2EE Server Container.



2. In the *Profiles and Servers* section of the page, click the on an existing Profile Name.

   Tip: If you plan to use this J2EE Server Container to run a JD Edwards EnterpriseOne Business Services Server, you should select a secure profile. This profile must be created and configured within the WebSphere Application Server itself.



3. On the *J2EE Servers* section of the page, use the form to create a new J2EE Server Container, complete these fields:

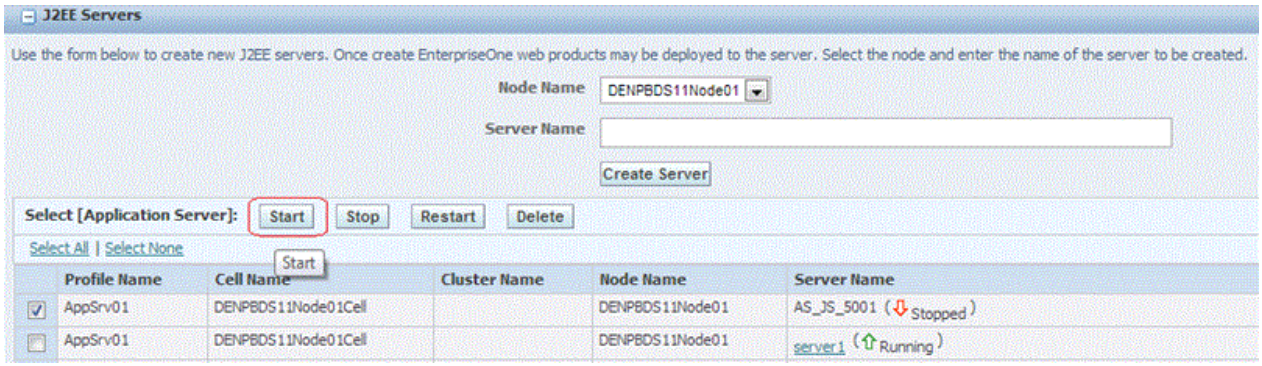
   - *Node Name*

     Use the dropdown to select an existing node name.

   - *Server Name*

     Enter a unique name for this J2EE Server Container.

4. Click the *Create Server* button.



5. On the *J2EE Servers* section of the page, select the J2EE Server Container that you just created and click the *Start* button.

   Note: While you are not required to start the J2EE Server, it is good practice to ensure that it is properly created and able to start. Otherwise, it might not start as expected during the installation process for a JD Edwards EnterpriseOne web-based server.

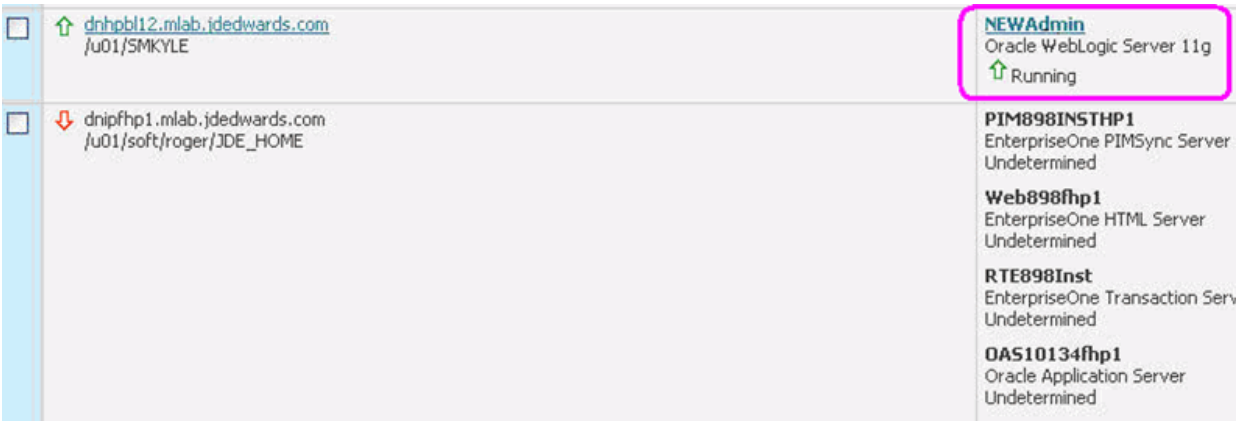
   Tip: The Server Manager displays a progress monitor indicating that the Start operation is in progress and will continue even if you close the browser. After the progress monitor is no longer displayed, you can refresh the Management Console page to verify that the newly-created J2EE Server starts as expected.

Note: If you do not install the JDBC drivers before installing the Web-Based Server Instance, the Web-Based Server Instance will not be able to start as expected at the end of the installation. Refer to Section 14.4, "Install or Uninstall JDBC Drivers to the J2EE Server (WLS or WAS)".

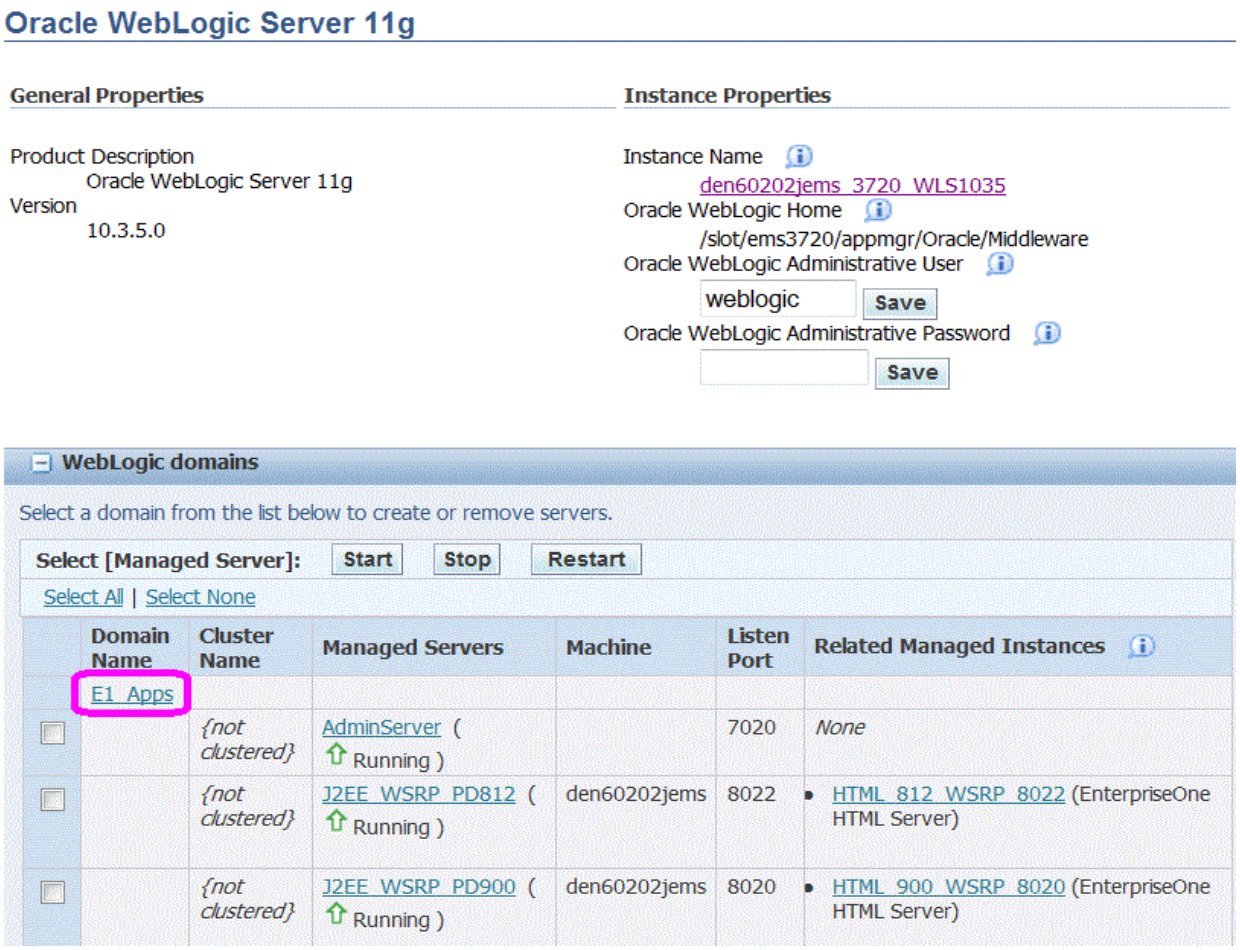
14.3 Create a J2EE Server for an Oracle WebLogic Server Domain

Note: There is a one-to-one relationship between a web-based server and a J2EE Server. You cannot install more than one web-based server in each J2EE Server.

To create a J2EE Server for an Oracle WebLogic Server domain:

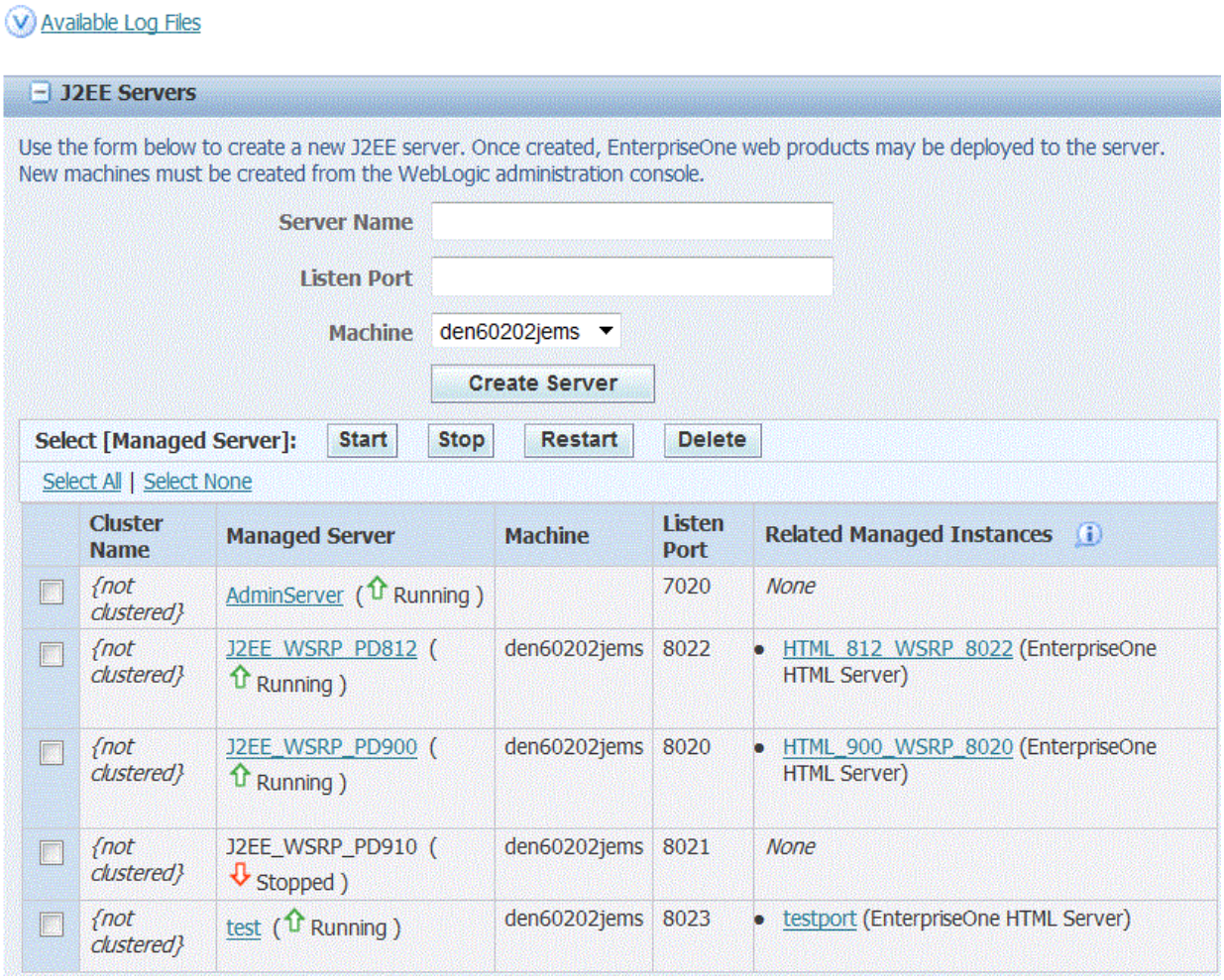


1. Select the existing Managed Instance for a running Oracle WebLogic Server Managed Instance with which you wish to create a new Server.



2. In the Oracle WebLogic domains section, click on the link for the domain into which you want to create a new Oracle WebLogic Server.

   For example, in the above screen shot, the Oracle WebLogic Server Domain is *E1_Apps*.



3. In the *J2EE Server* section of the page, use the form to create a new J2EE Server instance within the Oracle WebLogic Server domain by completing these fields:

   - *Server Name*

     Enter a unique name for this Oracle WebLogic Server instance.

   - *Listen Port*

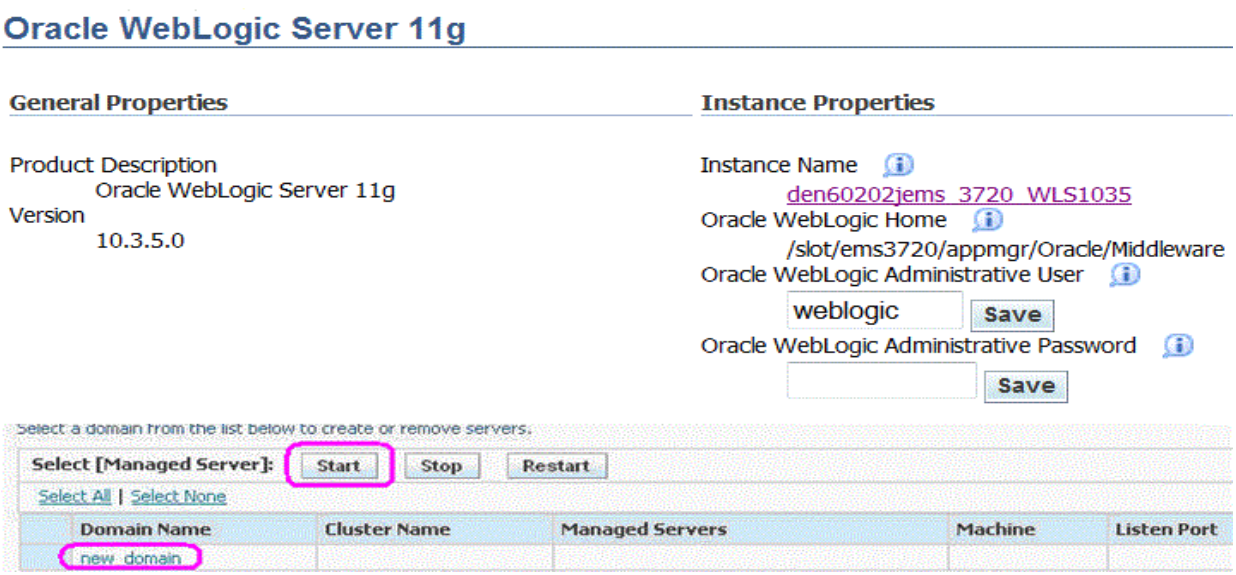
     Enter a unique port number. This Oracle WebLogic Server must listen on a port that is different from all of the others servers in the domain.

   - *Machine*

     Use the pull-down to select an existing machine to which this Server is associated. The machine must have already been created in the Oracle WebLogic Server Admin Console.

     Note: All Servers created within Server Manager must be associated with a machine so that they can be started and stopped through Server Manager.

4. After the above three (3) fields are complete, click the *Create Server* button.



5. On the *J2EE Servers* section of the page, select the J2EE Server that you just created and click the *Start* button.

Note: While technically you are not required to start the Oracle WebLogic domain, it is good practice to ensure that it is properly created and able to start. Otherwise, it might not start as expected during the installation process for a JD Edwards EnterpriseOne web-based server.

Tip: Server Manager displays a progress monitor indicating that the Start operation is in progress and will continue even if you close the browser. After the progress monitor is no longer displayed, you can refresh the Management Console page to verify that the newly-created Oracle WebLogic Domain starts as expected.

Note: If you do not install the JDBC drivers before installing the Web-Based Server Instance, the Web-Based Server Instance will not be able to start as expected at the end of the installation. Refer to Install or Uninstall JDBC Drivers to the J2EE Server (WLS or WAS)

.

14.4 Install or Uninstall JDBC Drivers to the J2EE Server (WLS or WAS)

After you have created a J2EE Server (WLS or WAS), you must ensure that requisite JDBC drivers are installed in the J2EE Server, as applicable. Select the database drivers that are required for the connection with your JD Edwards EnterpriseOne database server. If you have not already uploaded JDBC drivers to your Management Console, refer to Manage JDBC Drivers. Some versions of WebLogic Server automatically have a bundled Oracle Database JDBC driver already installed and configured. The JDBC driver install step is not needed if connecting to an Oracle database that is supported with the WebLogic bundled JDBC driver.

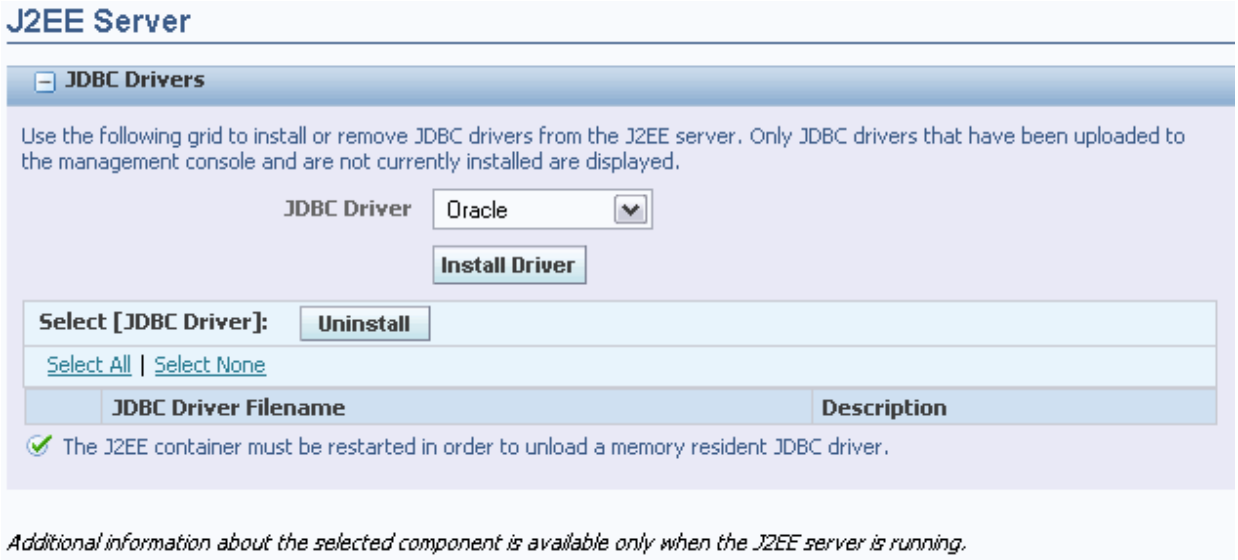
In addition to and in conjunction with the procedure previously described in Manage JDBC Drivers this section describes:

- Install JDBC Drivers to the J2EE Server (WLS or WAS)
- Uninstall JDBC Drivers from the J2EE Server (WLS or WAS)

14.4.1 Install JDBC Drivers to the J2EE Server (WLS or WAS)

To install JDBC drivers to the J2EE Server (WLS or WAS):

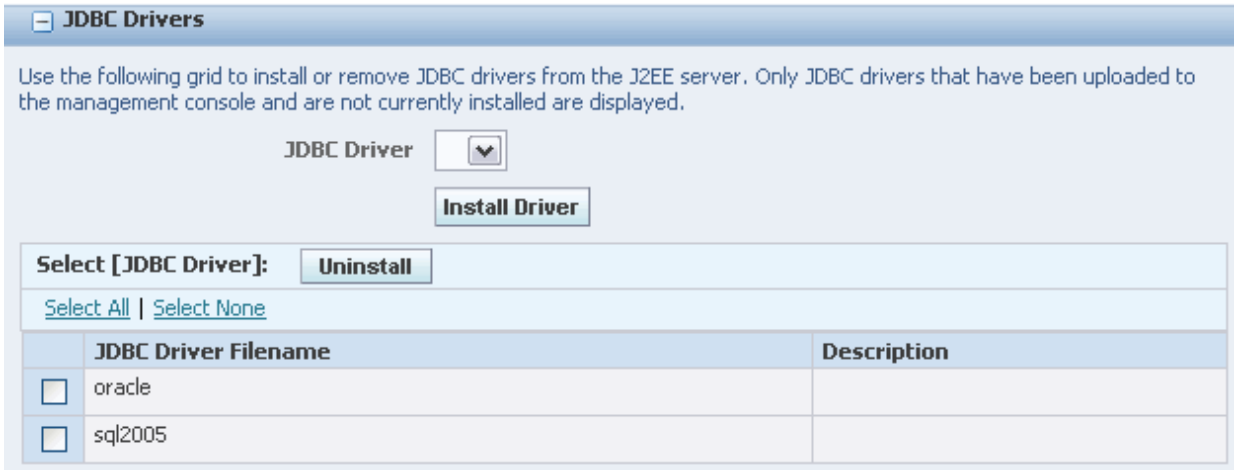
1. Click the link for a J2EE Server (WLS or WAS).



2. Use the *JDBC Driver* dropdown to select the JDBC driver to install.

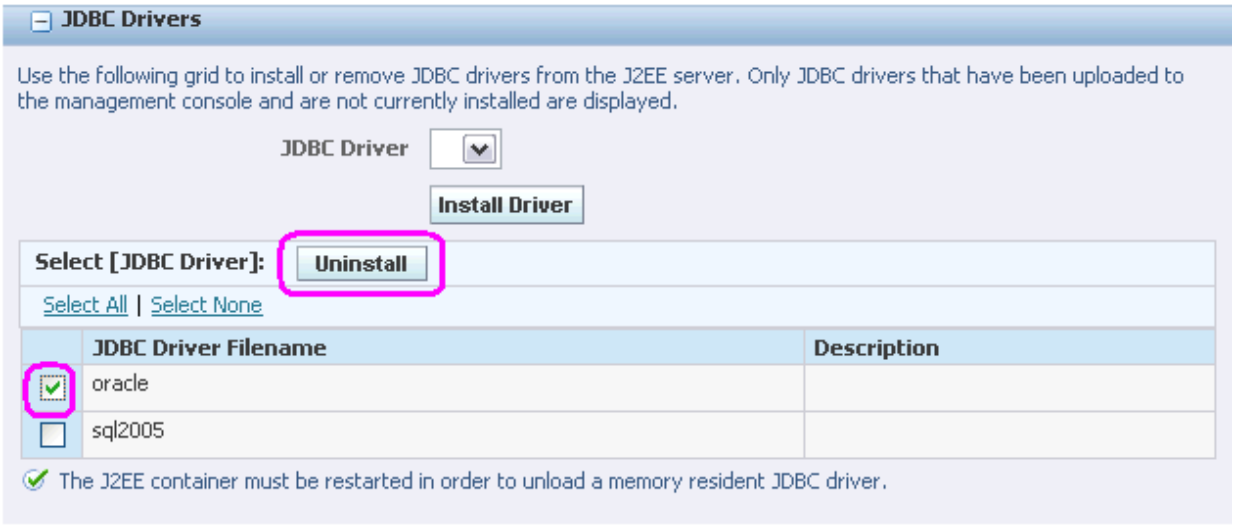
> **Note:** Only JDBC drivers that have been uploaded to the management console but are not currently installed are displayed.

3. Click the *Install Driver* button.



Server Manager installs the driver and adds it to the list of JDBC drivers that can be uninstalled.

14.4.2 Uninstall JDBC Drivers from the J2EE Server (WLS or WAS)



To uninstall a JDBC driver from a J2EE Server (WLS or WAS):

1. From the JDBC Drivers section of the page, select the *JDBC Driver Filename* to be deleted.
2. Click the *Uninstall* button.

Note: If you Uninstall a JDBC driver, the J2EE Server (WLS or WAS) must be restarted in order to unload a memory resident JDBC driver.

15

Manage an Application Server and Related Components

This chapter describes these application servers:

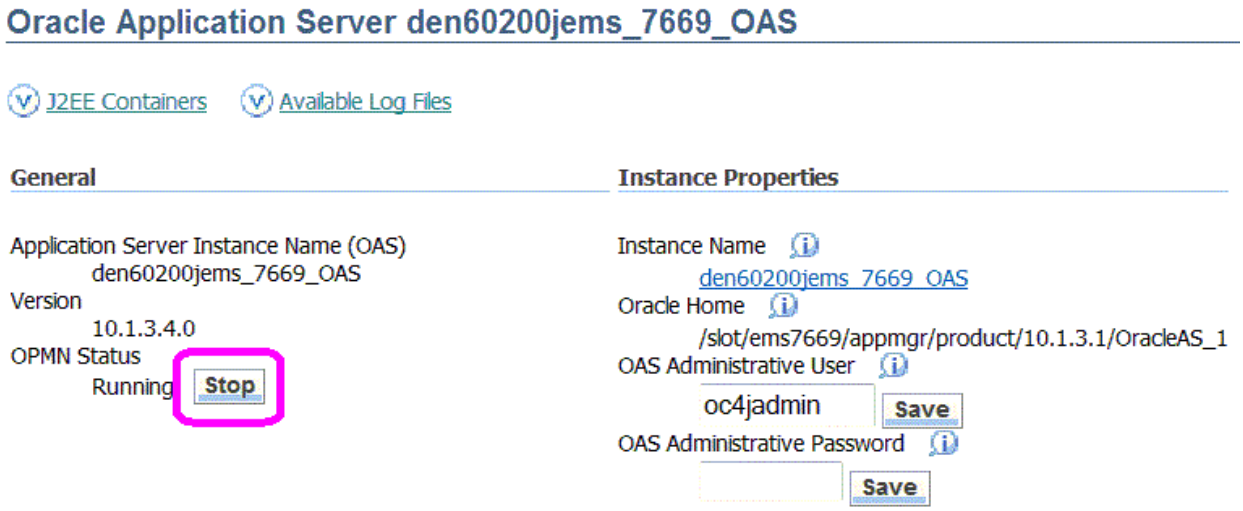
- Section 15.1, "Manage an Oracle Application Server (OAS) Instance"
- Section 15.2, "Manage a WebSphere Application Server (WAS) Instance"
- Section 15.3, "Manage a WebLogic Server Instance"

15.1 Manage an Oracle Application Server (OAS) Instance

This section describes:

- Start or Stop the Oracle Application Server
- General
- Instance Properties
- Start, Stop, or Restart the Oracle HTTP Server
- Grid Items for Oracle HTTP Servers
- Start, Stop, Restart, or Delete a J2EE Server Container
- Grid Items for J2EE Server Container
- Available Log Files

15.1.1 Start or Stop the Oracle Application Server



When you click a link for an installed Oracle Application Server Managed Instance, the operational status of the server is indicated by *OPMN Status* field:

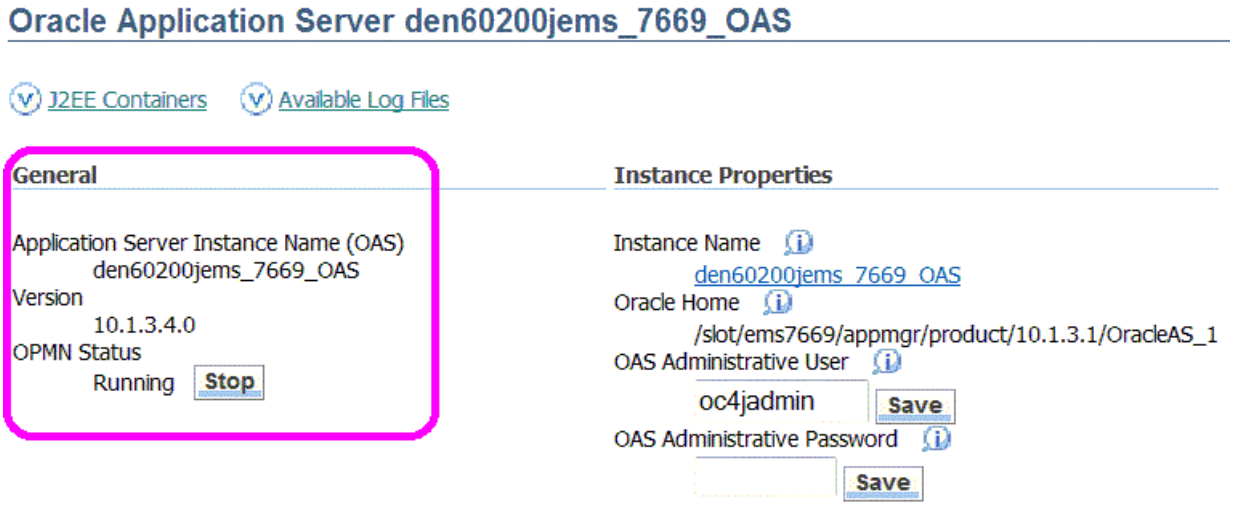
- *Started*

  If the status is *Started*, you can click the *Stop* button to stop the Oracle Application Server.

- *Stopped*

  If the status is *Stopped*, you can click the *Start* button to start the Oracle Application Server.

15.1.2 General



When you select an Oracle Application Server Managed Instance, the top left portion of the page contains a *General* area that includes these fields:

- *Application Server Instance Name (OAS)*

  Displays the name of the OAS Application Server.

  In this example, the Instance Name is: *Application Server1*.

- *Version*

  Displays the version of the Oracle Application Server.

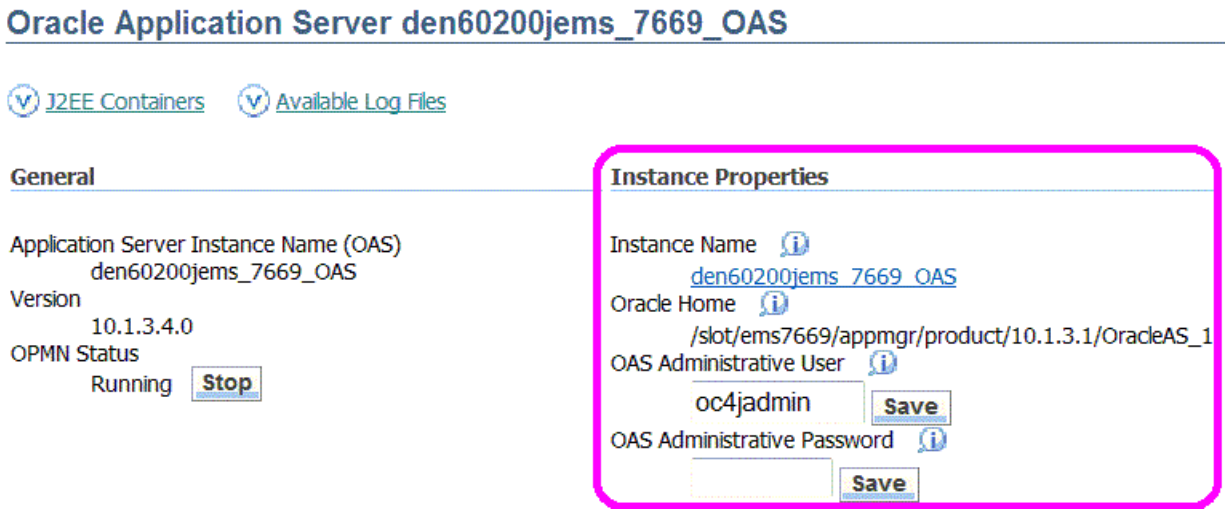
  In this example, the Version is 10.1.3.1.0.

- *OPMN Status*

  Displays the operational status of the Oracle Process Manager and Notification (OPMN) Server.

  OPMN is installed and configured with every Oracle Application Server installation type and is essential for running Oracle Application Server.

15.1.3 Instance Properties



When you select an Oracle Application Server Managed Instance, the top right portion of the page contains an *Instance Properties* area that includes these fields:

- *Instance Name*

  Identifies the unique name assigned to the managed instance at the time it was created or registered.

  In this example, the Instance Name is: *Application Server1*.

- *Oracle Home*

  Displays the complete path to the Oracle home where this Oracle Application Server instance was installed.

  In this example, the Oracle Home is `/u02/oracle10131`.

- *OAS Administrative User*

  Displays the administrative user credential that is used by Server Manager to perform administrative tasks on the Oracle Application Server instance. This is typically the oc4jadmin administrative account.

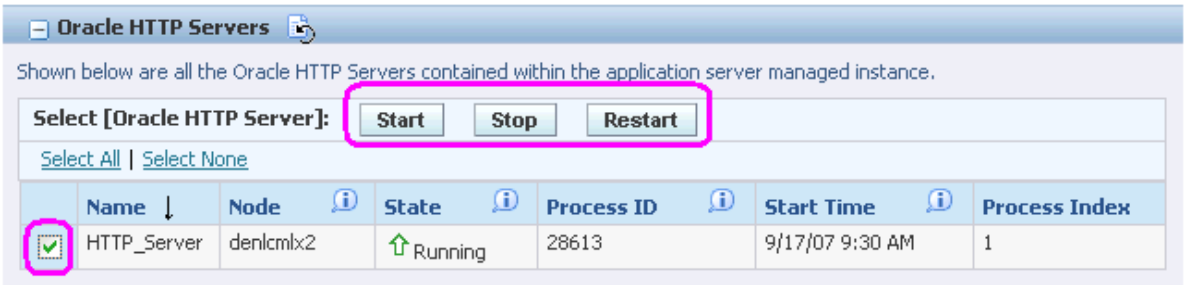
  This section includes a Save button that enables you to change your administrative user name.

- *OAS Administrative Password*

Displays the administrative password credential that is used by Server Manager to perform administrative tasks on the oracle application server instance. This is typically the oc4jadmin administrative account.

This section includes a Save button that enables you to change your administrative user password.

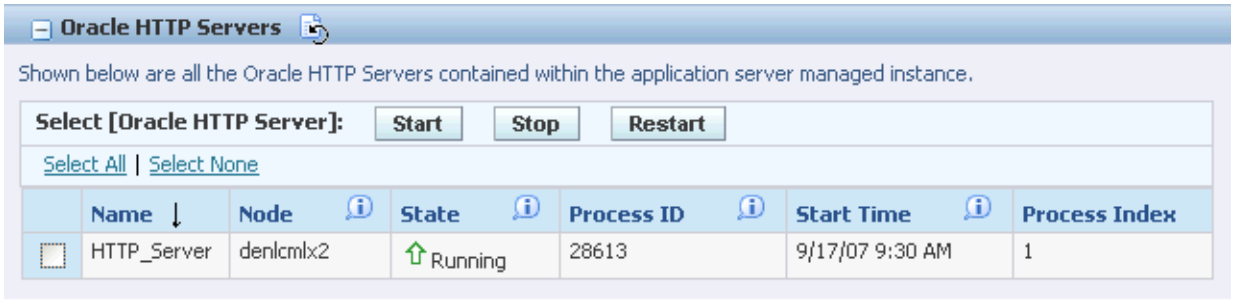
15.1.4 Start, Stop, or Restart the Oracle HTTP Server



To start, stop, and restart an Oracle HTTP Server, first select the server using the check box and then click the appropriate button.

Tip: After you perform any Start, Stop, or Restart action on this page, you can click the Reload icon on the Oracle HTTP Servers title bar to update the grid.

15.1.5 Grid Items for Oracle HTTP Servers



When you select an Oracle Application Server Managed Instance, the *Oracle HTTP Servers* section includes all the Oracle HTTP Servers contained within the application server Managed Instance. These grid items are displayed:

- *Name*

  Displays the name of the Oracle HTTP Server that was assigned when the Oracle Application Server was installed.

- *Node*

  Displays the name of the host on which the process is running.

- *State*

  Indicates the current state of the HTTP server.

- *Process ID*

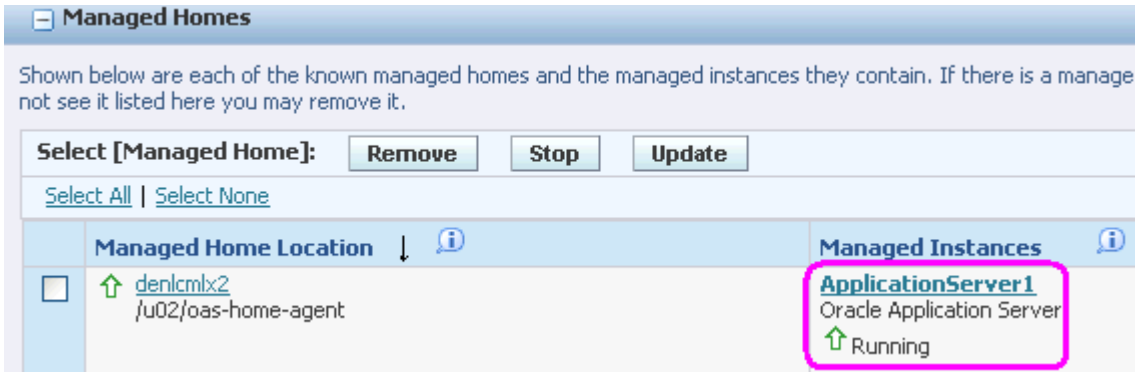
Displays the process identifier of the running Oracle HTTP Server process.

- *Start Time*

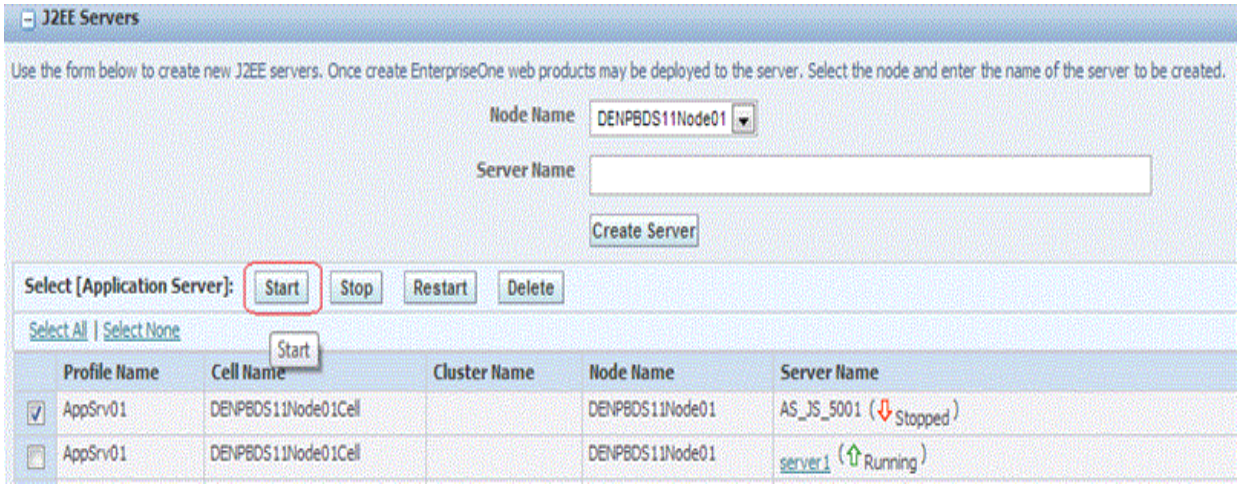
  Indicates the time that the HTTP server was started.

15.1.6 Start, Stop, Restart, or Delete a J2EE Server Container

To start, stop, restart, or delete a J2EE Server Container:



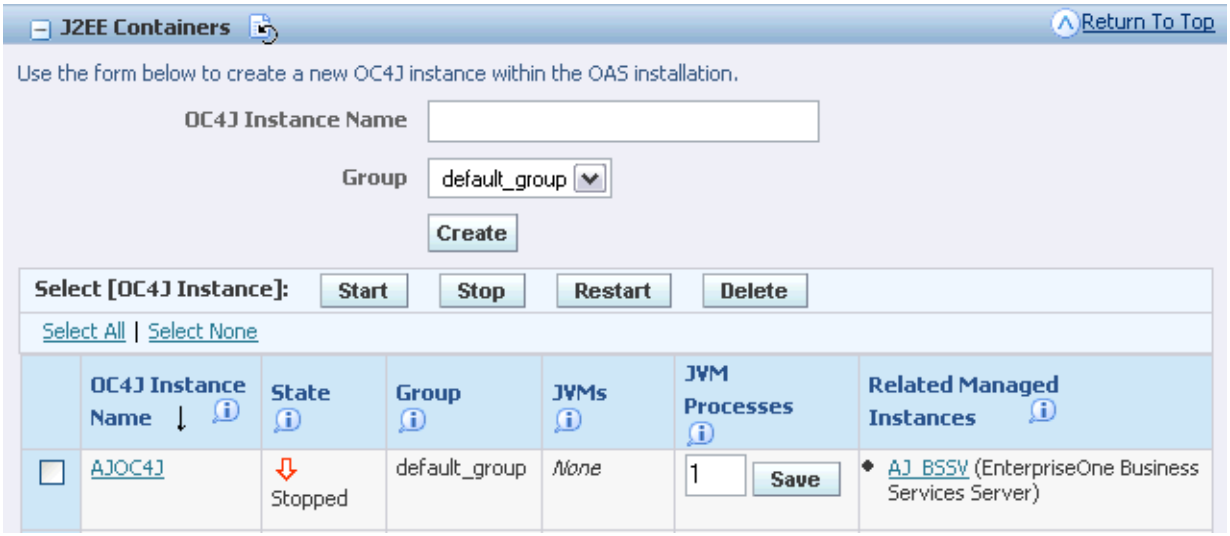
1. Select the existing Managed Instance for a running Oracle Application Server Managed Instance with which you wish to start, stop, restart, or delete a J2EE Server.



2. In the *J2EE Servers* section of the page, select the J2EE Server which you want to start, stop, restart, or delete.
3. Click the *Start*, *Stop*, *Restart*, or *Delete* button as appropriate.

Tip: The Server Manager displays a dialog indicating that the selected operation is in progress and will continue even if you close the browser. After the dialog is no longer displayed, you can refresh the Management Console page to verify that the newly-created J2EE Server Container is in the expected state.

15.1.7 Grid Items for J2EE Server Container



When you select an Oracle Application Server Managed Instance, the *J2EE Server Containers* section lists all the OC4J Instances contained within the OAS installation. These grid items are displayed:

- *OC4J Instance Name*

  Displays the name of the OC4J instance.

- *State*

  Shows the current state of the OC4J instance.

- *Group*

  Displays the Oracle Application Server defined group to which the OC4J instance belongs.

- *JVMs*

  Specifies the number of Java virtual machines that are currently running within the OC4J instance.

- *JVM Processes*

  Defines the number of JVM processes to simultaneously run within this container.

- *Related Managed Instances*

  Lists any EnterpriseOne servers that are deployed to this OC4J instance.

15.1.8 Available Log Files

Refer the chapter of this guide entitled: Available Log Files

15.2 Manage a WebSphere Application Server (WAS) Instance

This section describes:

- Start, Stop, or Restart the WebSphere Application Server
- Profiles and Servers
- Start, Stop, or Restart a J2EE Server

- Available Log Files

15.2.1 Start, Stop, or Restart the WebSphere Application Server

When you click on the Managed Instance for your installed WebSphere Application Server, you can view the status of the installed applications servers in the *Application Servers* column of the grid.

- *Started*

  If the status is *Started*, you can select one or more application servers using the check box and then click the *Stop* button to stop the WebSphere Application Server.

- *Stopped*

  If the status is *Stopped*, you can select one or more application servers using the check box and then click the *Start* or *Restart* button to start or restart the WebSphere Application Server.

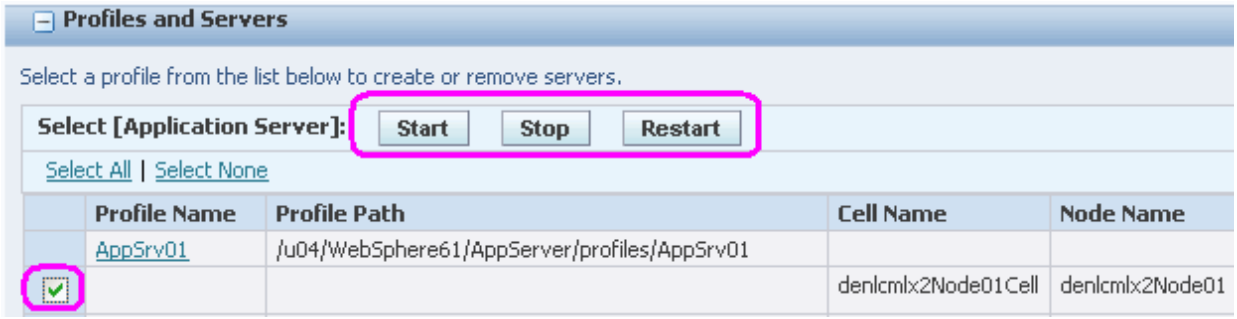
15.2.2 Profiles and Servers

This section describes:

- Start, Stop, or Restart a WebSphere Application Server
- Grid Items for Profiles and Servers

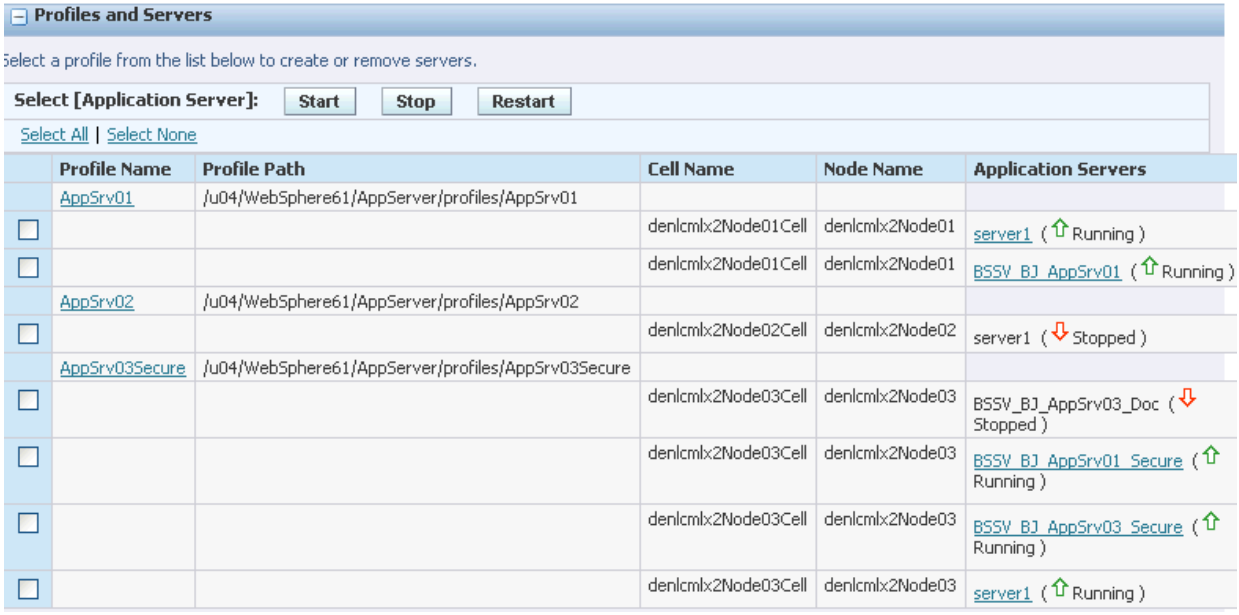
15.2.2.1 Start, Stop, or Restart a WebSphere Application Server

When you select a WebSphere Application Server the *Profiles and Servers* section allows you to select a profile from a list that to start, stop, or restart a selected application server.



15.2.2.2 Grid Items for Profiles and Servers

The *Profiles and Servers* section of the page includes these grid items:



- *Profile Name*

  These are clickable links to existing profiles in the WebSphere environment. These profiles can only be created using the WebSphere administration tool.

- *Profile Path*

  Displays the path to the WebSphere profile.

- *Cell Name*

  Displays the name of the cell within the WebSphere profile.

- *Node Name*

  Displays the name of the node within the WebSphere cell.

- *Application Servers*

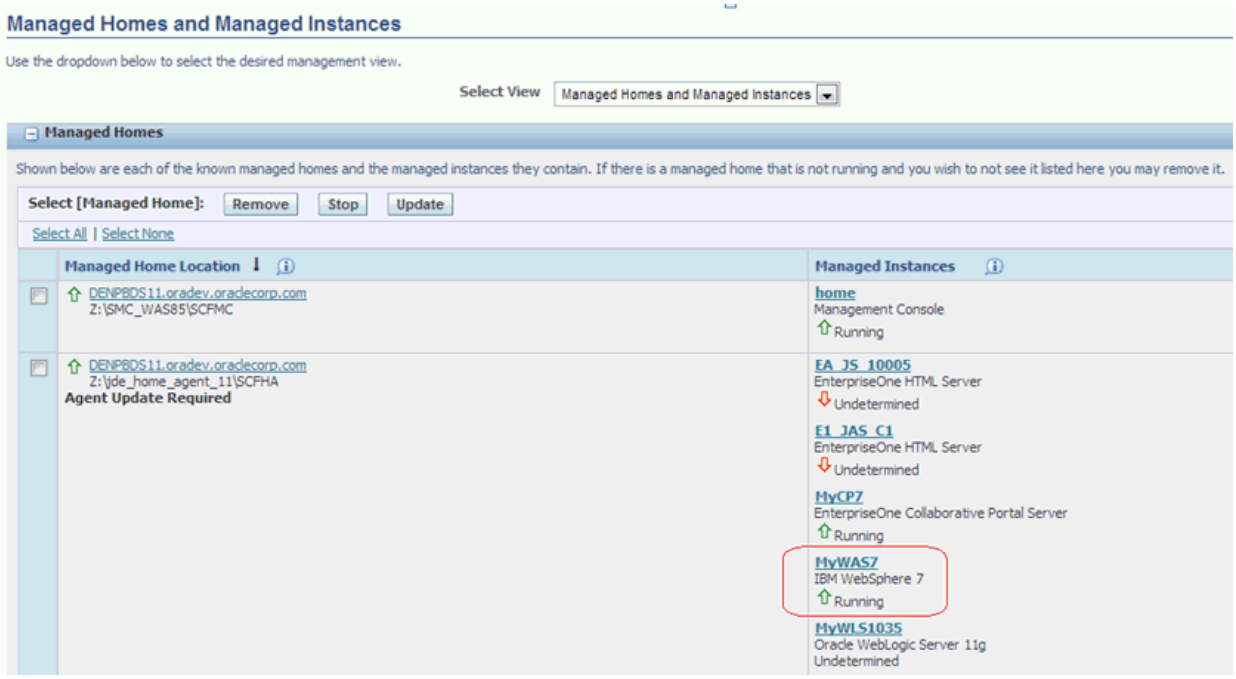
  Lists all applications servers associated with each profile. The status of the application servers is also shown. If the status is Running, the display includes a clickable link to the application server.

- *Related Managed Instances*

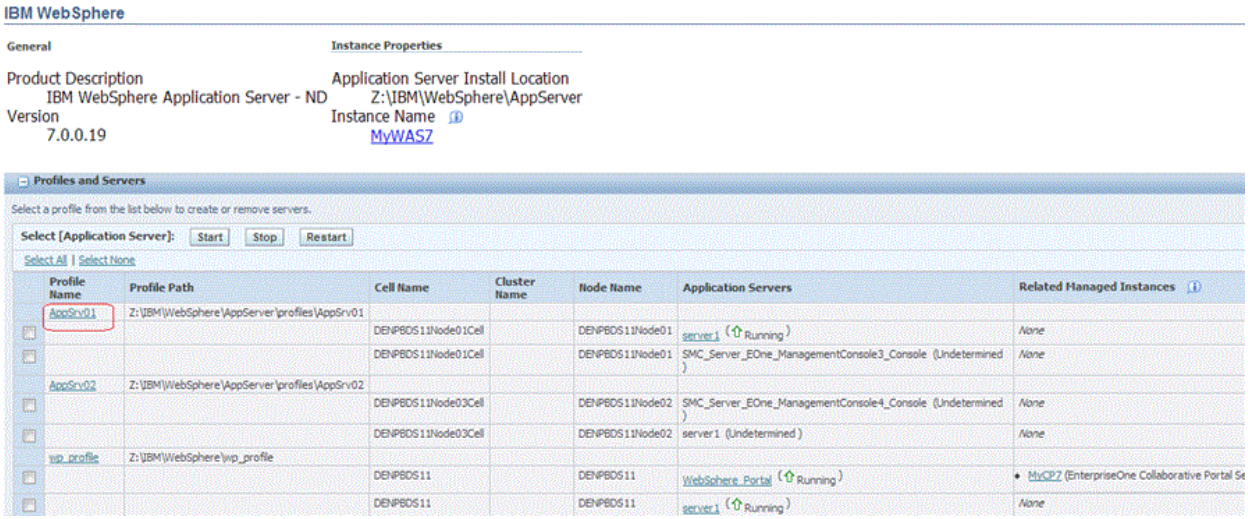
  Lists clickable links to EnterpriseOne servers that are deployed for this profile on this WebSphere application server.

15.2.3 Start, Stop, or Restart a J2EE Server

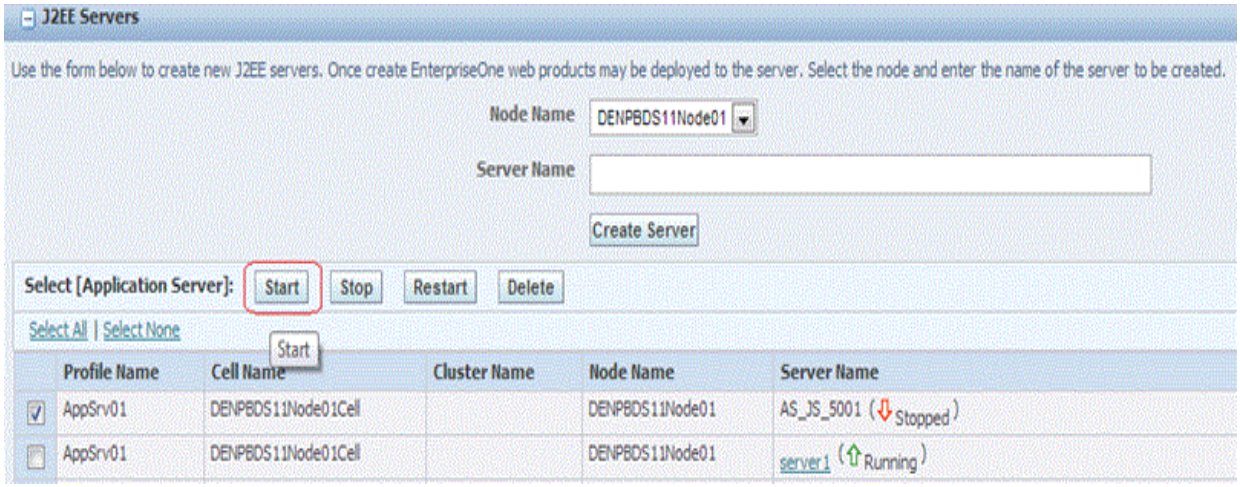
To start, stop, or restart a J2EE Server:



1. Select the existing Managed Instance for a running WebSphere Application Server with which you wish to start, stop, or restart J2EE Server.



2. In the *Profiles and Servers* section of the page, click the Profile Name that contains the J2EE Server that you want to start, stop, or restart.



3. Click the *Start*, *Stop*, or *Restart* button as appropriate.

> **Tip:** The Server Manager displays a progress monitor indicating that the Start operation is in progress and will continue even if you close the browser. After the progress monitor is no longer displayed, you can refresh the Management Console page to verify that the J2EE Server is in the expected state.

15.2.4 Available Log Files

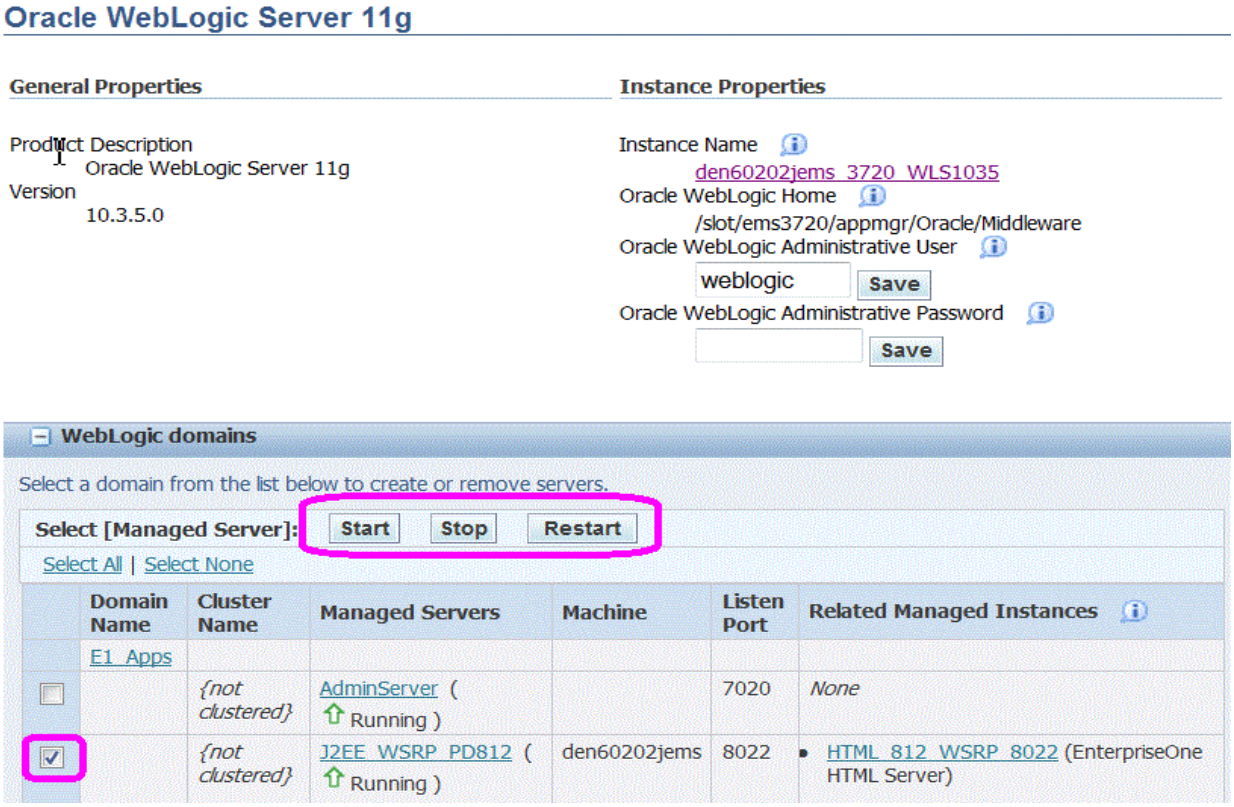
For information on log files for Managed Instances, refer to the chapter entitled: Available Log Files.

15.3 Manage a WebLogic Server Instance

This section describes:

- Start, Stop, or Restart the WebLogic Server
- Instance Properties

15.3.1 Start, Stop, or Restart the WebLogic Server



To start, stop, and restart an Oracle WebLogic Server, first select the server using the check box and then click the appropriate button.

- *Started*

  If the status is *Started*, you can select one or more application servers using the check box and then click the *Stop* button to stop the WebSphere Application Server.

- *Stopped*

  If the status is *Stopped*, you can select one or more application servers using the check box and then click the *Start* or *Restart* button to start or restart the WebSphere Application Server.

15.3.2 Instance Properties

When you select an Oracle WebLogic Server Managed Instance, the top right portion of the page contains an *Instance Properties* area that includes these fields:

- *Instance Name*

  Identifies the unique name assigned to the managed instance at the time it was created or registered.

  In this example, the Instance Name is: *NEWAdmin*.

- *Oracle WebLogic Home*

  Displays the complete path to the Oracle Home where this Oracle WebLogic Server instance was installed. In this example, the Oracle Home is:

  In this example, the Oracle Home is `/u01/Middleware2`.

  > **Tip:** You can determine the complete path to your Oracle Home by issuing the pwd command from the root directory where your Oracle WebLogic Server is installed.

- *Oracle WebLogic Administrative User*

  Displays the administrator user credential that you specified when creating the domain and is used by Server Manager to perform administrative tasks on the Oracle WebLogic Server instance. By definition, all servers in the same domain have the same administrative user and password.

  This section includes a Save button that enables you to change your administrative user name.

- *Oracle WebLogic Administrative Password*

  Displays the administrator password credential that you specified when creating the domain and is used by Server Manager to perform administrative tasks on the Oracle WebLogic Server instance. By definition, all servers in the same domain have the same administrative user and password.

  This section includes a Save button that enables you to change your administrative user password.

16

Register or Create a JD Edwards Enterprise Server as a New Managed Instance

This chapter discusses these topics that are necessary to register an existing or create a new managed Enterprise Server as a Managed Instance:

- Section 16.1, "Visual Studio Requirements for Microsoft Windows-based Enterprise Servers"
- Section 16.2, "Prerequisites and Recommended Registration or Creation Sequence for an Enterprise Server as New Managed Instance"
- Section 16.3, "Register an Existing Enterprise Server as a New Managed Instance"
- Section 16.4, "Create (Install) an Enterprise Server as a New Managed Instance"

16.1 Visual Studio Requirements for Microsoft Windows-based Enterprise Servers

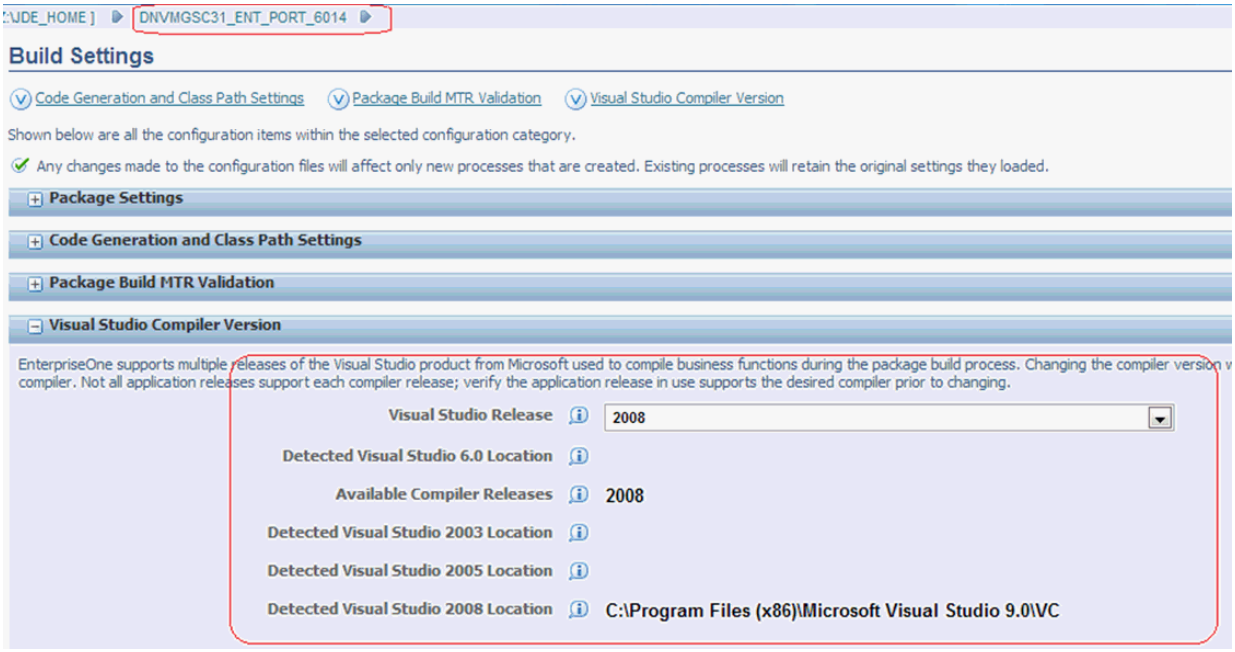
Server Manager detects the supported and installed versions of Visual Studio for Microsoft Windows-based Enterprise Server.

The supported version versions of Visual Studio are 6.0, 2003, 2005, 2008, 2010.

> **Caution:** Not all JD Edwards EnterpriseOne Applications and Tools releases support all of the above Visual Studio versions. Refer to the JD Edwards EnterpriseOne Certifications (MTRs) and Package Management Guide for support levels.

The JD Edwards EnterpriseOne Administrator can navigate to the Compiler Selection screen by navigating to the Enterprise Server Instance and clicking the **Package Builds** link.

As shown below, the supported and detected versions of Visual Studio on Microsoft Windows-based JD Edwards EnterpriseOne Enterprise Server. The Administrator can select the appropriate version of Visual Studio and click the **Apply** button. As a result, Server Manager updates the entries in the `[JDE_CG]` section and `[BSFN BUILD]` section of the `jde.ini` file.



16.2 Prerequisites and Recommended Registration or Creation Sequence for an Enterprise Server as New Managed Instance

The following steps represent the prerequisites and recommended sequence for registering or creating an Enterprise Server as a new Managed Instance:

1. Prerequisite: Management Agent is installed on target machine.

   Refer to Chapter 5, "Install a Management Agent".

2. Prerequisite: The Enterprise Server Software Component is uploaded to the Management Console.

   Refer to Chapter 11.1, "Upload Software Components".

3. Prerequisite: The Enterprise Server Software Component is distributed to the target Managed Home.

   Refer to Chapter 11.2.1, "Distribute Software Components to Managed Homes".

4. Register an existing Enterprise Server or Create (Install) an Enterprise Server as a New Managed Instance.

See Also

- Refer to the *JD Edwards EnterpriseOne Tools Release 8.98 Reference Guide* for additional tasks and topics related to Server Manager.

16.3 Register an Existing Enterprise Server as a New Managed Instance

The only Managed Instance that can be registered after being installed by a method other than Server Manager is a JD Edwards EnterpriseOne Enterprise Server. The Enterprise Server may have been installed using the Platform Pack installer or manually created outside of Server Manager. Regardless of the method of creation any Enterprise Server running Tools Release

8.91 (and later) may be registered with Server Manager in preparation for upgrading to 8.97 (and later). Management of Tools Releases 8.96 outside the immediate upgrade steps is not supported.

Only JD Edwards EnterpriseOne Enterprise Servers that are registered with the Management Console can be managed by the Management Console. The Enterprise Server may have been installed using the Platform Pack installer or manually created outside of Server Manager. Regardless of the method of creation, any Enterprise Server running Tools Release 8.97 (and later), including multi-foundation Enterprise Servers, is fully supported.

Note: Registration of an Enterprise Server requires that a Management Agent first be installed on Enterprise Server. Refer to Chapter 5, "Install a Management Agent".

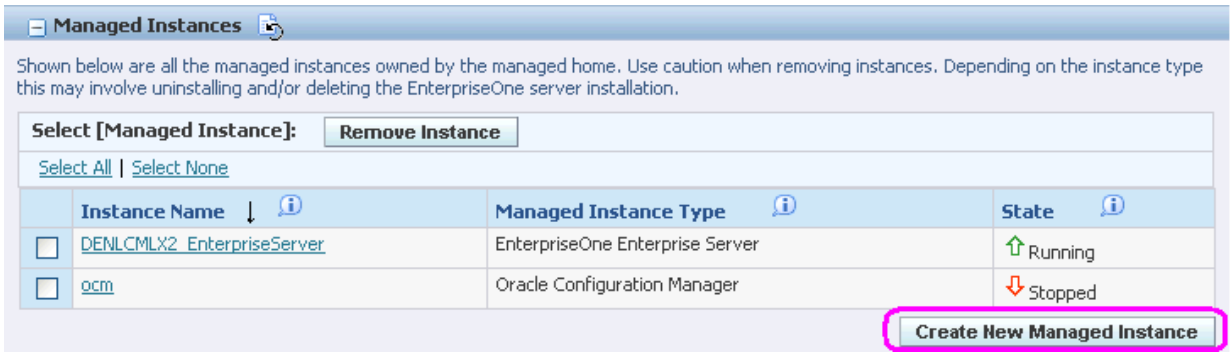
Registration of Tools Release prior to 8.97 is only intended to facilitate an upgrade to Tools Release 8.97 (and later). Once you have upgraded to Tools Release 8.97 and later you cannot use Server Manager to revert to a release prior to the base release of Tools Release 8.97. If you want to run simultaneous releases of 8.97 (and later) and releases prior to 8.97, you should use Multiple Foundations, which is described in the *JD Edwards EnterpriseOne Tools Release 8.98 Reference Guide*.

UNIX Installation Note.

On UNIX-based platforms, you must install and run the Management Agent as the same operating system user as the JD Edwards EnterpriseOne Enterprise Server.

To register an existing Enterprise Server instance:

1. Select the Managed Home with which you wish to register the Enterprise Server.

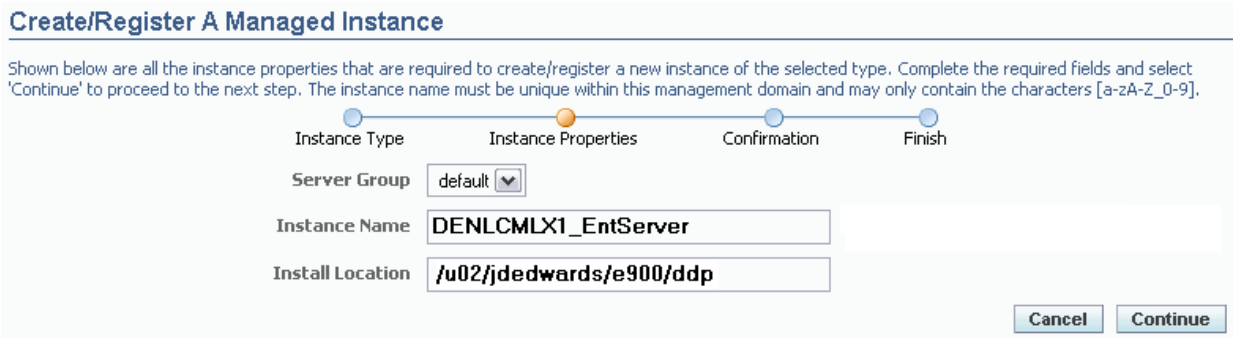


2. Click the *Create a New Managed Instance* button to create the Managed Instance within the Managed Home.

3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   Register an Existing Enterprise Server

4. Click Continue.



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the dropdown to select the Server Group to which you want this instance to belong.

   - *Instance Name*

     Enter a unique name for the instance name.

   - *Install Location*

     Enter a valid install location for the existing Enterprise Server. For example:

     UNIX:

     `/u02/jdedwards/e900/ddp`

     Windows:

     `c:\jdedwards\e900\ddp`

     For both Windows and UNIX, you must specify the *Install Location* as the full path including the *ddp* suffix.

Note: The DDP folder is only available through release 9.0. It is not available in release 9.1.

AS/400:

`e900SYS`

AS/400 Enterprise Servers. These systems do not require a full path. Instead, you should only enter the library name that corresponds to the IFS directory in which JD Edwards EnterpriseOne is installed. Ensure that there are no slash characters in the Install Location.

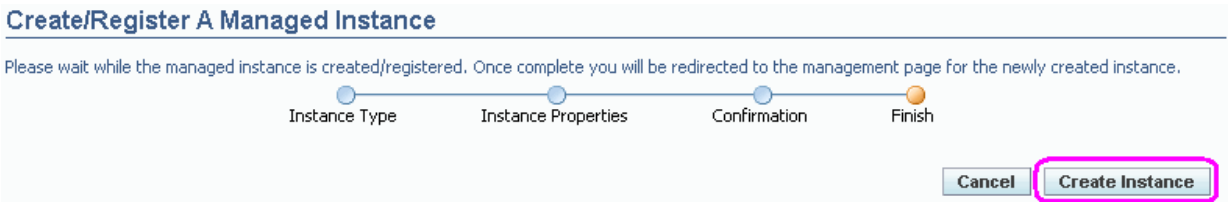
6. Click Continue.

7. On Create/Register a Managed Instance, Confirmation, review the key configuration items, where the web page displays a variety of fields depending on the database and environments of your installation

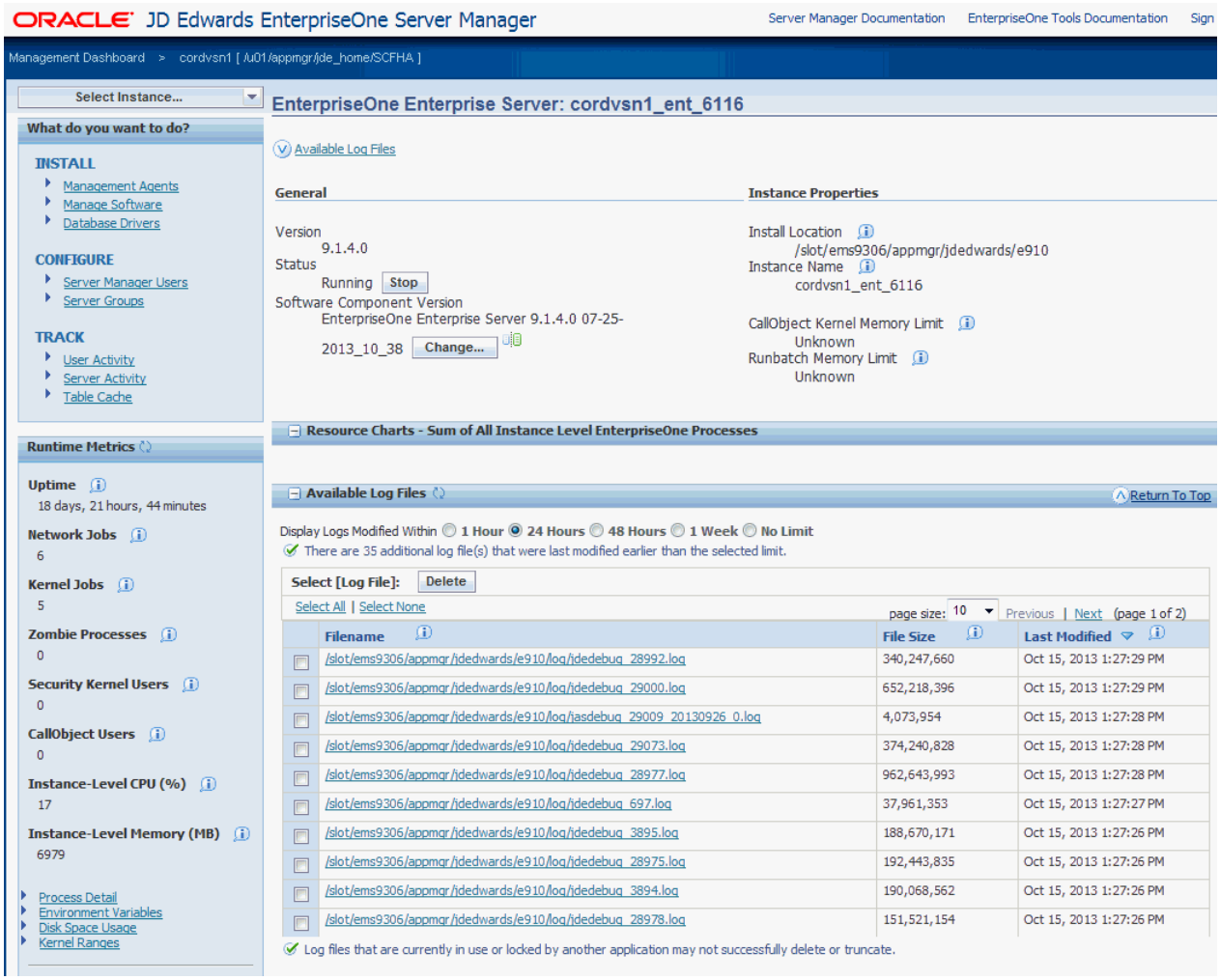
   You can further configure any item as required.

Note: If the server was installed using the Platform Pack installer, typically you are not required to perform further configuration. Server Manager reads these values from the existing Enterprise Server installation; they are valid if the Enterprise Server was functioning properly at the time of registration.

8. Click Continue.



9. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the registration of the Enterprise Server.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Enterprise Server. This server also appears as a Managed Instance in the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the web page:

- *General*
  - Software Component Version

    Displays the version of this software component.
  - Status

    Valid values are:

    Running

    When the status is Running, the *Stop* button is available.

    Stopped

    When the status is Stopped, the *Start* button is available.
- *Instance Properties*

  Install Location

Displays the full path for the install location of the selected Managed Instance.

Instance Name

Displays a clickable link for the name of the selected Managed Instance.

For information on log files, refer to the chapter entitled Chapter 23, "Available Log Files".

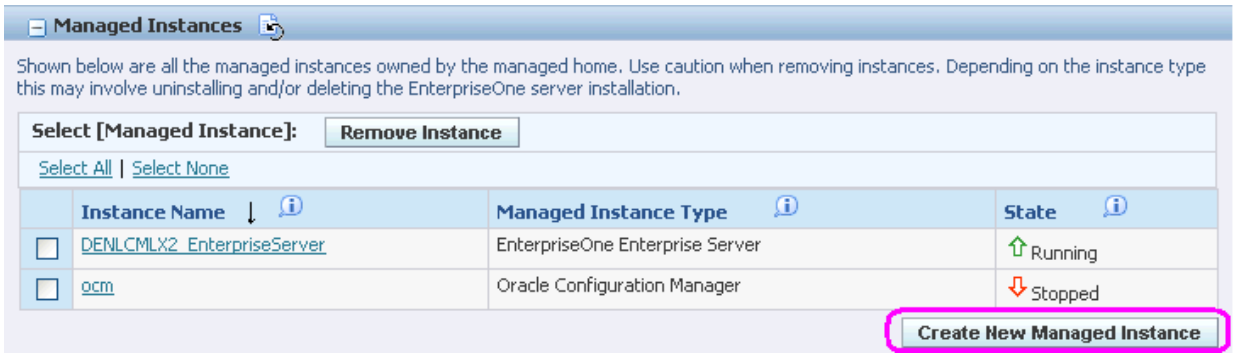
16.4 Create (Install) an Enterprise Server as a New Managed Instance

You can use Server Manager to install new Enterprise Servers. However, these Enterprise Servers only contain a system (foundation) and no package or path-code. These Enterprise Servers are not fully functional. Additional steps are required to convert them into functional servers. Additionally, at least one Enterprise Server in your installation must be installed outside of Server Manager using the Platform Pack installer which includes the platform- and database-dependent application data and path codes.

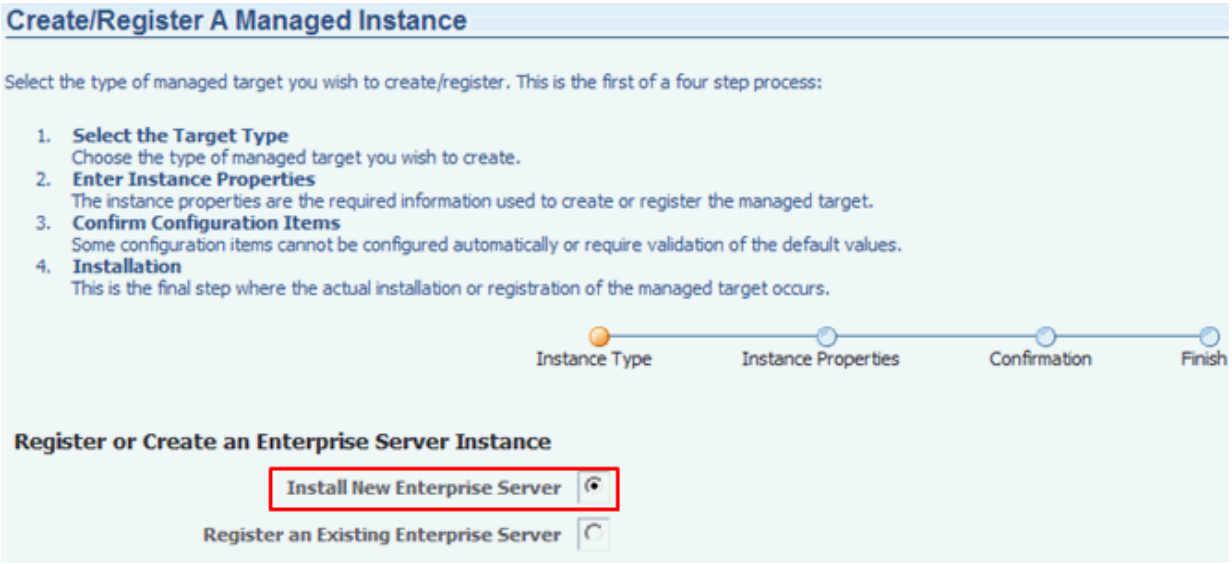
To create an Enterprise Server as a new Managed Instance using Server Manager, you must obtain the appropriate Enterprise Server software component either directly from the Management Console or from Customer Connection using Change Assistant. The Managed Software Component must be uploaded to the Management Console and distributed to the Management Agent to which you wish to install the new Enterprise Server. For additional information, refer to Chapter 11, "Managed Software Components".

To create an Enterprise Server as a new Managed Instance:

1. Select the Managed Home with which you wish to create the Enterprise Server as a new Managed Instance.



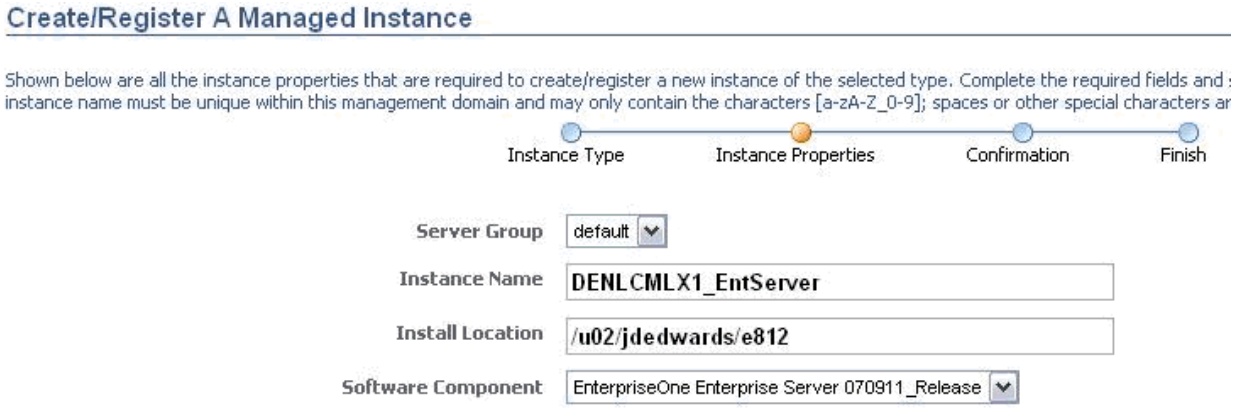
2. Click the *Create a New Managed Instance* button to create the Managed Instance in the Managed Home.



3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   Install New Enterprise Server

4. Click Continue.



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the dropdown to select the Server Group to which you want this instance to belong.

   - *Instance Name*

     Enter a unique name for the instance name.

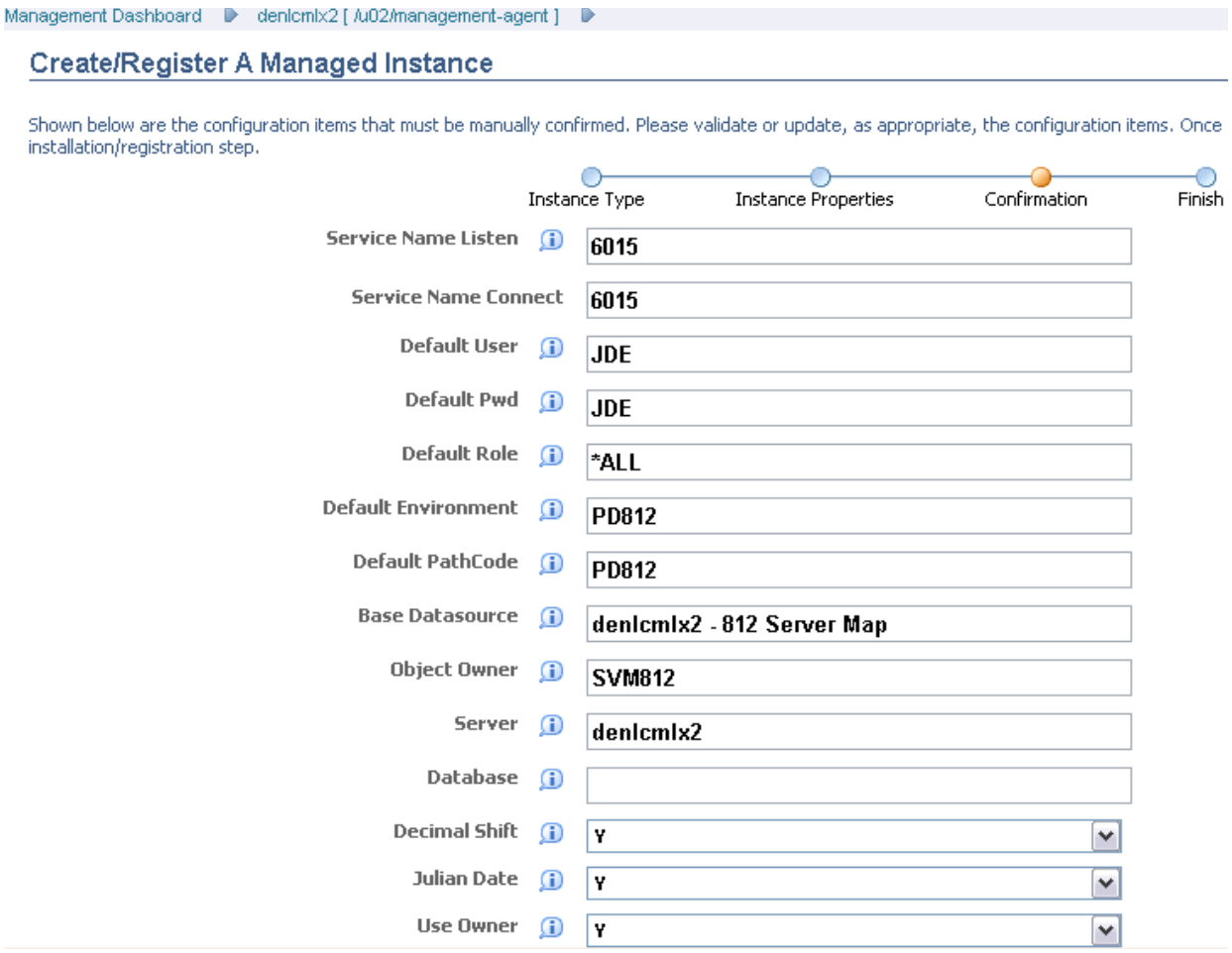
   - *Install Location*

     Enter a valid install location for the existing Enterprise Server.

   - *Software Component*

     Use the dropdown to select the software component from the list of Enterprise Server components distributed to this Management Agent.

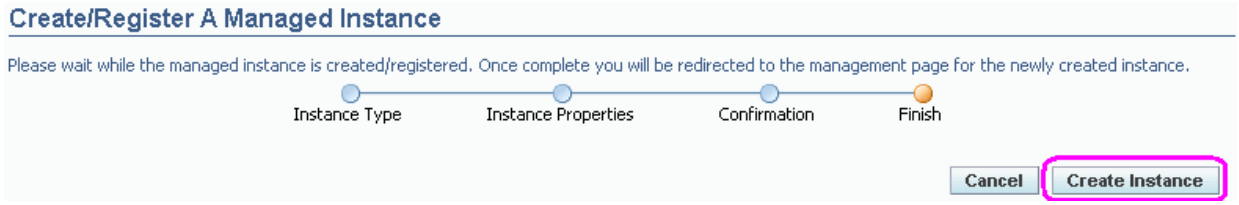
6. Click Continue.



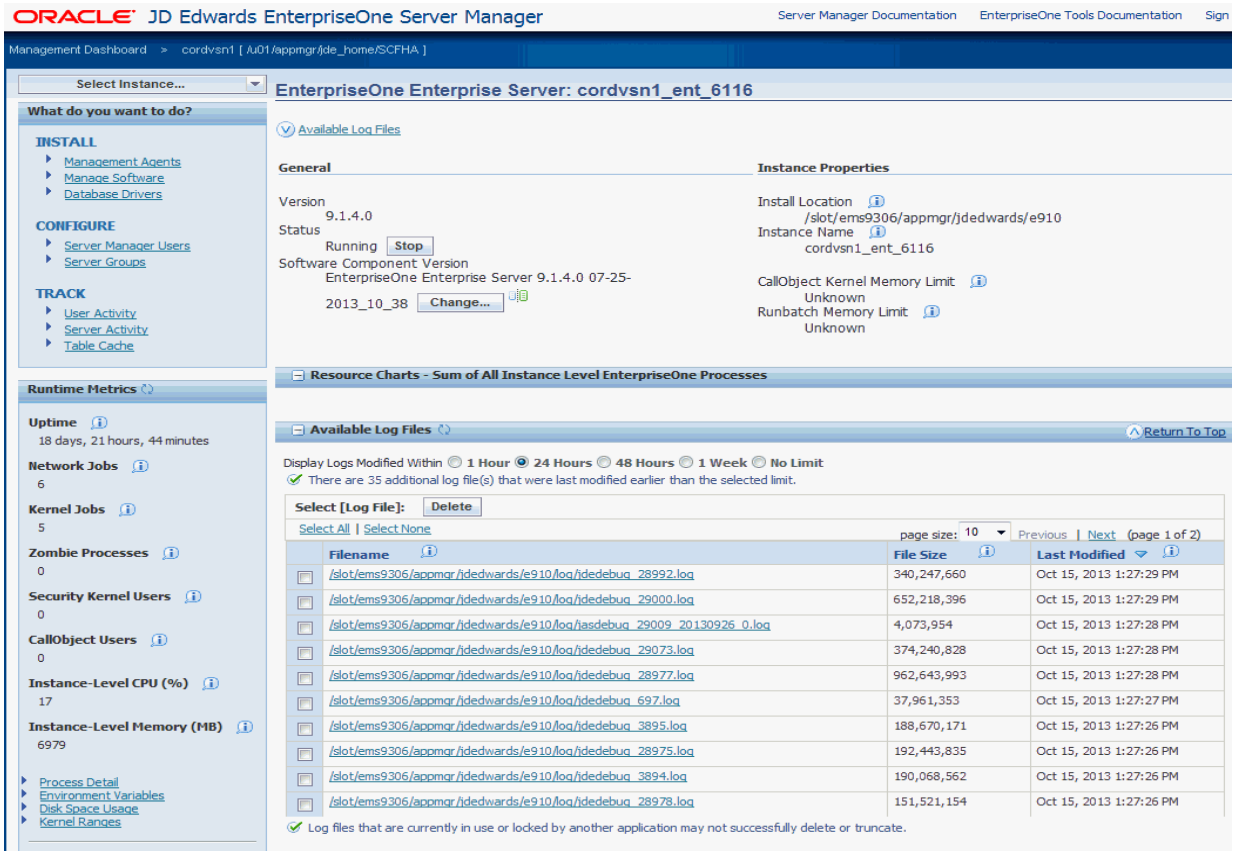
7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The web page displays a variety of fields depending on the database and environments of your installation.

   You can further configure any item as required.

8. Click Continue.



9. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the installation of the Enterprise Server.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Enterprise Server. This server also appears as a Managed Instance in the corresponding Managed Home.

After you have used Server Manager to install your 8.97 (and later) Tools Release to an IBM i-based Enterprise Server, as in previous JD Edwards EnterpriseOne Tools Releases, you must re-link the Business Functions. For instructions, refer to the chapter entitled: *Re-Linking Business Functions* in the *JD Edwards EnterpriseOne Tools Release 8.98 Reference Guide*.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the web page:

- *General*
  - Software Component Version

    Displays the version of this software component.
  - Status

    Valid values are:

    Running

    When the status is Running, the *Stop* button is available.

    Stopped

    When the status is Stopped, the *Start* button is available.
- *Instance Properties*
  - Install Location

Displays the full path for the install location of the selected Managed Instance.

– Instance Name

  Displays a clickable link for the name of the selected Managed Instance.

For information on log files, refer to the chapter entitled: Chapter 23, "Available Log Files".

17

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

This chapter discusses:

- Section 17.1, "Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances"
- Section 17.2, "Create a HTML Web Server as a New Managed Instance"
- Section 17.3, "Create a Transaction Server as a New Managed Instance"
- Section 17.4, "Create a Collaborative Portal Server as a New Managed Instance"
- Section 17.5, "Create a Business Services Server as a New Managed Instance"
- Section 17.6, "Create an Application Interface Services (AIS) Server as a New Managed Instance (Release 9.1 Update 4.2)"

17.1 Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances

These steps represent the prerequisites and recommended installation sequence Managed Instances for JD Edwards EnterpriseOne web-based servers:

1. Prerequisite: Management Agent is installed on the target machine.

   Refer to Install a Management Agent.

2. Prerequisite: Application Server (WLS or WAS) is installed on target machine.

   Refer to *JD Edwards EnterpriseOne HTML Web Server Reference Guide* for details on installing and configuring WLS and WAS.

3. Prerequisite: The Web-Based Server Software Component is uploaded to the Management Console.

   Refer to Upload Software Components.

   Note: *Exception.* There is no Software Component available or required for creating the Business Services Server.

4. Prerequisite: The Web-Based Server Software Component is distributed to the Managed Home.

   Refer to Section 11.2.1, "Distribute Software Components to Managed Homes".

Note: *Exception.* There is no Software Component available or required for creating the Business Services Server.

5. Register an Application Server (WAS or WLS) to create a new Managed Instance for an Application Server in the target Managed Home.

   For WLS 11g, refer to Section 13.4, "Register an Oracle WebLogic Server 11g".

   For WLS 12c, refer to Section 13.5, "Register an Oracle WebLogic Server 12c".

   For WAS 8.5, refer to Section 13.3, "Register a WebSphere Application Server, Version 8.5 (Tools Release 9.1 Update 2.3)".

   For WAS 7.0, refer to Section 13.2, "Register a WebSphere Application Server, Version 7.0".

6. Create a J2EE Container (WLS) or J2EE Server (WAS) in the Application Server.

   Note: There is a one-to-one relationship between a web-based server and a J2EE container. You cannot install more than one web-based server in each J2EE container.

   For WLS 11g, refer to Section 13.4, "Register an Oracle WebLogic Server 11g".

   For WLS 12c, refer to Section 13.5, "Register an Oracle WebLogic Server 12c".

   For WAS 8.5, refer to Section 13.3, "Register a WebSphere Application Server, Version 8.5 (Tools Release 9.1 Update 2.3)".

   For WAS 7.0, refer to Section 13.2, "Register a WebSphere Application Server, Version 7.0".

7. Install JDBC drivers to the J2EE Server (except Collaborative Portal Server).

   Refer to Section 14.4.1, "Install JDBC Drivers to the J2EE Server (WLS or WAS)".

   Note: If you do not install the JDBC drivers before installing the Web-Based Server Instance, the Web-Based Server Instance does not start as expected at the end of the installation unless the server already has a bundled JDBC driver as part of the install.

8. Install the web-based server Managed Instance

   Refer to:

- Section 17.2, "Create a HTML Web Server as a New Managed Instance"
- Section 17.3, "Create a Transaction Server as a New Managed Instance"
- Section 17.4, "Create a Collaborative Portal Server as a New Managed Instance"
- Section 17.5, "Create a Business Services Server as a New Managed Instance"

17.2 Create a HTML Web Server as a New Managed Instance

You must use Server Manager to install a new HTML Web Server instance.

WebSphere Security Consideration for Federated Servers. For WebSphere Federated Servers only, if Administrative Security is turned on for the profile containing the deployment manager,

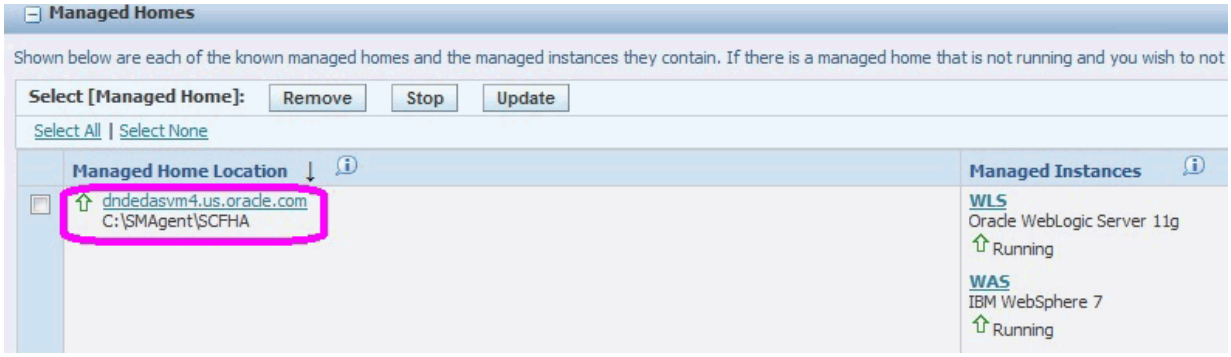
you must turn it OFF before proceeding with the creation of the Managed Instance for the HTML Web Server. After disabling security, you must restart the deployment manager. All nodes in the management domain will also have to be restarted and resynchronized. The Management Agent to which the WebSphere Application Server is registered must also be restarted. For additional details, refer Post Install for a Federated Server in Network Deployment Mode to in this chapter.

See Also

- Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances
- *JD Edwards EnterpriseOne HTML Web Server Reference Guide* for details on installing and configuring WLS or WAS and additional tasks and topics related to Server Manager.

To install an JD Edwards EnterpriseOne HTML Web Server instance:

1. Select the Managed Home in which you wish to install the HTML Web Server.

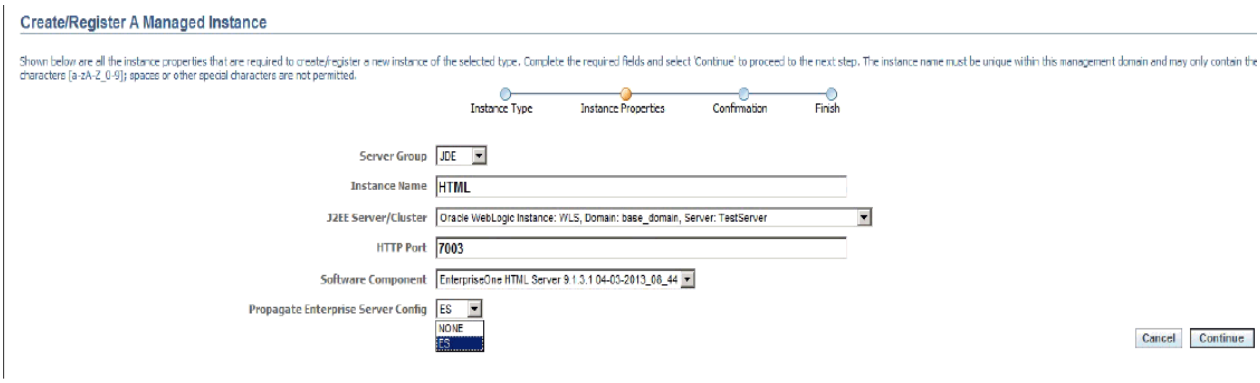


2. Click the *Create a New Managed Instance* button to create the Managed Instance in the Managed Home.

3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   EnterpriseOne HTML Server

4. Click Continue.



Note: The Propagate Enterprise Server Config drop-down appears only if any enterprise server is registered within the Server Manager console. The Propagate Enterprise Server Config drop-down contains the available enterprise server instances registered with the SM console within a particular selected server group. NONE is added to the drop-down by default.

5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the dropdown to select the Server Group to which you want this instance to belong.

     Also refer to Chapter 31, "Administer Server Groups".

   - *Instance Name*

     Enter a unique name for the instance name.

     Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

     `PRODUCT_SERVER_PORT`

     where `PRODUCT` is the JD Edwards EnterpriseOne server type, such as `Enterprise_Server, HTML_Web_Server, RTE_Transaction_Server, Collaborative_Portal`, or `Business_Services`, and

     where `SERVER` is the machine on which the instance is installed, and

     where `PORT` is the HTTP port which is defined for use by this server.

   - *J2EE Server*

     Use the dropdown to select a valid J2EE server.

   - *HTTP Port*

     You must ensure that the port that you specify is available and is not being used by any other application currently installed and running on the server on which the application server is running.

     See Also:

     - Appendix A.6, "Verify HTTP Ports"
     - Appendix A.7, "HTTP Ports on UNIX Operating Systems"

   - *Software Component*

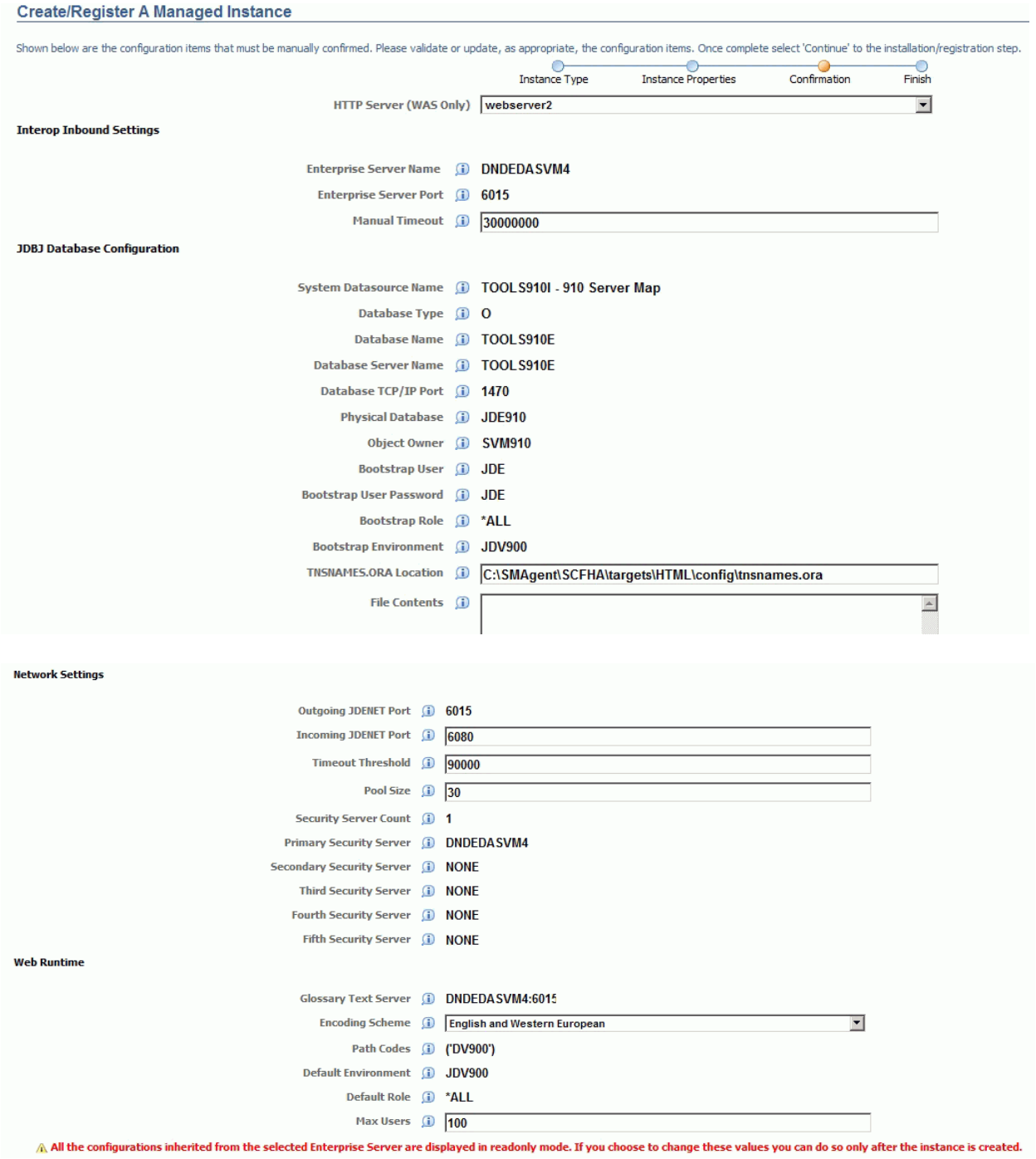
     Use the dropdown to select the version of this Software Component that you wish to install.

   - *Propagate Enterprise Server Config* (Release 9.1 Update 3.1)

     Select the enterprise server from the drop-down list to propagate the configurations.

Note: By default, the selected item is set to NONE. Selecting NONE signifies that you do not wish to propagate configurations from any available enterprise server. If any enterprise server is selected, all of the inherited values are seen in the next screen, otherwise the properties are seen with blank/default values. If propagated, the propagated values are not editable on the confirmation page, however they can be modified post installation.

6. Click Continue.



Note: This example illustrates an installation on a WebSphere Application Server by selecting an enterprise server to be propagated. If installing on WLS, the HTTP Server (WAS Only) field is not displayed.

Note: This example illustrates an installation on a WebSphere Application Server by selecting NONE under Propagate Enterprise Server Config. If installing on WLS, the HTTP Server (WAS Only) field is not displayed.

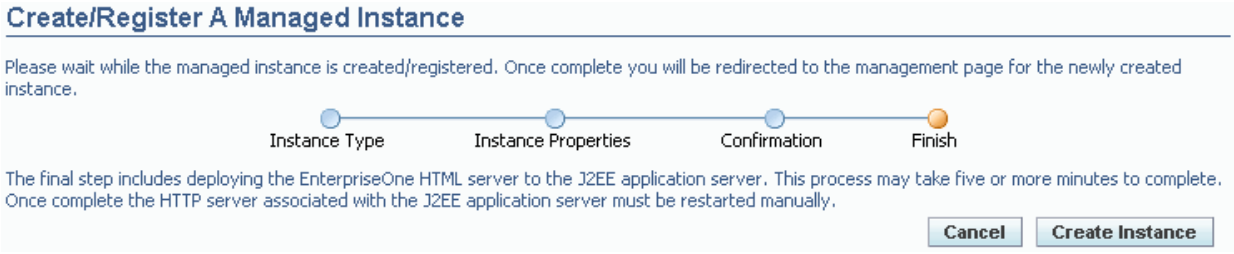
7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The page displays a variety of fields depending on your application server (WAS or WLS). The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items.

   Tip: For help, click the Information icon next to the title of a field.

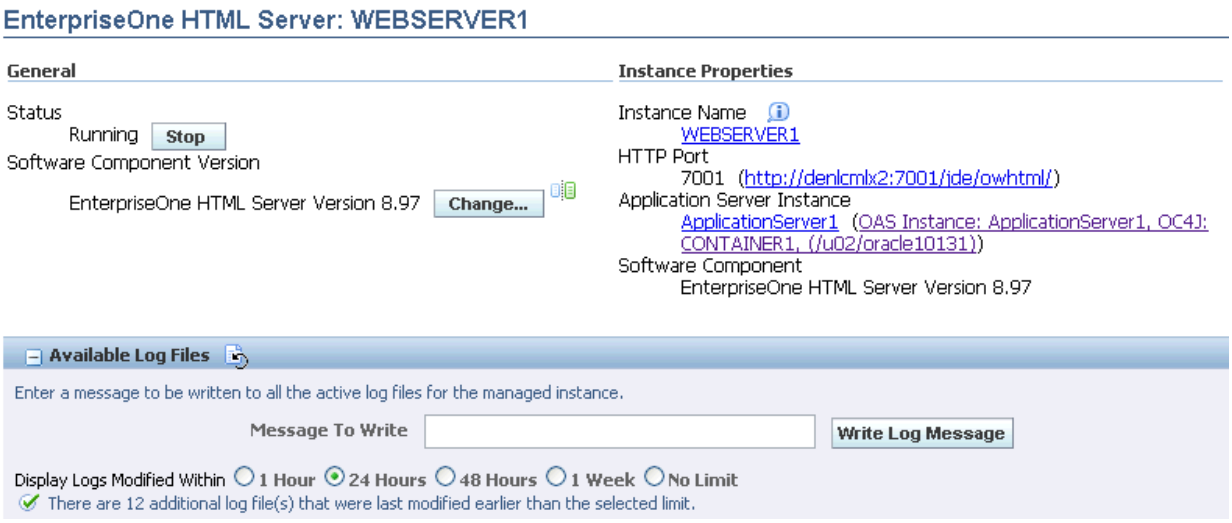
   See Also:

   - Chapter 9, "Configure the Default Server Group Configuration Settings"

8. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.



9. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the installation of the HTML Web Server.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered HTML Server. This server also appears as a Managed Instance in the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- *General*

– *Status*

Valid values are:

Running

When the status is Running, the *Stop* button is available.

Stopped

When the status is Stopped, the *Start* button is available.

See Also: Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"

– *Software Component Version*

Displays the version of this Software Component.

See Also: Section 11.4, "Change a Managed EnterpriseOne Software Component"

? *Instance Properties*

– *Instance Name*

The unique name assigned to the Managed Instance at the time it was created or registered.

– *HTTP Port*

Displays the HTTP Port for this server and also provides a link to the HTTP server.

– *Application Server Instance*

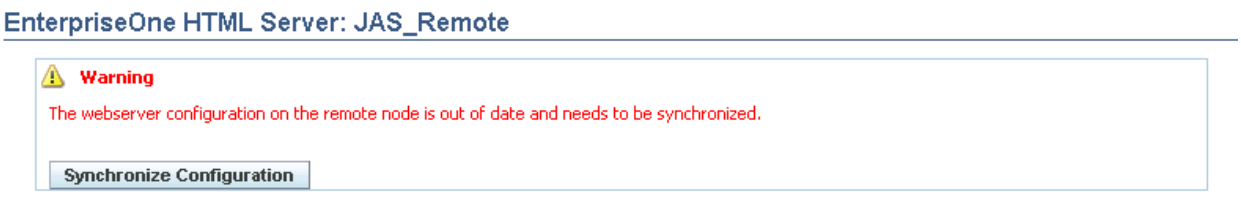
Displays the application server into which this EnterpriseOne server is installed and also provides a link to the application server instance and associated OC4J (Oracle Application Server) or profile (WebSphere Application Server).

Note: The display of some information is dependent on the status of the Managed Instances. For example, if a Managed Instance is not running, then the Software Component information cannot be displayed.

For information on log files, refer to the chapter entitled: Chapter 23, "Available Log Files".

17.2.1 Post Install for a Federated Server in Network Deployment Mode

After you have completed the creation of a JD Edwards EnterpriseOne HTML Web Server as a Managed Instance in Server Manager the Management Console displays this warning:



Do not click the *Synchronize Configuration* button yet. Follow the steps in this section.

To install a HTML Web Server HTML Web Server to a WebSphere Federated Server in Network Deployment Mode:

Note: Steps 1 and 3 below are only applicable if the J2EE server you selected to create the HTML Web Server managed instance resides on a machine different that the deployment manager. The remainder of the steps are applicable to all federated deployments. You may ignore steps 2 and 4 if the federated server you selected resides on the same machine as the deployment manager.

---

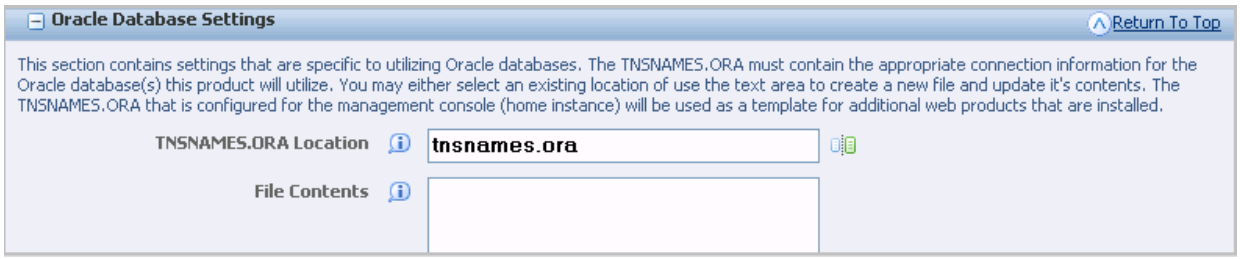
1. If you are using an Oracle database, configure the `tnsnames.ora` setting using these steps:

   a. Use this navigation path for the Managed Instance you just created in Server Manager:

   Configuration > JDBJ Database Configuration > Oracle Database Settings > TNSNAMES.ORA Location

   b. Configure the setting to `tnsnames.ora` without the full file path.

   For example:



2. If you have not already done so, install the JDBC driver to the J2EE container. Refer to Install JDBC Drivers to J2EE Servers in this guide.

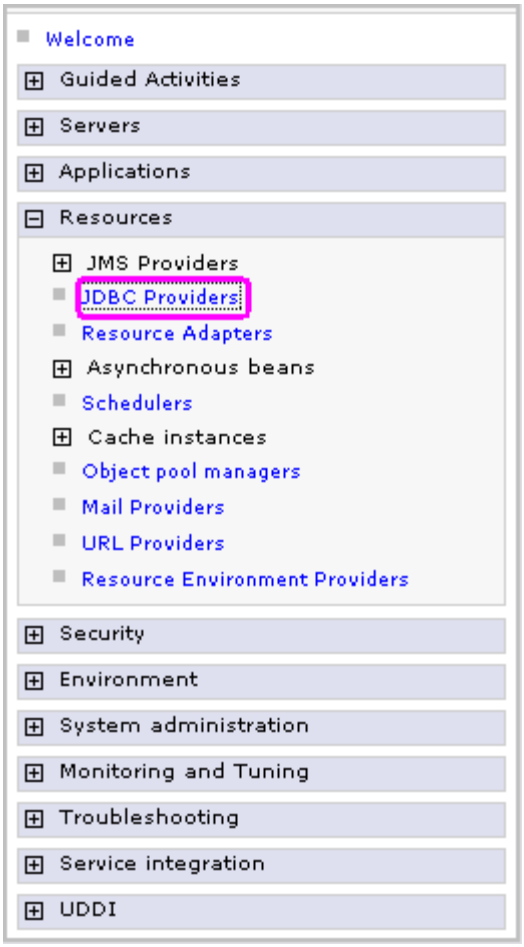
3. After installing the JDBC driver, you must modify the WebSphere JDBC provider as described in these steps:

   a. Copy the JDBC driver file(s) appropriate to your database to a location on the physical machine on which the federated server resides. For example:

   `/u01/JDBCDriver`

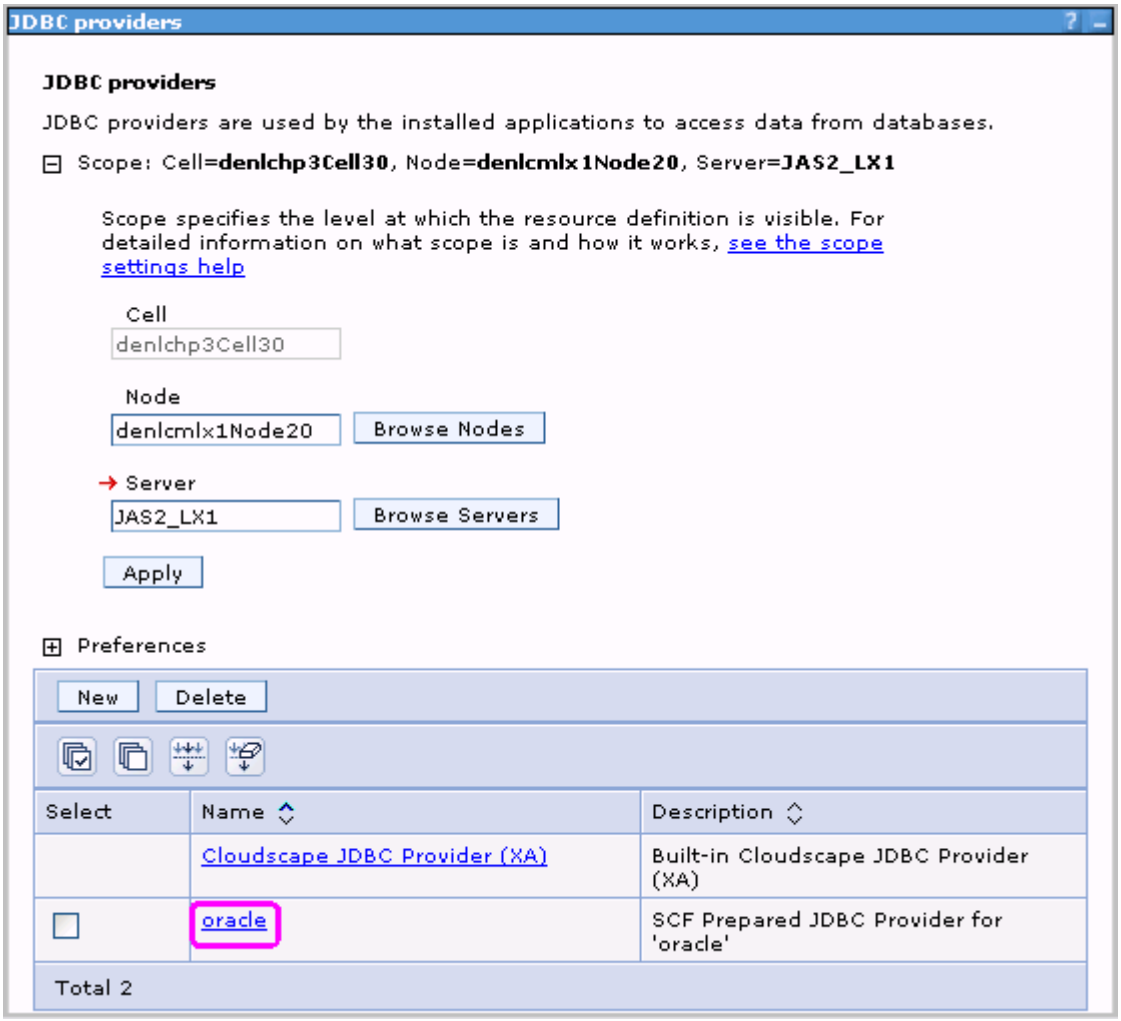
   b. Use these steps to modify the JDBC provider for the remote J2EE container in WebSphere to point to the driver file in this new location.

   i. In the WebSphere Administrative Console (for the deployment manager), navigate to the section called *JDBC Providers* as shown in this screen:



ii. Complete the filter fields with the appropriate Cell, Node and Server information for the J2EE Container to which the HTML Web Server was deployed.

For example:



iii. Click the **Apply** button.

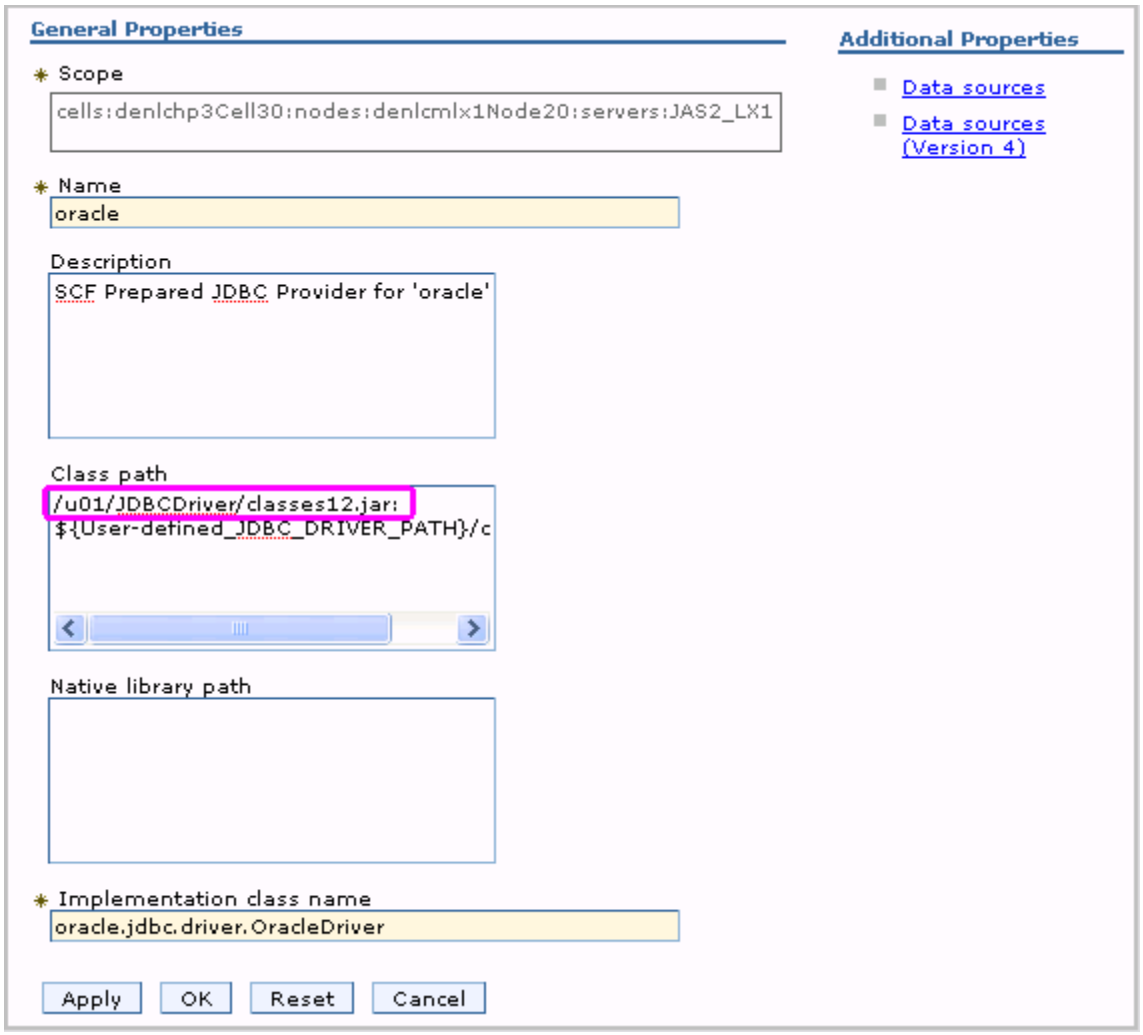
iv. On JDBC Providers, click on the appropriate JDBC provider for the database which you are using with HTML Web Server.

Note: The preceding example screen assumes an Oracle database.

---

v. Replace the path to the JDBC driver files as configured by Server Manager to the machine-specific path where you previously placed the drivers. Refer to the preceding Step 3 where you copied the JDBC driver file(s) appropriate to your database to a location on the physical machine on which the federated server resides.

This example screen assumes Oracle JDBC driver files were placed in the location `/u01/JDBCDriver`:



vi. Click the **OK** button to save the configuration change and initiate node synchronization through the deployment manager.

c. This completes the modification of the WebSphere JDBC provider.

4. Configure the HTTP Server by copying the appropriate text:

from this file:

`JDE_HOME/targets/e1_html_server_instance_name/Readme.txt`

to this file:

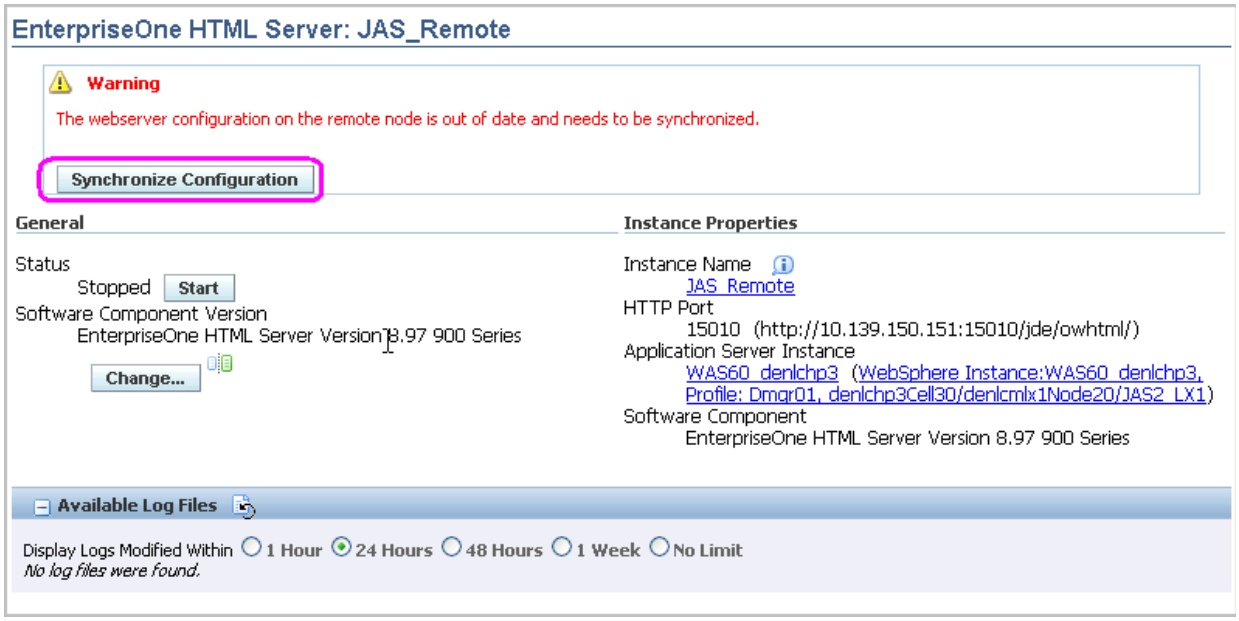
The `httpd.conf` file of the HTTP server you wish to use for this Managed Instance.

where **e1_html_server_instance_name** is the name you defined in Server Manager.

You must modify the path to the `Readme.txt` file to reflect the `JDE_HOME` location and the Managed Instance name in your environment. This is an example of a properly configured `Readme.txt` file:

```
# The following configuration was added by the EnterpriseOne Server Manager
Listen 15010
<VirtualHost *:15010>
Alias /jde
"/u01/WebSphere60/AppServer/profiles/FedProf/installedApps/denlchp3Cell30/JAS
_Remote.ear/webclient.war"
</VirtualHost>
<Directory
"/u01/WebSphere60/AppServer/profiles/FedProf/installedApps/denlchp3Cell30/JAS
_Remote.ear/webclient.war/WEB_INF">
Order Deny,Allow
Deny from All
</Directory>
<Directory
"/u01/WebSphere60/AppServer/profiles/FedProf/installedApps/denlchp3Cell30/JAS
_Remote.ear/webclient.war">
Order Deny,Allow
Allow from All
</Directory>
```

5. Make any other configuration changes required to define this Managed Instance.



6. In Server Manager, navigate to the page for the Managed Instance and click on the *Synchronize Configuration* button.

   The synchronization process may take a few minutes to complete. The JD Edwards EnterpriseOne Managed Instance is configured and ready to use after the preceding steps have been completed.

For any subsequent configuration changes made to this Managed Instance, Management Console re-displays the *Synchronize Configuration* button with the corresponding warning message. You must click the button to apply the configuration changes to the remote server. After the changes are applied, the Management Console no longer displays the button and warning message.

17.3 Create a Transaction Server as a New Managed Instance

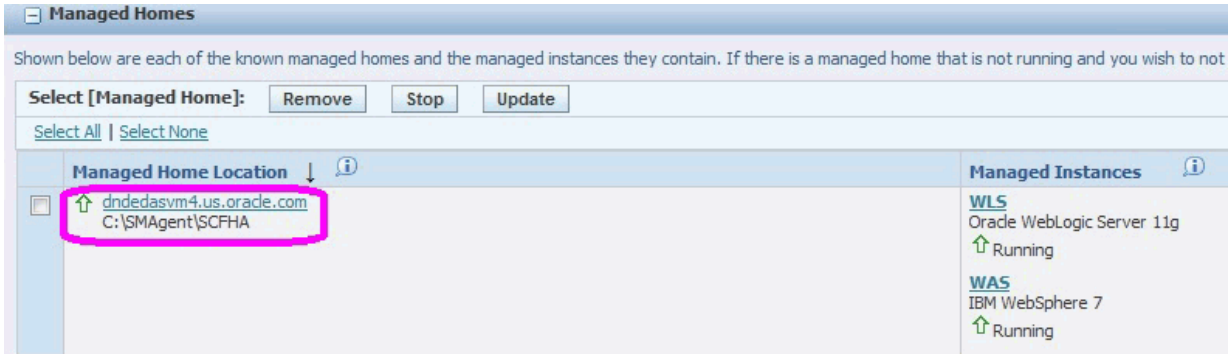
You must use Server Manager to install a new Transaction Server instance.

See Also:

- Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances
- Refer to the *JD Edwards EnterpriseOne Transaction Server Reference Guide* for details on additional tasks and topics related to Server Manager.

To install a Transaction Server instance:

1. Select the Managed Home in which you wish to install the Transaction Server.

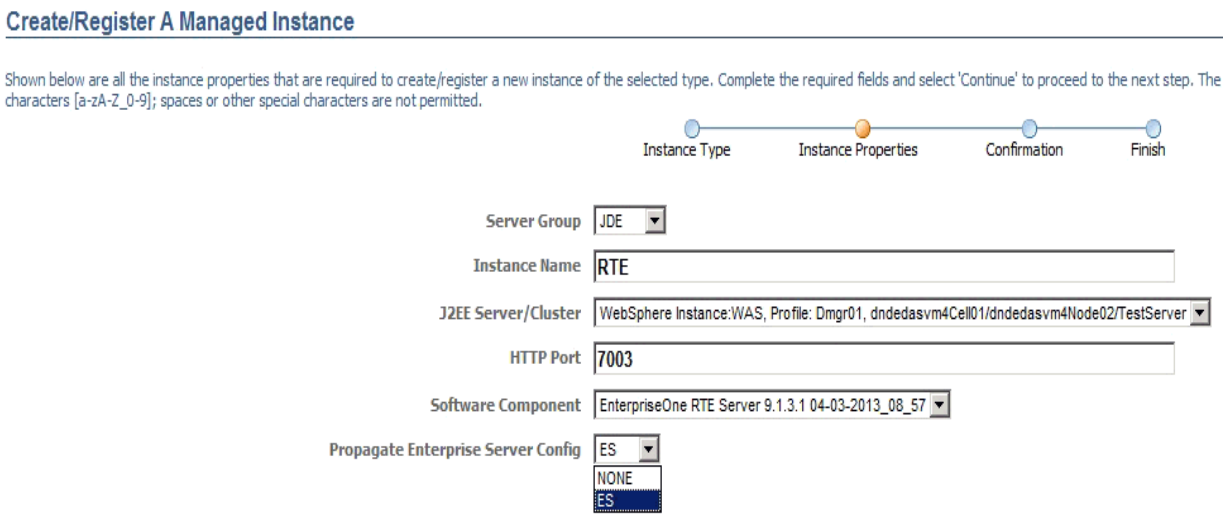


2. Click the *Create a New Managed Instance* button to create the Managed Instance in the Managed Home.

3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   EnterpriseOne Transaction Server

4. Click Continue.



Note: The Propagate Enterprise Server Config drop-down appears only if any enterprise server is registered within the Server Manager console. The Propagate Enterprise Server Config drop-down contains the available enterprise server instances registered with the SM console within a particular selected server group. NONE is added to the drop-down by default.

5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the dropdown to select the Server Group to which you want this instance to belong.

     Also refer to Chapter 31, "Administer Server Groups".

   - *Instance Name*

     Enter a unique name for the instance name.

     Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

     `PRODUCT_SERVER_PORT`

     where `PRODUCT` is the JD Edwards EnterpriseOne server type, such as `Enterprise_Server`, `HTML_Web_Server`, `RTE_Transaction_Server`, `Collaborative_Portal`, or `Business_Services`, and

     where `SERVER` is the machine on which the instance is installed, and

     where `PORT` is the HTTP port which is defined for use by this server.

   - *J2EE Server*

     Use the dropdown to select a valid J2EE server.

   - *HTTP Port*

     You must ensure that the port that you specify is available and is not being used by any other application currently installed and running on the server on which the application server is running.

     See Also:

     - Appendix A.6, "Verify HTTP Ports"
     - Appendix A.7, "HTTP Ports on UNIX Operating Systems"

   - *Software Component*

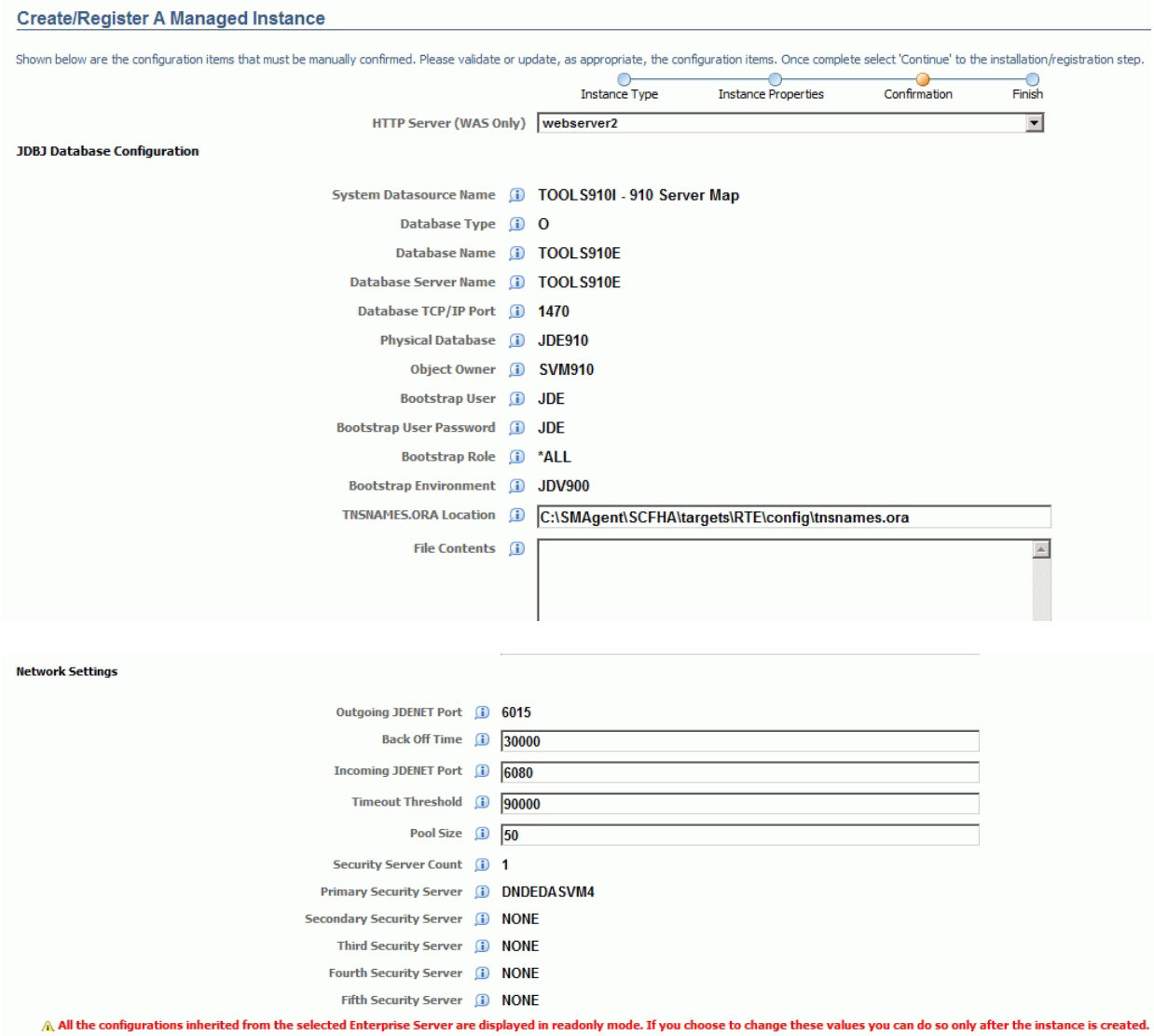
     Use the dropdown to select the version of this Software Component that you wish to install.

   - *Propagate Enterprise Server Config* (Release 9.1 Update 3.1)

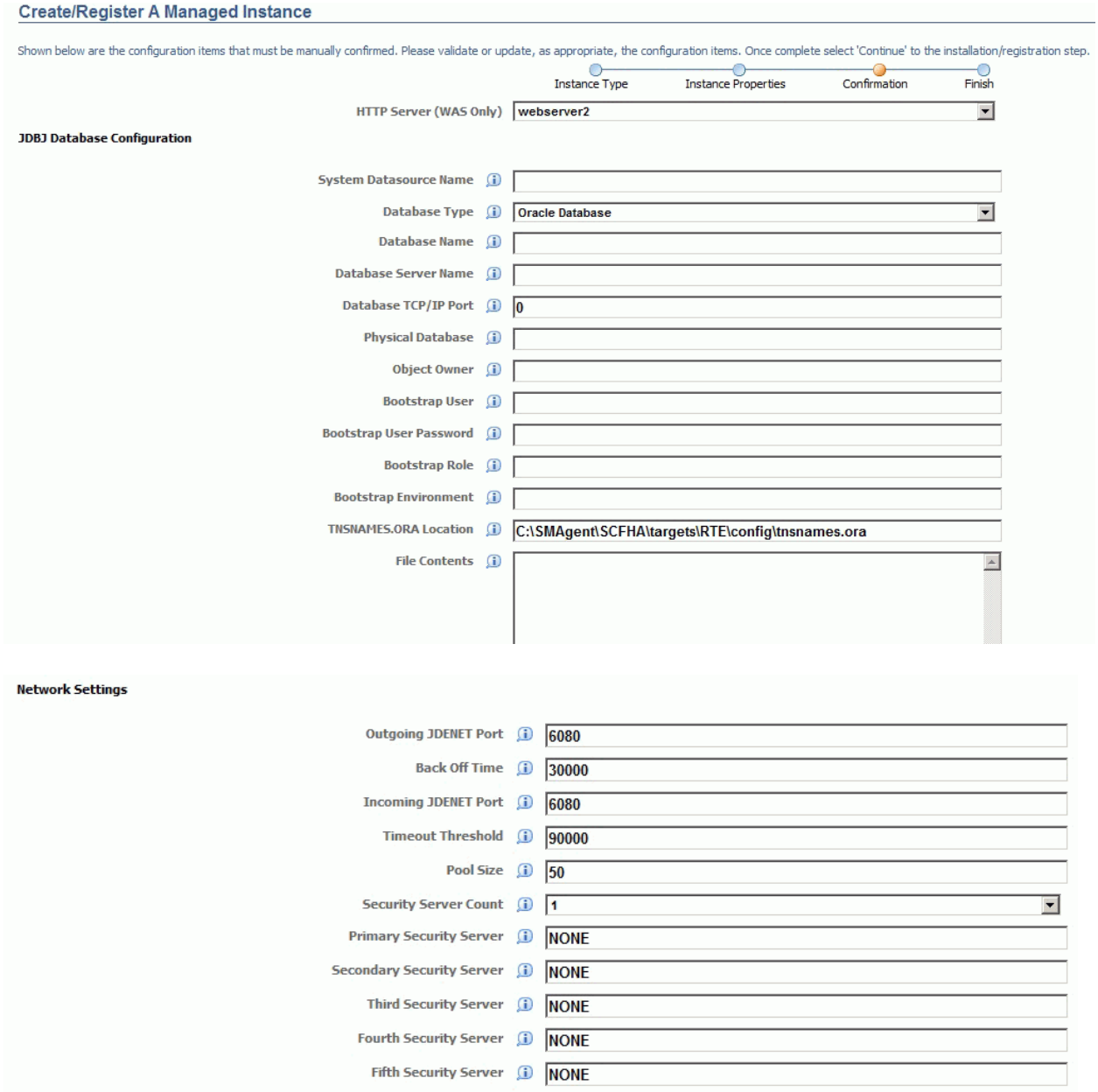
     Select the enterprise server from the drop-down list to propagate the configurations.

Note: By default, the selected item is set to NONE. Selecting NONE signifies that you do not wish to propagate configurations from any available enterprise server. If any enterprise server is selected, all of the inherited values are seen in the next scree, otherwise the properties are seen with blank/default values. If propagated, the propagated values are not editable on the confirmation page, however they can be modified post installation.

6. Click Continue.



Note: This example illustrates an installation on a WebSphere Application Server by selecting an enterprise server to be propagated. If installing on WLS, the HTTP Server (WAS Only) field is not displayed.



Note: This example illustrates an installation on a WebSphere Application Server by selecting NONE under Propagate Enterprise Server Config. If installing on WLS, the HTTP Server (WAS Only) field is not displayed.

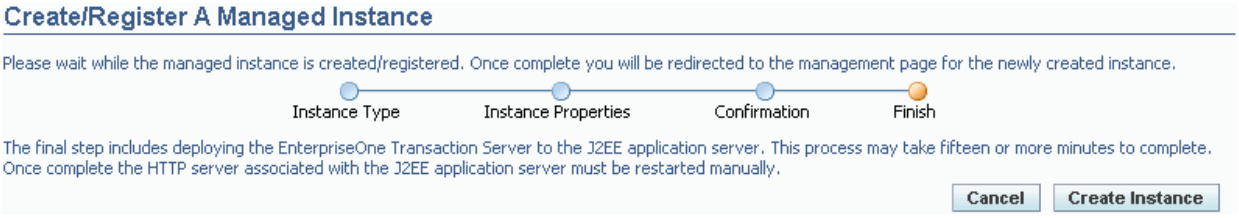
7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The page displays a variety of fields depending on your application server (WAS or WLS). The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items.

   Tip: For help, click the Information icon next to the title of a field.

   See Also:

   - Chapter 9, "Configure the Default Server Group Configuration Settings"

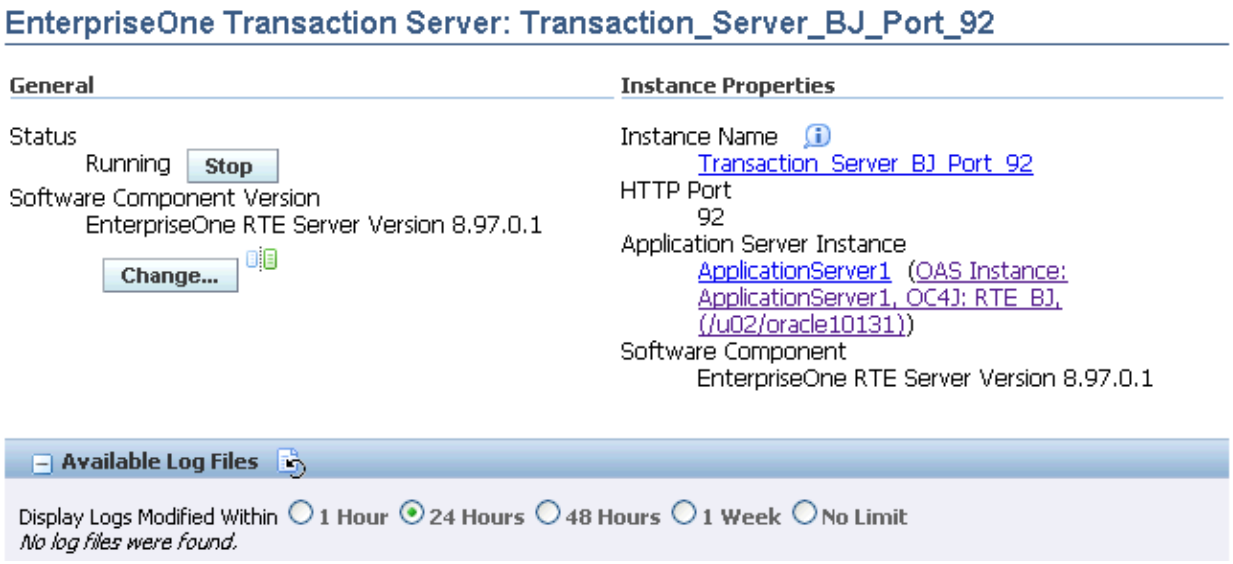
8. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.



9. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the installation of the Transaction Server.

Note: This process may take fifteen or more minutes to complete.

After you have completed the installation, the HTTP server associated with the J2EE Server (WAS) must be restarted manually. If you do not restart the HTTP server, you will not be able to login to JD Edwards EnterpriseOne.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Transaction Server. This server also appears as a Managed Instance in the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- *General*
  - *Status*

    Valid values are:

    Running

    When the status is Running, the *Stop* button is available.

    Stopped

    When the status is Stopped, the *Start* button is available.

See Also: Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"

- *Software Component Version*

  Displays the version of this Software Component.

See Also: Section 11.4, "Change a Managed EnterpriseOne Software Component"

- *Instance Properties*
  - *Instance Name*

    The unique name assigned to the Managed Instance at the time it was created or registered.
  - *HTTP Port*

    Displays the HTTP Port for this server and also provides a link to the HTTP server.
  - *Application Server Instance*

    Displays the application server into which this EnterpriseOne server is installed and also provides a link to the application server instance and associated OC4J (Oracle Application Server) or profile (WebSphere Application Server).

For information on log files, refer to the chapter entitled: Chapter 23, "Available Log Files".

17.4 Create a Collaborative Portal Server as a New Managed Instance

You must use Server Manager to install a new Collaborative Server instance.

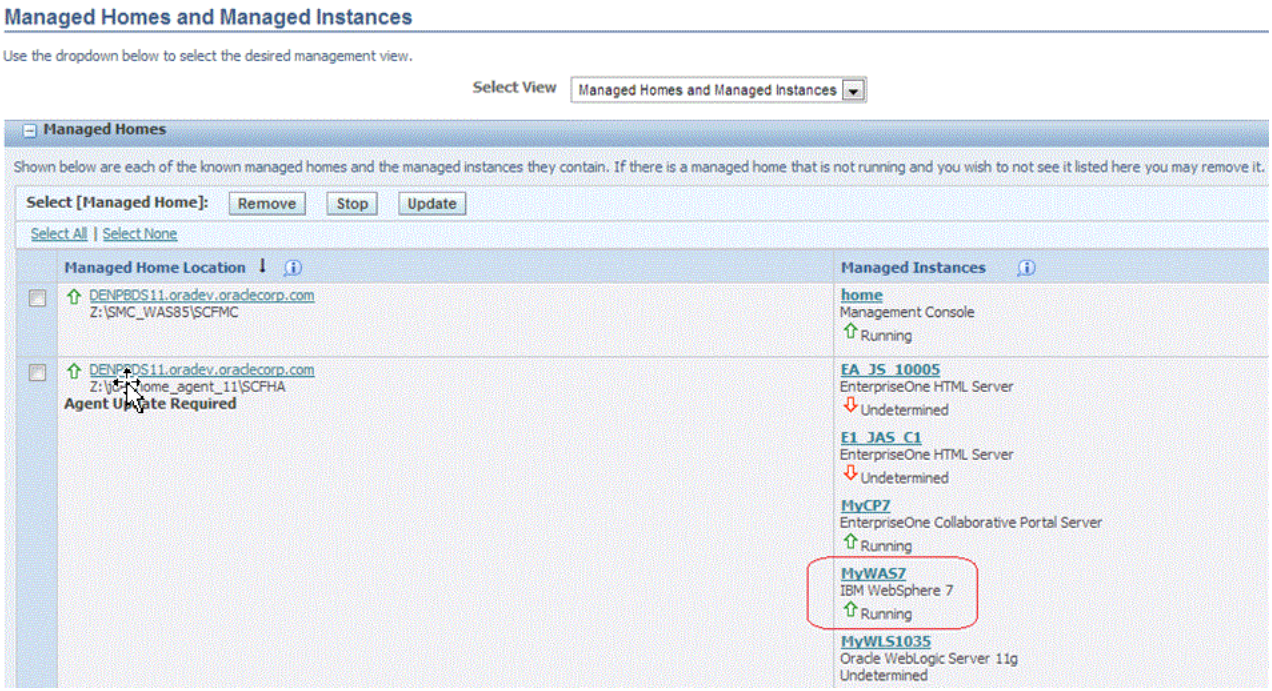
The WebSphere 7.0 or 8.5 installation must also include an HTTP Server.

See Also:

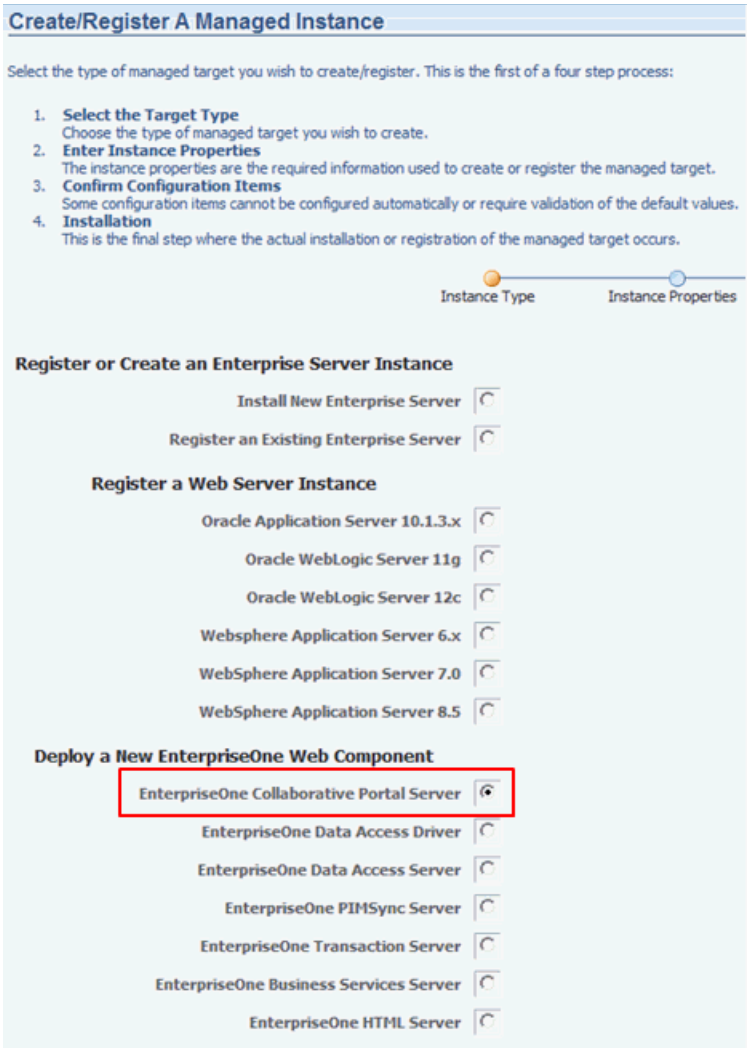
- Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances
- Refer to the *JD Edwards EnterpriseOne Collaborative Portal Server Reference Guide* for details on additional tasks and topics related to Server Manager.

To install a Collaborative Portal Server instance:

1. Select the Managed Home in which you wish to install the Collaborative Portal Server.



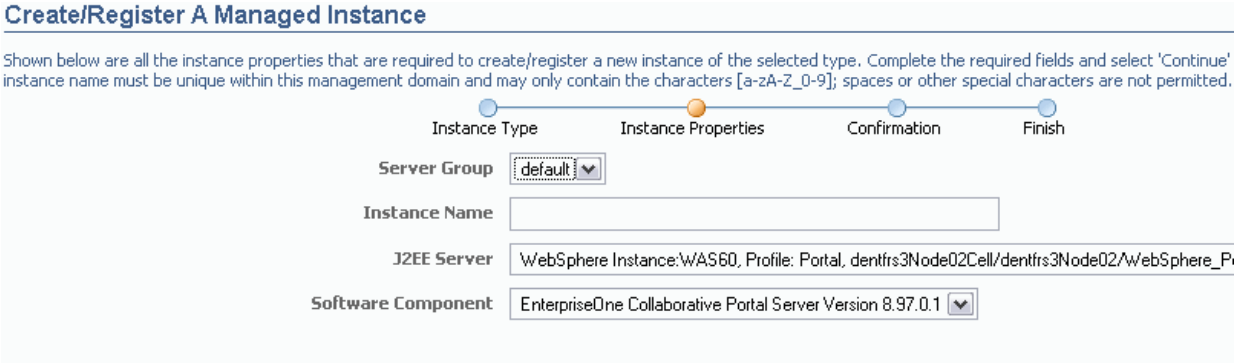
2. Click the *Create a New Managed Instance* button to create the Managed Instance in the Managed Home.



3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   EnterpriseOne Collaborative Portal Server

4. Click Continue.



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the dropdown to select the Server Group to which you want this instance to belong.

Also refer to Chapter 31, "Administer Server Groups".

- *Instance Name*

  Enter a unique name for the instance name.

  Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

  `PRODUCT_SERVER_PORT`

  where `PRODUCT` is the JD Edwards EnterpriseOne server type, such as `Enterprise_Server`, `HTML_Web_Server`, `RTE_Transaction_Server`, `Collaborative_Portal`, or `Business_Services`, and

  where `SERVER` is the machine on which the instance is installed, and

  where `PORT` is the HTTP port which is defined for use by this server.

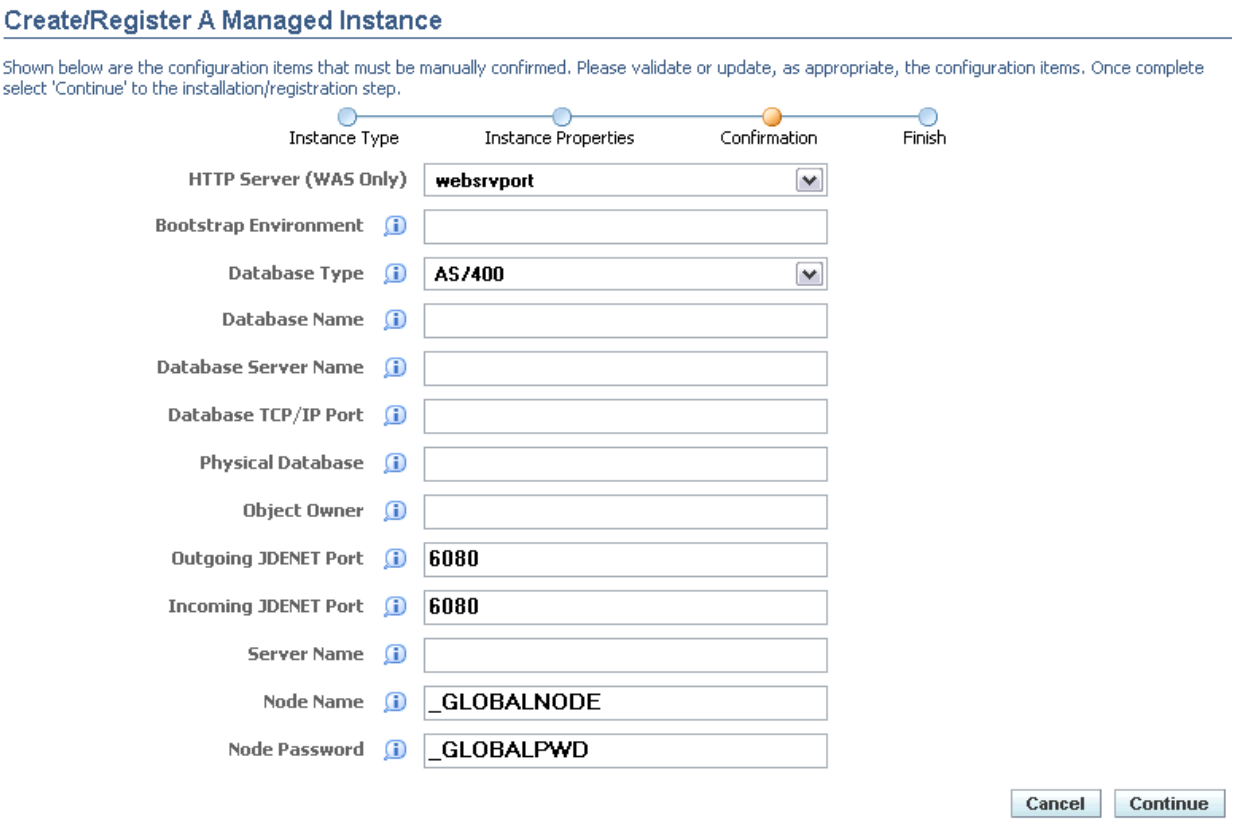
- *J2EE Server*

  Use the dropdown to select a valid J2EE server.

- *Software Component*

  Use the dropdown to select the version of this Software Component that you wish to install.

6. Click Continue.



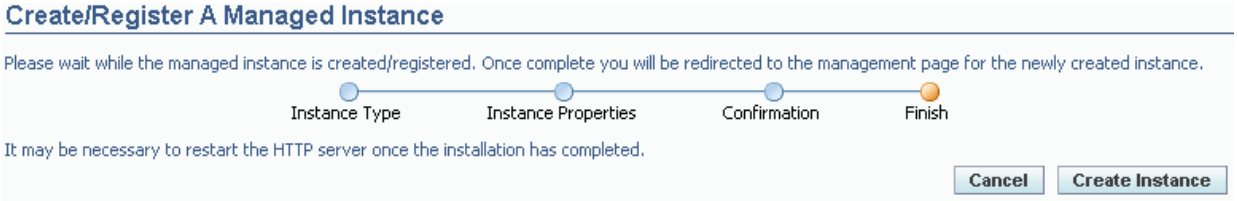
7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items.

Tip: For help, click the Information icon next to the title of a field.

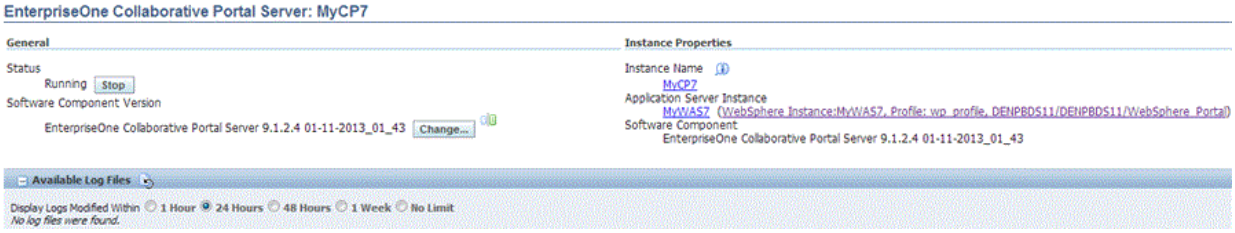
See Also:

- Chapter 9, "Configure the Default Server Group Configuration Settings"

8. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.



9. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the installation of the Collaborative Portal Server.



After you have completed the installation, the browser is redirected to the Management Console page for the newly registered Collaborative Portal. This server also appears as a Managed Instance in the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- *General*
  - *Status*

    Valid values are:

    Running

    When the status is Running, the *Stop* button is available.

    Stopped

    When the status is Stopped, the *Start* button is available.

See Also:

- Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"

  - *Software Component Version*

    Displays the version of this Software Component.

See Also:

- Section 11.4, "Change a Managed EnterpriseOne Software Component"

- *Instance Properties*
  - *Instance Name*

    The unique name assigned to the Managed Instance at the time it was created or registered.
  - *Application Server Instance*

    Displays the application server into which this EnterpriseOne server is installed and also provides a link to the application server instance and associated WebSphere Application Server profile.

For information on log files, refer to the chapter entitled: Chapter 23, "Available Log Files".

17.5 Create a Business Services Server as a New Managed Instance

Caution: This Caution is applicable only if you are creating a Business Services Server on a WebSphere application server.

Ensure that you have already installed a version of WebSphere that is compatible with the Business Services Server (refer to Section 3.1, "Accessing the Certifications (Minimum Technical Requirements)" in this guide).

In order to enable Server Manager to install a Managed Instance for a Business Services Server, you must have configured the supported version of WebSphere with a *secure profile*. For general security settings directly related to Server Manager, refer to Section 13.2.1, "Configure WebSphere Application Server to Work With Server Manager When Administrative Security is Enabled" in this guide. For recommendations for securing the WebSphere profile, refer to the *Business Service Server Reference Guide.*

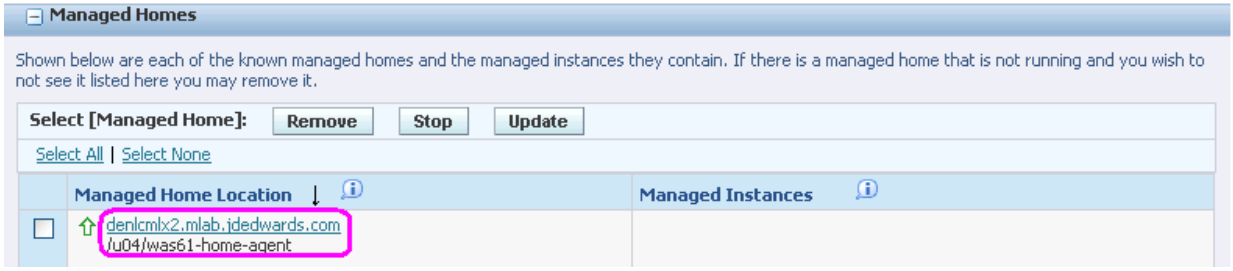
You should also ensure that the server profile associated with the J2EE Server that you created for the Business Services Server is in the Running state before installing the Business Services Server through Server Manager. If this server is not running, the installation will fail.

Note: To deploy JAX-WS business services to a business services server instance on WLS or WAS, ensure that your Server Manager Console and Agent (under which the business services server instance on WLS or WAS are registered) are at JD Edwards EnterpriseOne Tools Release 9.1 update 2 or later.

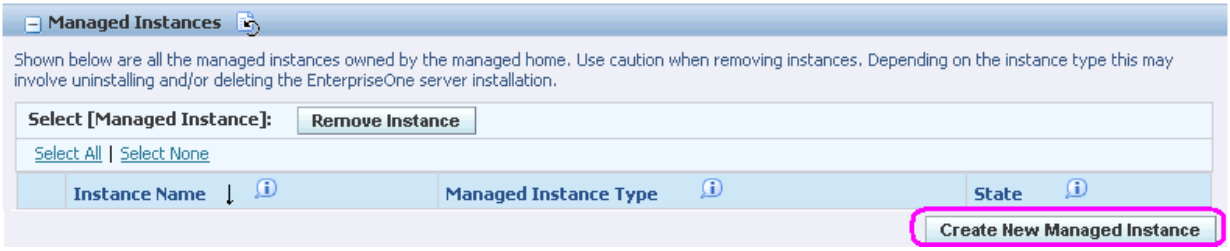
See Also

- Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances
- Refer to the *JD Edwards EnterpriseOne Business Services Server Reference Guide* for details on additional tasks and topics related to Server Manager.
- Refer to the for details on other tasks and topics extraneous to Server Manager.

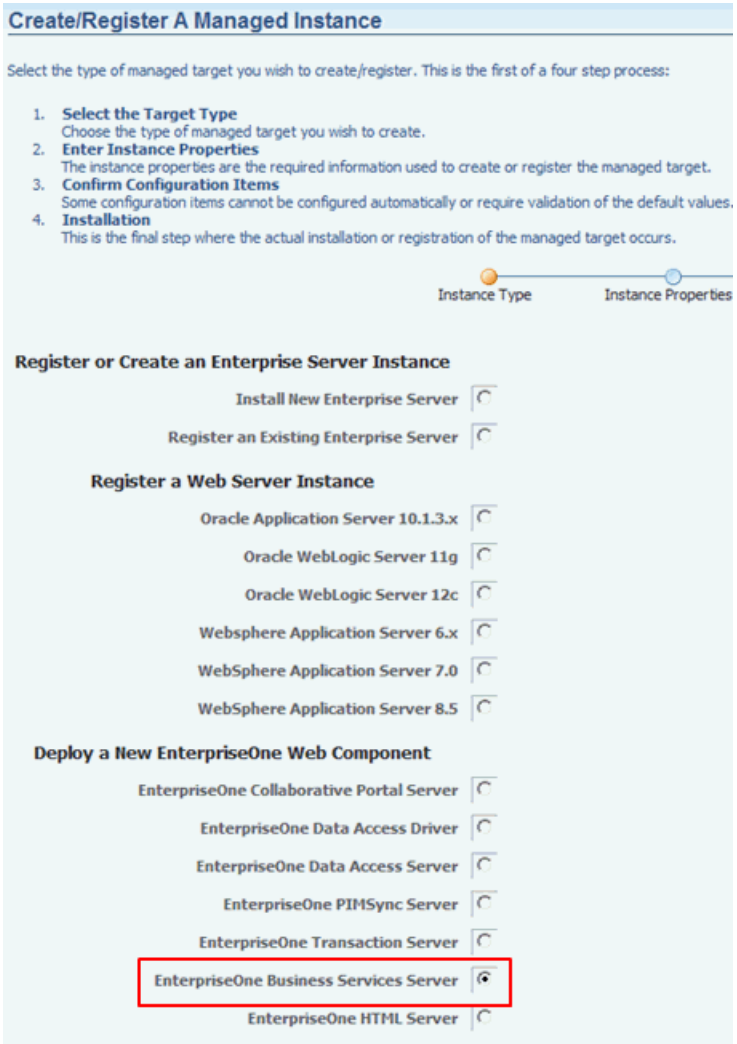
To install a Business Services Server Instance:



1. Select the Managed Home in which you wish to install the Business Services Server.

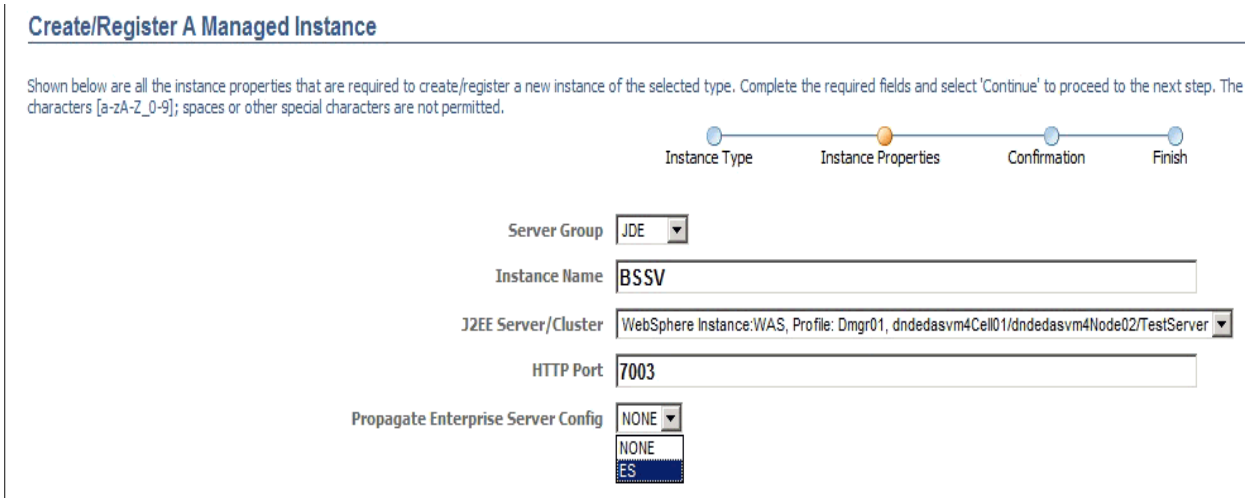


2. In the Managed Instances section of the page, click the *Create a New Managed Instance* button.



3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   EnterpriseOne Business Services Server



Note: The Propagate Enterprise Server Config drop-down appears only if any enterprise server is registered within the Server Manager console. The Propagate Enterprise Server Config drop-down contains the available enterprise server instances registered with the SM console within a particular selected server group. NONE is added to the drop-down by default.

4. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the dropdown to select the Server Group to which you want this instance to belong.

     Also refer to Chapter 31, "Administer Server Groups".

   - *Instance Name*

     Enter a unique name for the instance name.

     Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

     `PRODUCT_SERVER_PORT`

     where `PRODUCT` is the JD Edwards EnterpriseOne server type, such as `Enterprise_Server`, `HTML_Web_Server`, `RTE_Transaction_Server`, `Collaborative_Portal`, or `Business_Services`, and

     where `SERVER` is the machine on which the instance is installed, and

     where `PORT` is the HTTP port which is defined for use by this server.

   - *J2EE Server*

     Use the dropdown to select a valid J2EE server.

     Ensure the J2EE Server that you choose is a secure WebSphere 7.0 or 8.5 profile (releases prior to 7.0 are not supported). Otherwise, Server Manager will not allow you to continue the installation.

- *HTTP Port*

  You must ensure that the port that you specify is available and is not being used by any other application currently installed and running on the server on which the application server is running.

  See Also:

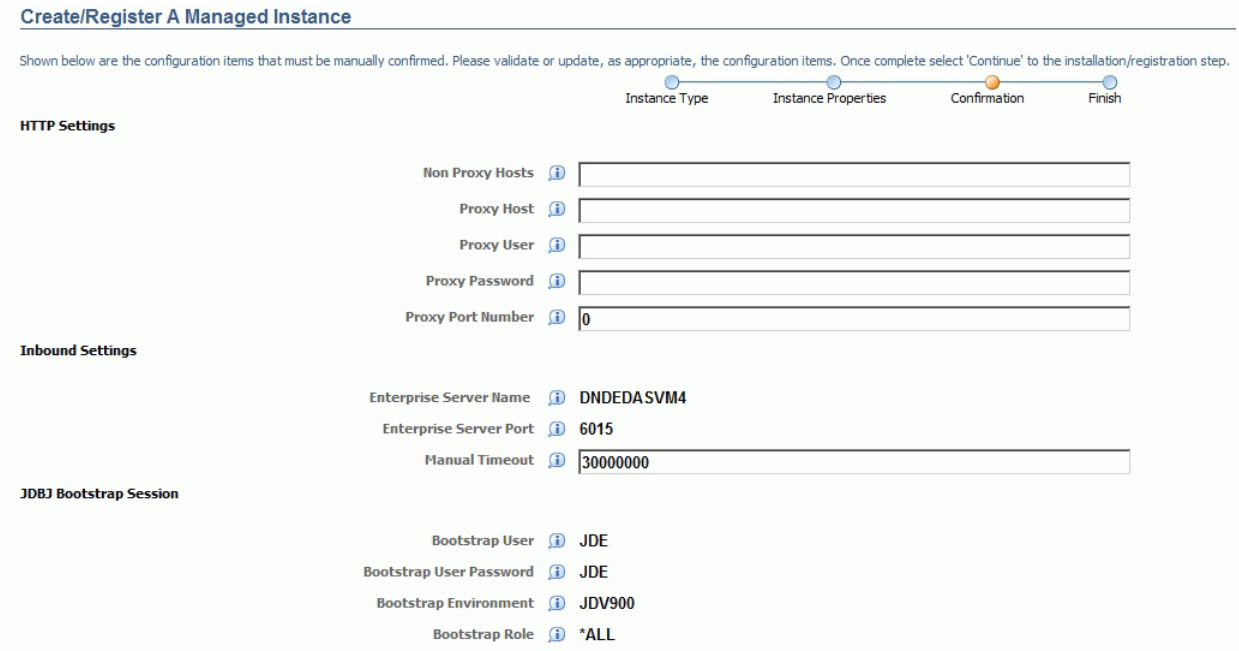
  - Appendix A.6, "Verify HTTP Ports"
  - Appendix A.7, "HTTP Ports on UNIX Operating Systems"

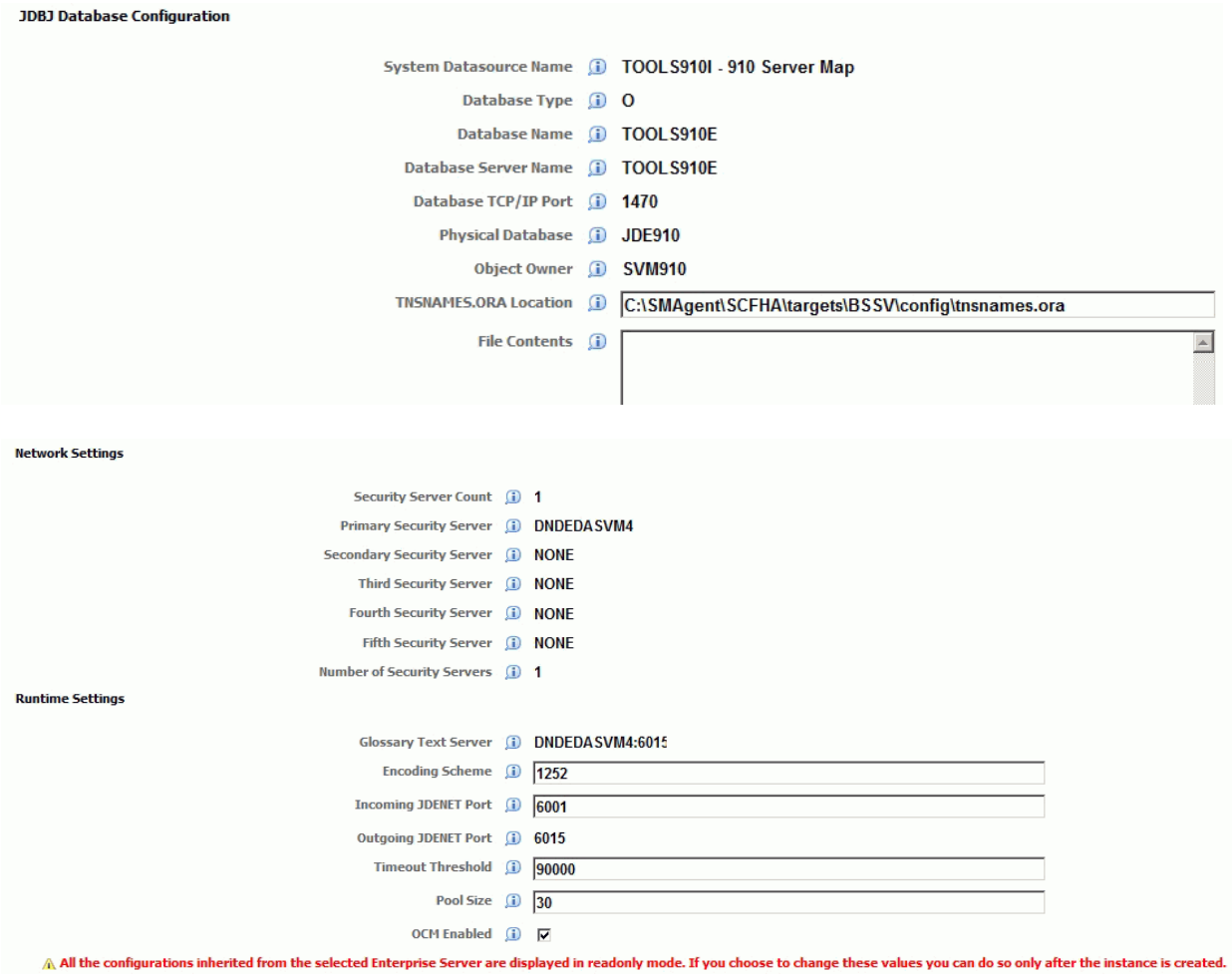
- *Propagate Enterprise Server Config* (Release 9.1 Update 3.1)

  Select the enterprise server from the drop-down list to propagate the configurations.

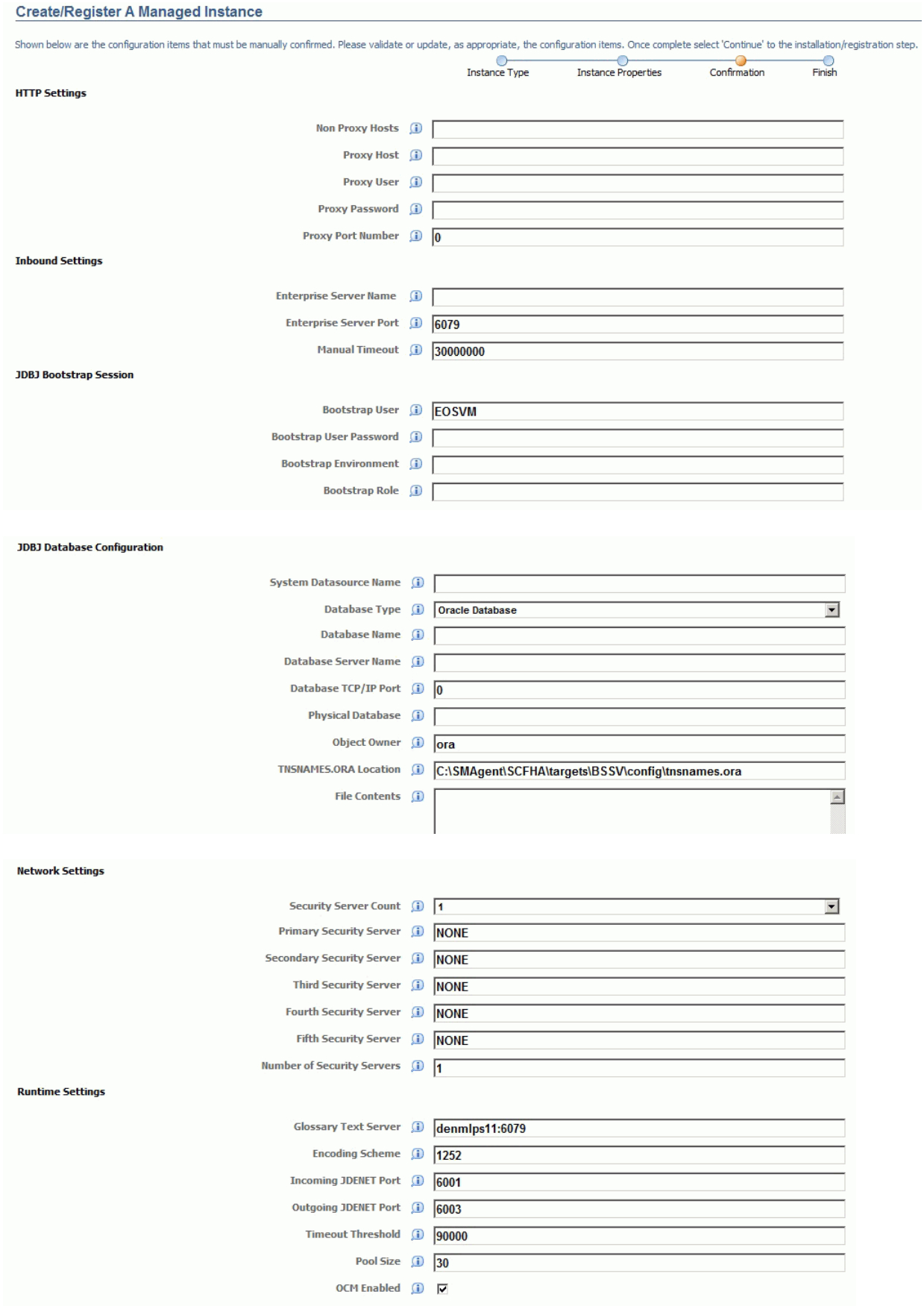
  Note: By default, the selected item is set to NONE. Selecting NONE signifies that you do not wish to propagate configurations from any available enterprise server. If any enterprise server is selected, all the inherited values are seen in the next screen, otherwise the properties are seen with blank/default values. If propagated, the propagated values are not editable on the confirmation page, however, they can be modified post installation.

5. Click Continue.





Note: This example illustrates an installation by selecting an enterprise server to be propagated.


Create/Register A Managed Instance
Shown below are the configuration items that must be manually confirmed. Please validate or update, as appropriate, the configuration items. Once complete select 'Continue' to the installation/registration step.
Instance Type
Instance Properties
Confirmation
Finish
HTTP Settings
Non Proxy Hosts
Proxy Host
Proxy User
Proxy Password
Proxy Port Number
0
Inbound Settings
Enterprise Server Name
Enterprise Server Port
6079
Manual Timeout
30000000
JDBJ Bootstrap Session
Bootstrap User
EOSVM
Bootstrap User Password
Bootstrap Environment
Bootstrap Role
JDBJ Database Configuration
System Datasource Name
Database Type
Oracle Database
Database Name
Database Server Name
Database TCP/IP Port
0
Physical Database
Object Owner
ora
TNSNAMES.ORA Location
C:\SMAgent\SCFHA\targets\BSSV\config\tnsnames.ora
File Contents
Network Settings
Security Server Count
1
Primary Security Server
NONE
Secondary Security Server
NONE
Third Security Server
NONE
Fourth Security Server
NONE
Fifth Security Server
NONE
Number of Security Servers
1
Runtime Settings
Glossary Text Server
denmlps11:6079
Encoding Scheme
1252
Incoming JDENET Port
6001
Outgoing JDENET Port
6003
Timeout Threshold
90000
Pool Size
30
OCM Enabled

Note: This example illustrates an installation by selecting NONE under Propagate Enterprise Server Config.

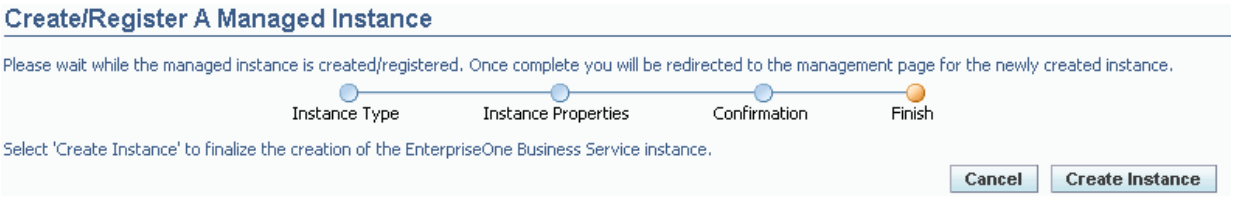
6. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The values on this form must be confirmed manually. You must validate or update, as appropriate, all configuration items.

   Tip: For help, click the Information icon next to the title of a field.

   See Also:

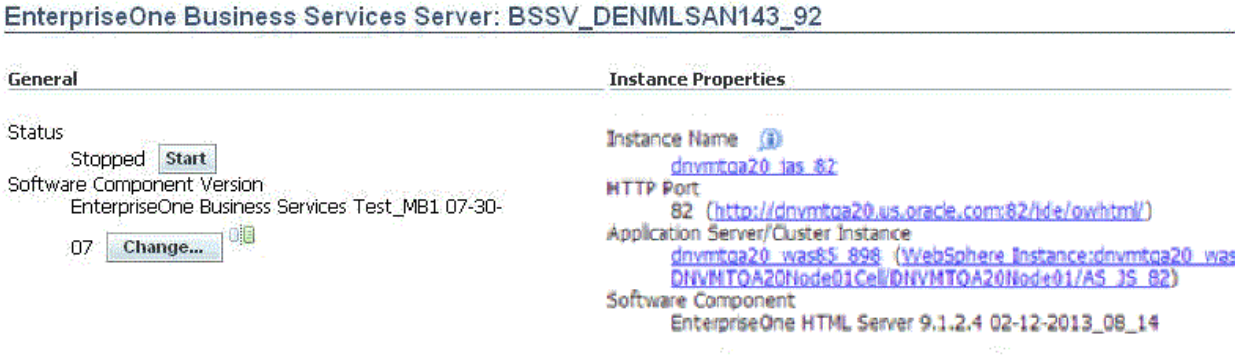
   - Chapter 9, "Configure the Default Server Group Configuration Settings"

7. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.



8. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the installation of the Business Services Server.

   After you have completed the installation, the browser is redirected to the Management Console page for the newly created Managed Instance. This Managed Instance also appears as a Managed Instance in the corresponding Managed Home.



Note: After you have created the EnterpriseOne Business Services Server Managed Instance, unlike all other web-based server products it does not start automatically. This is because the Managed Instance is not functional until the Business Services components are installed in it through the special JD Edwards EnterpriseOne package build process designed for that product. Refer to the *JD Edwards EnterpriseOne Tools Release 8.98 Package Management Guide*.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- *General*
  - *Status*

    Valid values are:

    Running

    When the status is Running, the *Stop* button is available.

    Stopped

    When the status is Stopped, the *Start* button is available.

    See Also: Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"

  - *Software Component Version*

    Displays the version of this Software Component.
- *Instance Properties*
  - *Instance Name*

    The unique name assigned to the Managed Instance at the time it was created or registered.
  - *HTTP Port*

    Displays the HTTP Port for this server and also provides a link to the HTTP server.
  - *Application Server Instance*

    Displays the application server into which this EnterpriseOne server is installed and also provides a link to the application server instance and associated WebSphere Application Server profile.

For information on log files for Managed Instances, refer to the chapter entitled: Chapter 23, "Available Log Files".

17.5.1 Configuring a Clustered Business Services Server Instance for Consumer Business Services (Release 9.1 Update 5)

Note: If you do not configure a clustered business services server instance, then clustering for consumer business services cannot be attained and only one business services server will run all consumer business services requests.

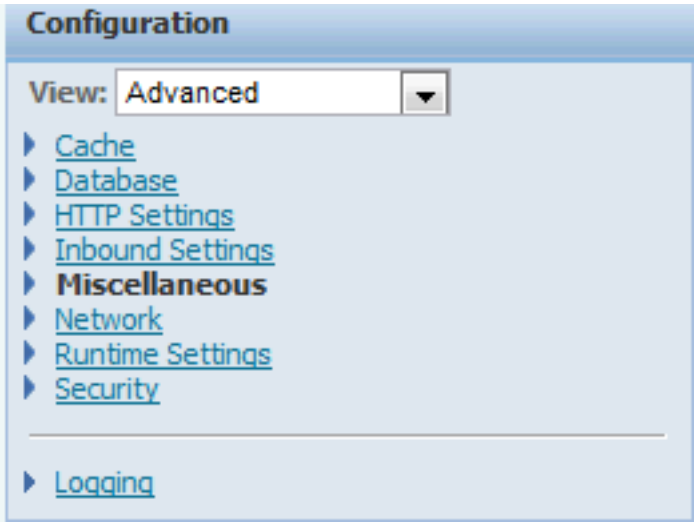
This configuration is not applicable if you are using a standalone business services server instance.

You can configure a clustered business services server instance to support clustering for consumer business services. This clustering feature enables scalability, load balancing, and high availability for consumer business services by providing multiple incoming ports so that multiple servers in the cluster can open socket connection to different ports to receive incoming JDENet messages from the Enterprise Server, and the Enterprise Server can send JDENet messages to multiple clustered business services server ports.

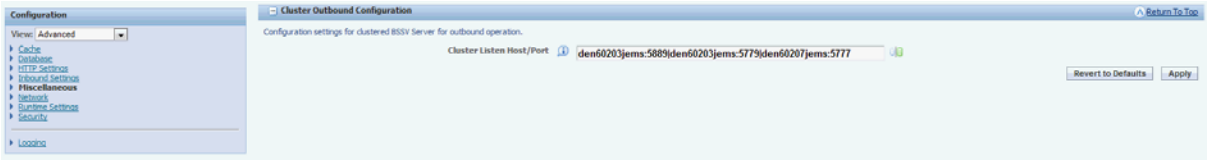
After you create and register a managed instance of a business services server, you can configure the business services server instance to support clustering for consumer business services.

To create a cluster for consumer business services:

1. Open the Server Manager console.
2. In the Managed Homes pane, click the EnterpriseOne Business Services Server instance.
3. In the left-hand side Configuration pane, select Advanced from the View drop-down list, and then click the Miscellaneous link.



4. In the Miscellaneous pane, expand the cluster Outbound Configuration item.
5. In the Cluster Listen Host/Port field, enter cluster servers with assigned ports.



Specify multiple servers in the cluster with assigned JDENet listen ports for each server in host1:port1|host2:port2|host3:port3 format. Host can be specified with machine name or fully qualified machine name and IP address.

17.6 Create an Application Interface Services (AIS) Server as a New Managed Instance (Release 9.1 Update 4.2)

You must use Server Manager to install a new Application Interface Services instance.

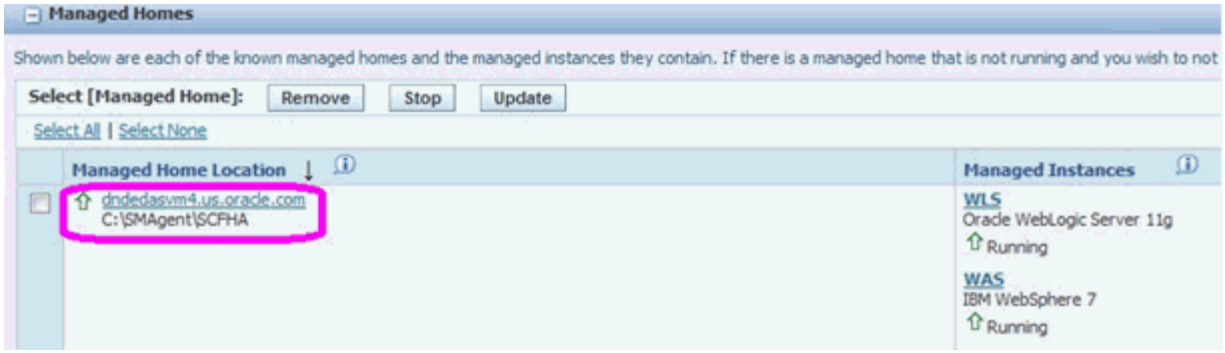
See Also:

- Section 17.1, "Prerequisites and Recommended Installation Sequence for Managed Instances for Web-Based Server Instances"
- JD Edwards EnterpriseOne Application Interface Services Server for Mobile Enterprise Applications Configuration Guide
- Refer to the JD Edwards EnterpriseOne Transaction Server Reference Guide for details on additional tasks and topics related to Server Manager.

To install an Application Interface Services Server instance:

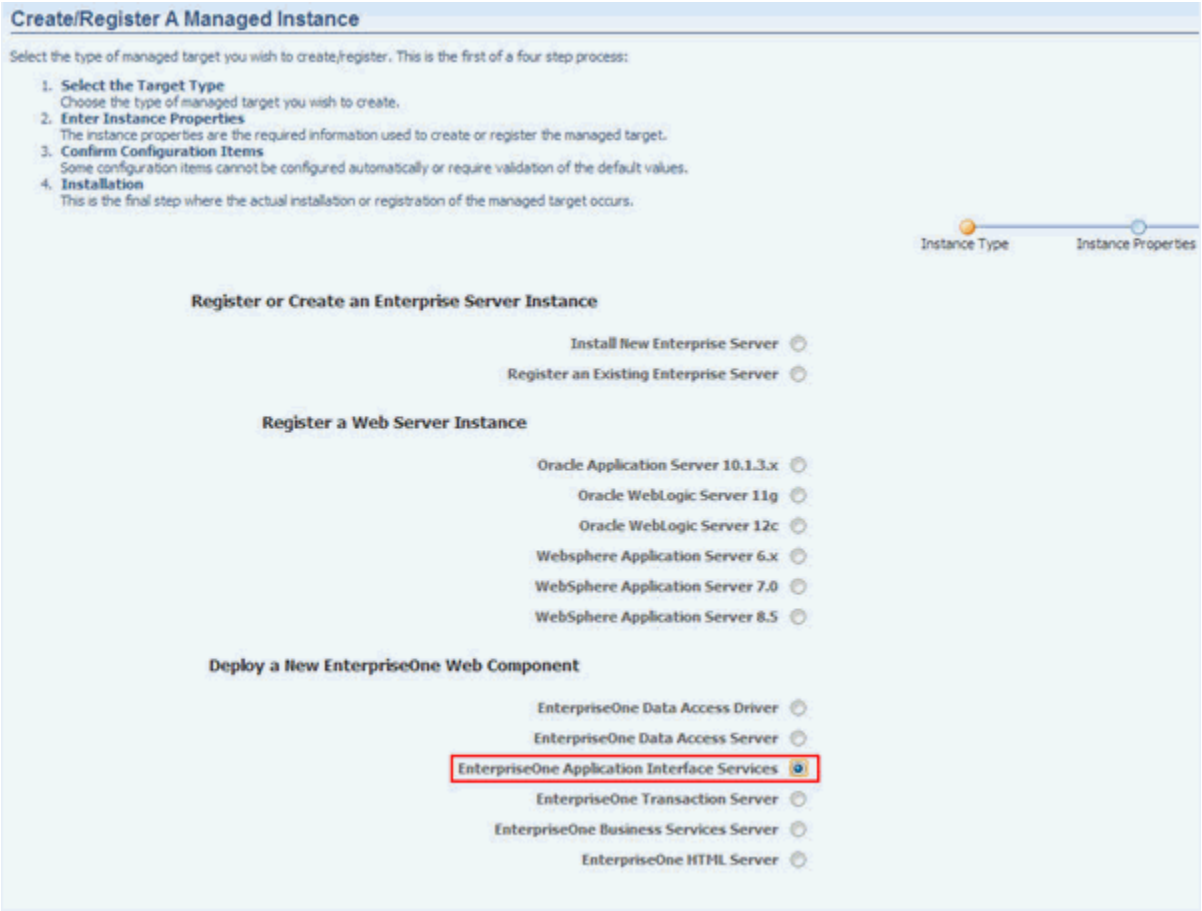
1. Select the Managed Home in which you wish to install the AIS Server.

Figure 17–1 AIS Managed Home Location



2. Click the Create a New Managed Instance button to create the Managed Instance in the Managed Home.

Figure 17–2 AIS Selection

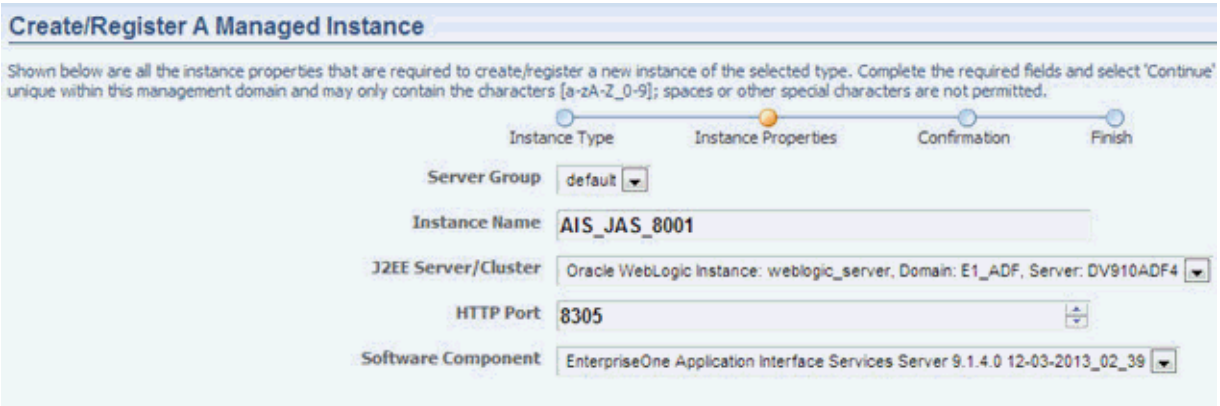


3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   EnterpriseOne Application Interface Services

4. Click Continue.

Figure 17–3 AIS Create Input Fields



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

Use the dropdown menu to select the Server Group where you want this instance to belong.

Also refer to Section 31, "Administer Server Groups"

- *Instance Name*

  Enter a unique name for the instance name.

  Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

  `PRODUCT_SERVER_PORT`

  where `PRODUCT` is the JD Edwards EnterpriseOne server type, such as JAS, RTE, CollabPortal, AIS, or BusSvcs;

  where `SERVER` is the machine on which the instance is installed;

  where `PORT` is the HTTP port which is defined for use by this server.

- *J2EE Server*

  Use the dropdown to select a valid J2EE server.

- *HTTP Port*

  You must ensure that the port that you specify is available and is not being used by any other application currently installed and running on the server on which the application server is running.

  See Also:

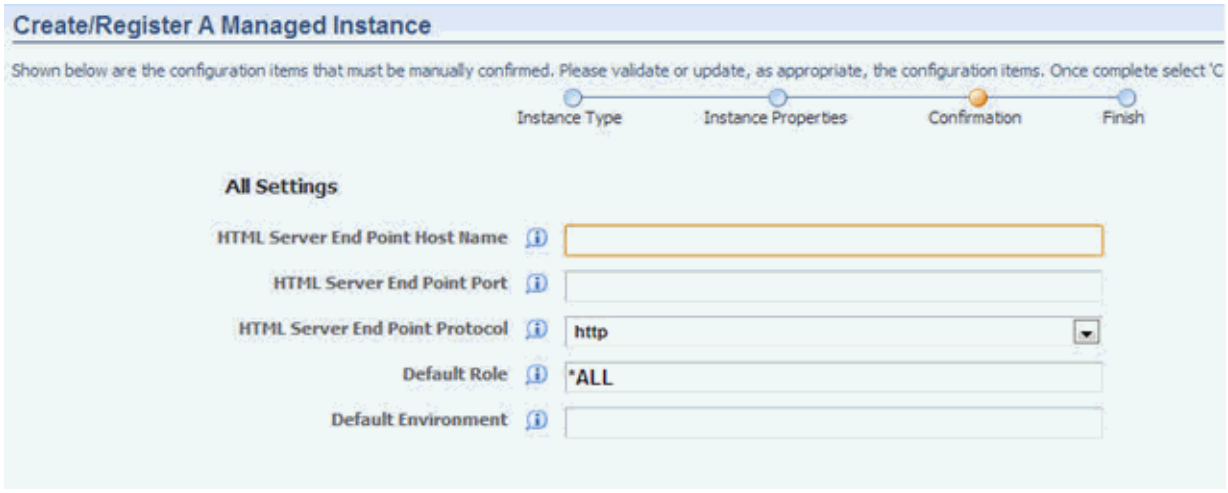
  - Section A.6, "Verify HTTP Ports"
  - Section A.7, "HTTP Ports on UNIX Operating Systems"

- *Software Component*

  Use the dropdown to select the version of this Software Component that you wish to install.

6. Click Continue.

Figure 17–4



7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The page displays the settings that are typically required to successfully start your instance. The values on this form must be confirmed manually. You should validate or update, as appropriate, all configuration items.

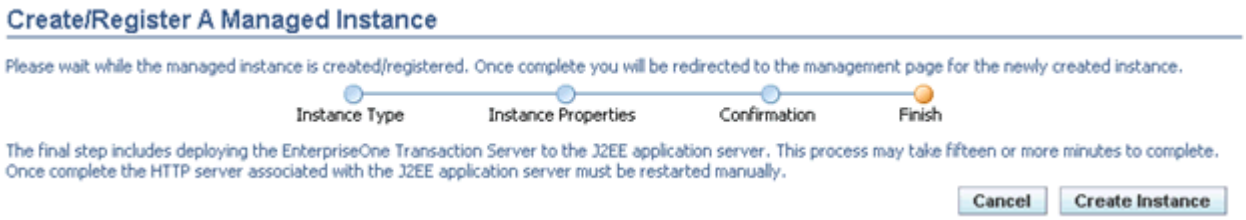
   Note: When setting up an AIS server instance, you should also review the **Allowed Hosts** setting for the corresponding EnterpriseOne HTML server instance.

   Tip: For help, click the Information icon next to the title of a field.

   See Also: Section 9, "Configure the Default Server Group Configuration Settings"

8. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.

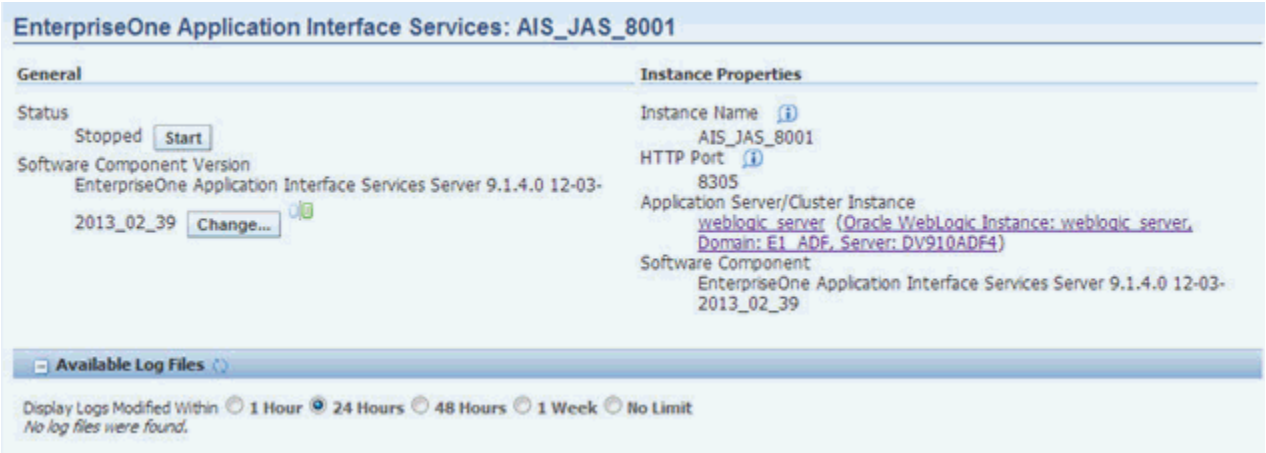
Figure 17–5



9. On Create/Register a Managed Instance, Finish, click the Create Instance button to complete the installation of the AIS Server.

After you have completed the installation, if you are running on WebSphere, the HTTP server associated with the J2EE Server must be restarted manually. If you do not restart the HTTP server, you will not be able to login to the AIS instance.

Figure 17–6 AIS EnterpriseOne Application Interface



To verify the installation is successful (Release 9.1 Update5):

1. Navigate to the AIS Server instance.

2. Click on the Test connection link.

   Note: The Test connection link is only enabled when the server is running.

3. Review the DefaultConfig file.

   >Tutorial: `Click here to view recordings on monitoring the AIS Server.`

After you have completed the installation, the browser is redirected to the Management Console page for the newly registered AIS Server. This server also appears as a Managed Instance in the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- ***General***
  - *Status*

    Valid values are:

    Running

    When the status is Running, the Stop button is available.

    Stopped

    When the status is Stopped, the Start button is available.

    See Also: Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"

  - *Software Component Version*

    Displays the version of this Software Component.

    See Also: Section 11.4, "Change a Managed EnterpriseOne Software Component"

- ***Instance Properties***
  - *Instance Name*

    The unique name assigned to the Managed Instance at the time it was created or registered.

  - *HTTP Port*

    Displays the HTTP Port for this server and also provides a link to the HTTP server.

  - *Application Server Instance*

    Displays the application server into which this EnterpriseOne server is installed and also provides a link to the application server instance and associated managed server (Oracle WebLogic Server) or profile (WebSphere Application Server).

For information on log files, refer to the chapter entitled: Section 23, "Available Log Files"

18

Install a JD Edwards EnterpriseOne Data Access Driver

It is important to note that the Data Access Driver differs from the existing Data Access Server. In addition to implementation differences, the Data Access Driver utilizes a different, more efficient, read-only JDBC driver to access the database.

> **Tip:** For integration with BI Publisher, the recommended configuration is the Data Access Driver.

For implementation details, refer to the *JD Edwards Interoperability Guide* on the Oracle Technology Network:

http://www.oracle.com/technology/documentation/index.html

This chapter discusses:

- Section 18.1, "Prerequisites and Recommendation Installation Sequence for the Data Access Driver"
- Section 18.2, "Create a Data Access Driver"

18.1 Prerequisites and Recommendation Installation Sequence for the Data Access Driver

This list shows the prerequisites and recommended installation sequence for the JD Edwards EnterpriseOne Data Access Driver:

1. *Prerequisite:* Management Agent is installed on target machine.

   Refer to Install a Management Agent.

2. *Prerequisite:* The Data Access Driver Software Component is uploaded to the Management Console.

   Refer to Upload Software Components.

3. *Prerequisite:* The Data Access Driver Software Component is distributed to the target Managed Home.

   Refer to Distribute or Delete Managed EnterpriseOne Software Components.

4. *Prerequisite:* Create a Data Access Driver.

   Refer to Create a Data Access Driver.

See Also:

- Refer to the *JD Edwards EnterpriseOne Interoperability Guide* in the chapter *Using Java Database Connectivity* for additional tasks and topics related to the Data Access Driver.
- *JD Edwards EnterpriseOne BI Publisher for JD Edwards EnterpriseOne Guide*

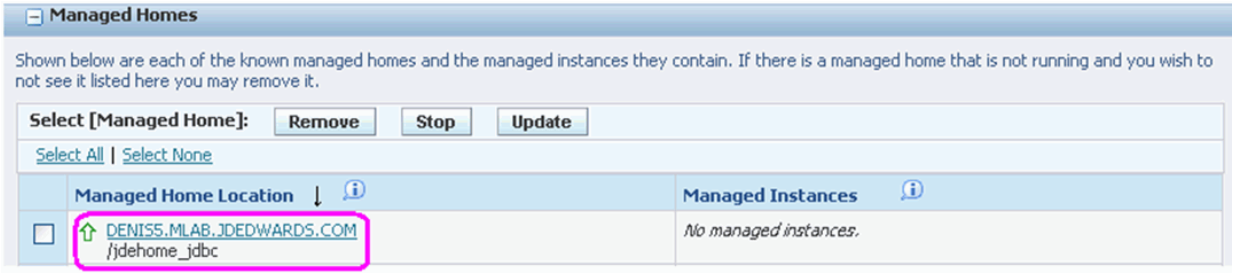
18.2 Create a Data Access Driver

You must use Server Manager to create a Data Access Driver.

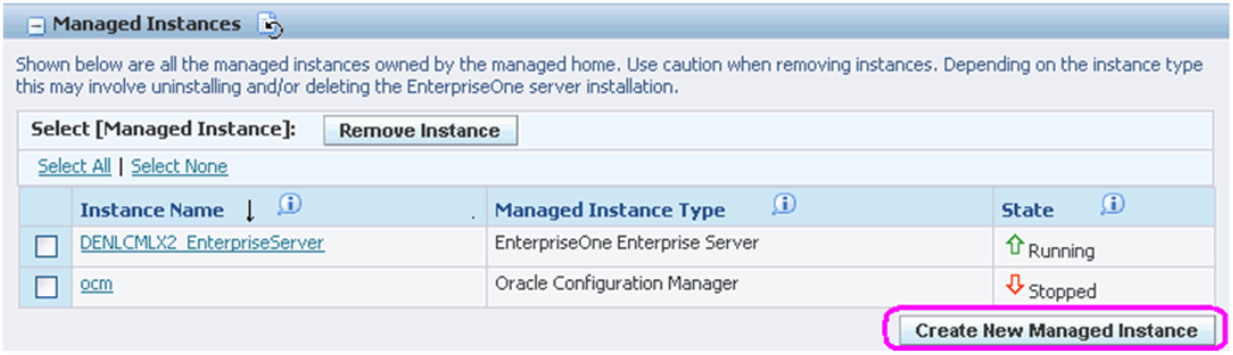
See Also:

- Section 18.1, "Prerequisites and Recommendation Installation Sequence for the Data Access Driver"

To install a JD Edwards EnterpriseOne Data Access Driver:



1. Select the Managed Home in which you wish to install the Data Access Driver.



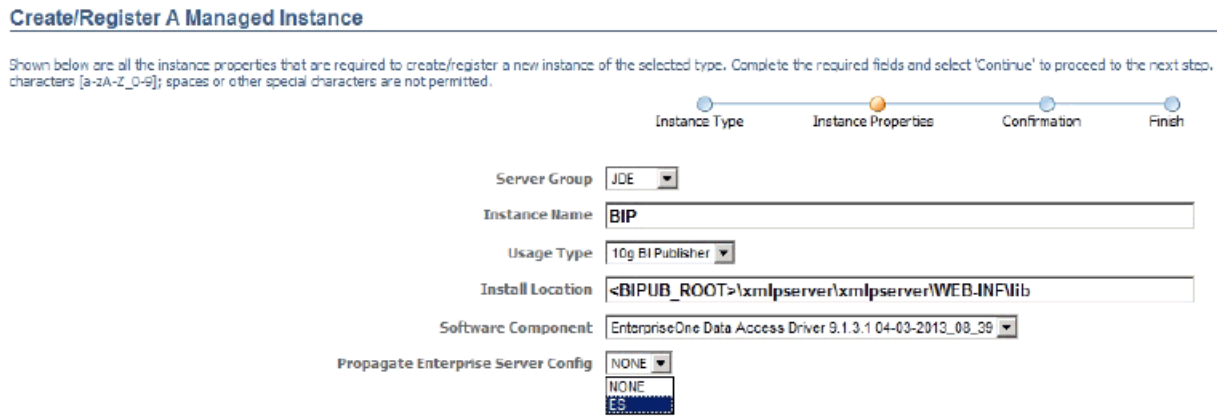
2. Click the *Create a New Managed Instance* button to create the Managed Instance in the Managed Home.

3. On Create/Register a Managed Instance, Instance Type, select this radio button:

EnterpriseOne Data Access Driver

> **Tip:** Ensure you choose the correct instance type for your intended installation. That is, there are two similar appearing instance types, one for Data Access Server and one for Data Access Driver.

4. Click Continue.



Note: The Propagate Enterprise Server Config drop-down appears only if any enterprise server is registered within the Server Manager console. The Propagate Enterprise Server Config drop-down contains the available enterprise server instances registered with the SM console within a particular selected server group. NONE is added to the drop-down by default.

5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

     Use the pull-down to select the Server Group to which you want this instance to belong.

     Also refer to Chapter 21, "Administer Management Console Users and User Groups".

   - *Instance Name*

     Enter a unique name for the instance name.

     Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

     `PRODUCT_SERVER_PORT`

     where `PRODUCT` is the JD Edwards EnterpriseOne instance type, such as `Data_Access_Driver`, and

     where `SERVER` is the machine on which the instance is installed, and

     where `PORT` is the HTTP port which is defined for use by this server.

   - *Usage Type*

     Use the pull-down to select the usage type for this Data Access Driver.

     If you choose *BI Publisher*, that application must already be installed. By default, Server Manager populates this field with the typical value for a BI Installation location, where you must manually complete this variable value for your installation:

     `<BIPUB_ROOT>`

     For example, a typical completed location to a BI Publisher installation might be:

     ```
     z:OraBIPub\oc4j_bi_
     j2ee\home\applications\xmlpserver\xmlpserver\WEB-INF\lib
     ```

If you choose *Generic*, you must provide the complete path to the application directory into which you wish to install the Data Access Driver. For example:

```
C:\jde_generic_read_only_driver_application
```

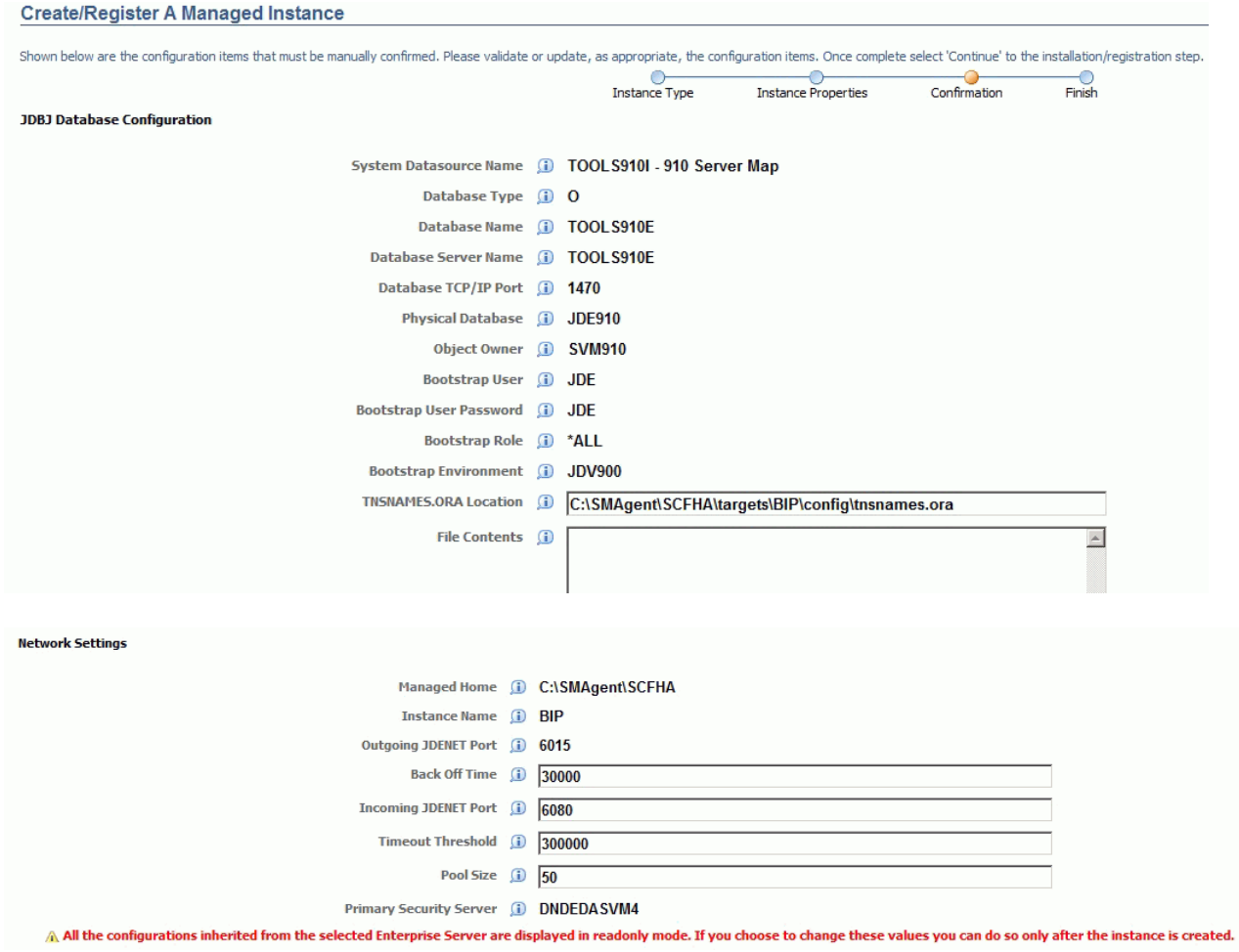
This location must be unique, must be empty, and must *not* be within the Management Agent directory structure.

- *Software Component*

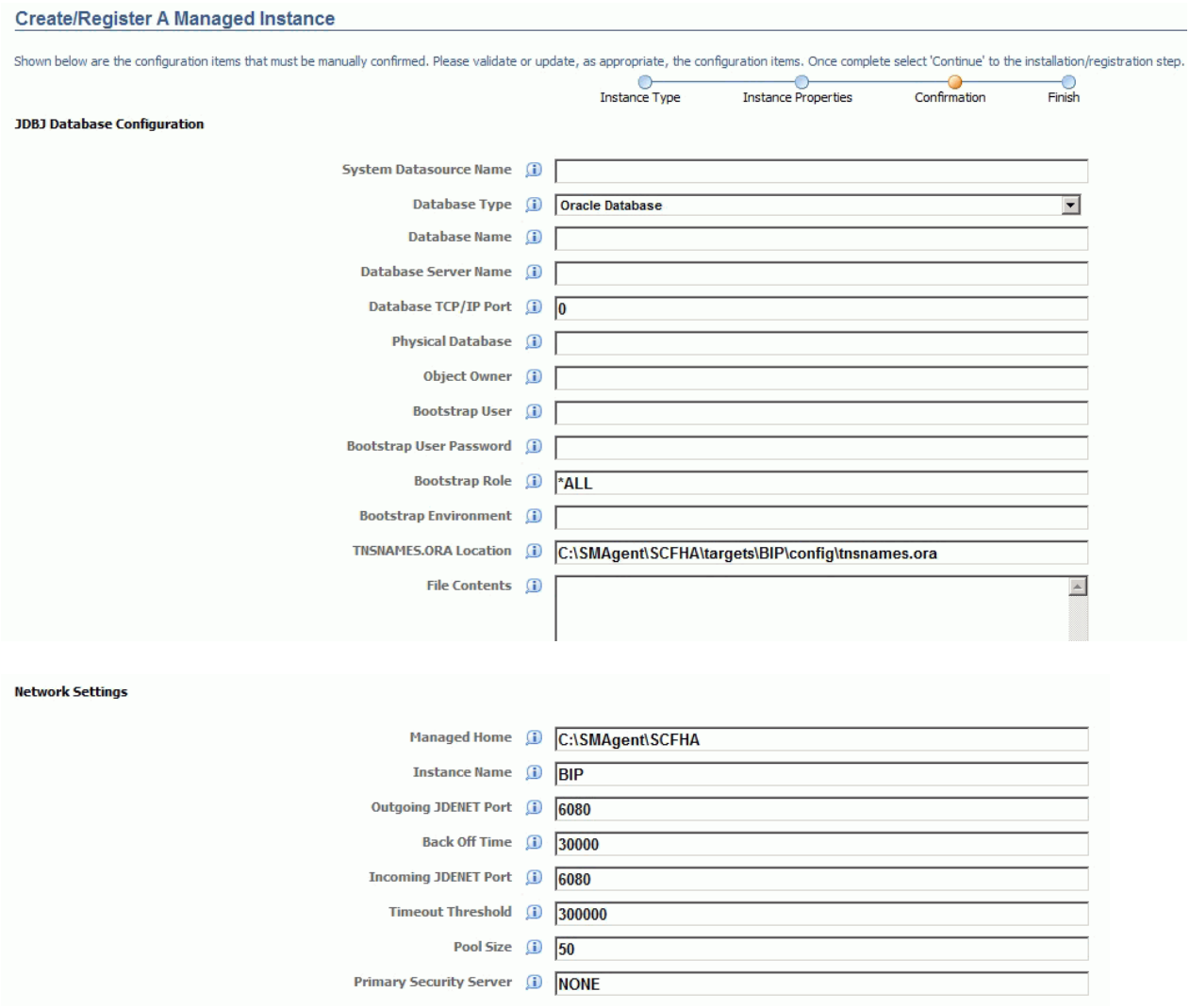
  Use the dropdown to select the version of this Software Component that you wish to install. For example:

  ```
  EnterpriseOne Data Access Driver Version 8.98.0.5_09225
  ```

6. Click Continue.



Note: This example illustrates an installation by selecting an enterprise server to be propagated.



Note: This example illustrates an installation by selecting NONE under Propagate Enterprise Server Config.

7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The values on this form must be manually confirmed. You must validate or update, as appropriate, all configuration items.

   Tip: For help, click the Information icon next to the title of a field.

   See Also:

   - Chapter 21, "Administer Management Console Users and User Groups"
   - Chapter 21, "Administer Management Console Users and User Groups"

8. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.

9. On Create/Register a Managed Instance, Finish, click the *Create Instance* button to complete the installation of the EnterpriseOne Data Access Driver.

Once the installation is complete the browser is redirected to the Management Console page for the newly registered Data Access Driver. This driver also appears as a Managed Instance within the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- *General*
  - *Status*

    Valid values are:

    – Running

      This status is set whenever the Management Agent on the machine where the Data Access Driver is installed reports that the Java class is loaded for use by BI Publisher or the Generic application. The agent checks and reports status periodically so the status shown by Server Manager will be accurate within a few minutes.

      Note that unlike Managed Instances for Servers, there is no option to Stop the driver from Server Manager. Therefore, no Stop button is displayed.

    – Stopped

      This status is set whenever the Management Agent on the machine where the Data Access Driver is installed reports that the Java class is unloaded by BI Publisher or the Generic application. The agent checks and reports status periodically so the status shown by Server Manager will be accurate within a few minutes.

      Note that unlike Managed Instances for Servers, there is no option to Start the driver from Server Manager. Therefore, no Start button is displayed.

  - *Software Component Version*

    Displays the version of this Software Component.

You must stop the system using the Data Access Driver (BI Publisher or Generic) before you can change the Software Component Version.

See Also:

- Change a Managed EnterpriseOne Software Component

- *Instance Properties*
  - *Install Location*

    The location where the Data Access Driver was installed.
  - *Instance Usage Type*

    Identifies the usage type of the Data Access Driver as either *BI Publisher* or *Generic*.
  - *Instance Name*

    The unique name assigned to the Managed Instance at the time it was created or registered.

For information on log files, refer to the chapter entitled: Available Log Files.

19

Remove a Managed Instance

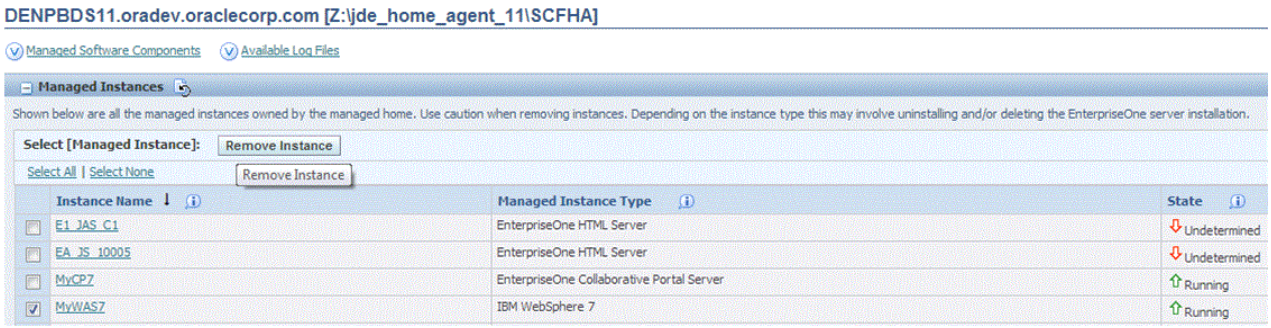
This chapter discusses:

- Section 19.1, "Remove an Application Server Managed Instance"
- Section 19.2, "Remove a JD Edwards EnterpriseOne Server Instance"

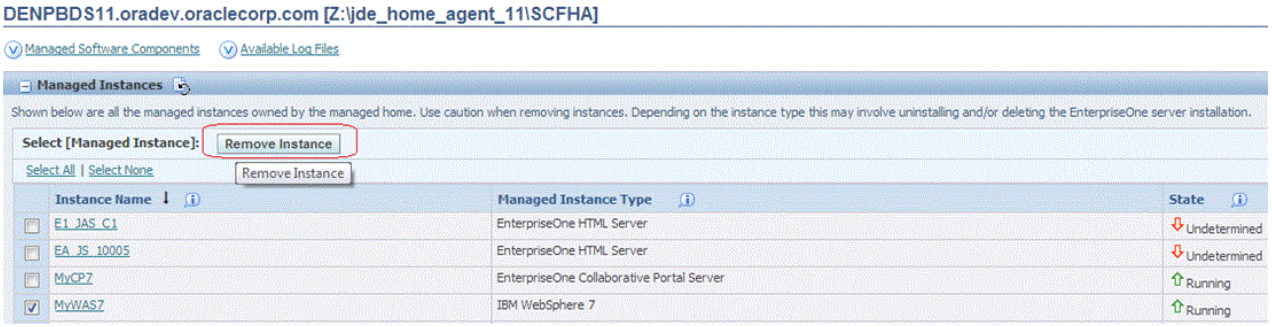
19.1 Remove an Application Server Managed Instance

You cannot remove an application server (either WebSphere Application Server or Oracle Application Server) Managed Instance that has a Server Manager dependent Managed Instance. You must remove all dependent Managed Instances before removing the application server Managed Instance.

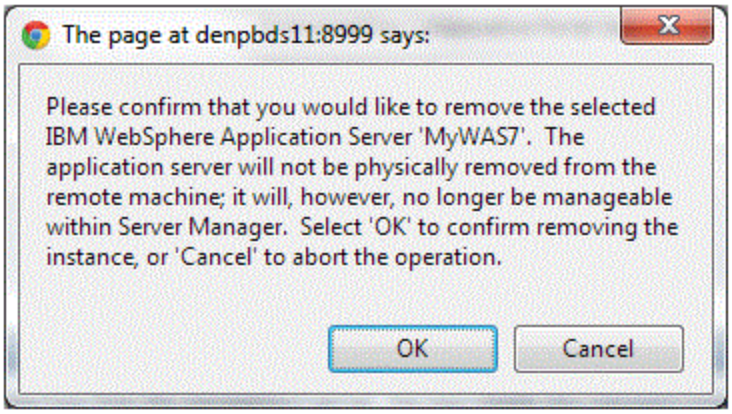
To remove an application server Managed Instance:



1. On the Managed Instances section of the page, select the Managed Instance Type associated with the application server that you want to remove.



2. Click the Remove Instance button to remove the selected application server Managed Instance.



3. On the confirmation dialog, click OK if you are sure that you want to remove the selected Managed Instance.

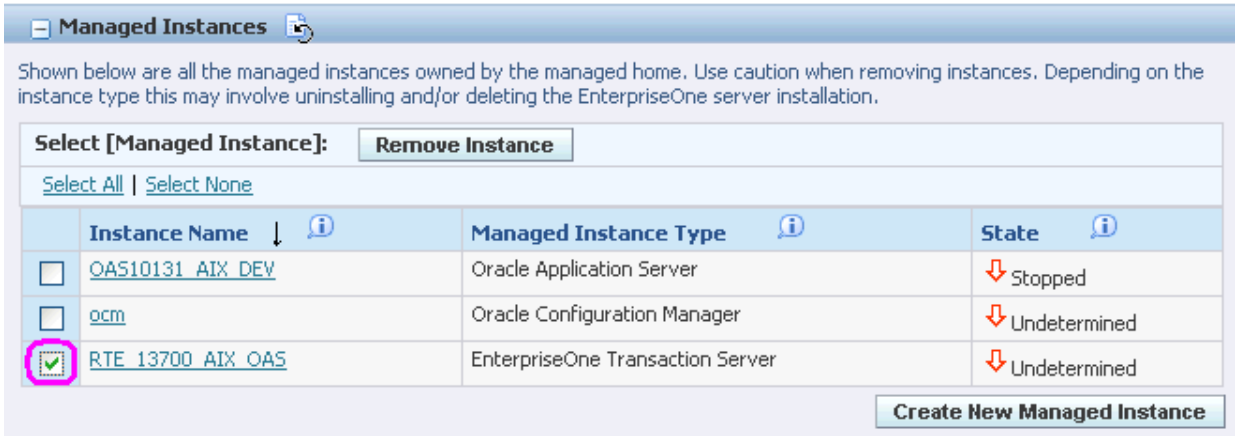
   If you choose OK, the application server will not be physically removed from the remote machine. It will, however, no longer be manageable with Server Manager.

If you attempt to remove an application server that has a dependent Managed Instance, the Management Console displays this error message:

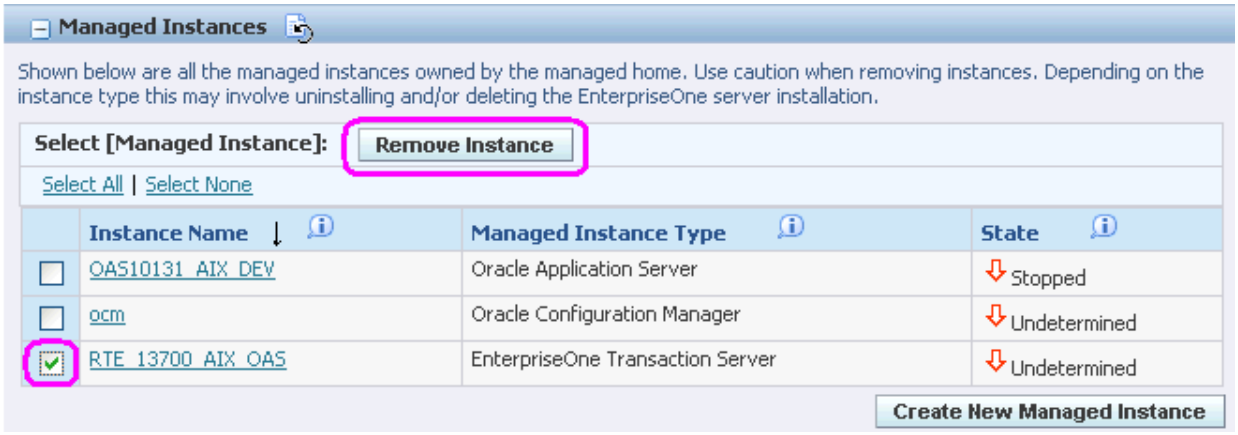
19.2 Remove a JD Edwards EnterpriseOne Server Instance

Note: This section uses screen captures of the JD Edwards EnterpriseOne "RTE" (Transaction Server) as an example. However, the procedure is identical for all JD Edwards EnterpriseOne servers with the exception of a JD Edwards EnterpriseOne Enterprise Server that was registered to (not created by) Server Manager. If you used Server Manager to register an existing JD Edwards EnterpriseOne Enterprise Server that was created outside of Server Manager, and you use Server Manager to remove that Managed Instance, the JD Edwards EnterpriseOne Enterprise Server is not actually removed from the machine; only the Managed Instance is removed from Server Manager.

To remove a JD Edwards EnterpriseOne server Managed Instance:



1. On the Managed Instances section of the page, select the Managed Instance Type associated with the JD Edwards EnterpriseOne server you want to remove.



2. Click the Remove Instance button to remove the selected JD Edwards EnterpriseOne server Managed Instance.

3. On the confirmation dialog, click OK if you are sure that you want to remove the selected Managed Instance.

   If you choose OK, the Managed Instance will be permanently removed from the application server to which it was installed.

20

Overview of Management Console Administration

Administering the Management Console involves these tasks:

- Setting up Management Console users and user groups

  The Management Console supports granular control of the managed instances a user may view and actions a user may perform. The Management Console employs user groups as an efficient way to manage permissions and servers. Instead of administering these items at the user level, you can associate permissions to a user group. You can determine which JD Edwards EnterpriseOne users have access to the Management Console and the user group or user groups to which the user should belong.

- Assigning permissions to user groups

  The Management Console contains two sets of permissions that you can assign to user groups: global permissions and server group permissions. Global permissions allow members of a user group to perform particular administrative tasks in the Management Console. Server group permissions allow users to perform certain administrative tasks on the servers that are managed centrally through the Management Console.

- Creating server groups

  - Control the default configuration for all servers in a group.
  - Manage updates to the server group members from one release to the next.
  - Control the tasks that Management Console users can perform on the servers in a server group.

21

Administer Management Console Users and User Groups

This section discusses how to:

- Configure the Management Console for User Setup
- Section 21.2, "Manage Management Console Users"
- Section 21.3, "Manage User Groups"
- Section 21.4, "Assign Server Manager Permissions"
- Section 21.5, "Run the User Access Report"

21.1 Configure the Management Console for User Setup

This section describes:

- Specify the JD Edwards EnterpriseOne Server Used for User Authentication
- Change the jde_admin User Password

You must use the jde_admin user ID and password to sign into the Management Console initially. This non-JD Edwards EnterpriseOne user ID and password are configured during the Server Manager installation. The jde_admin user has the authority to perform all functions within the Management Console and is responsible for adding and setting up the initial Management Console users from JD Edwards EnterpriseOne, as well as assigning permissions to those users.

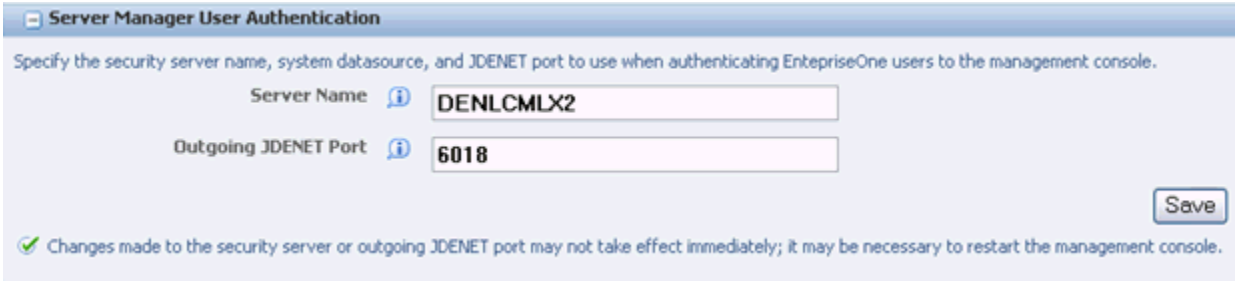
You can import users from JD Edwards EnterpriseOne using the Management Console Setup and Configuration Wizard, or you can add them as needed using the Management Console. JD Edwards EnterpriseOne users are authenticated using the security server services of an EnterpriseOne Enterprise Server. The Enterprise Server name and port used by the Management Console must be properly configured.

Note: JD Edwards EnterpriseOne users cannot access the Management Console with their JD Edwards EnterpriseOne user IDs and passwords until they have been added as Management Console users.

See Complete the Management Console Setup Wizard for information about using the Management Console Setup Wizard to add JD Edwards EnterpriseOne users to the Management Console.

21.1.1 Specify the JD Edwards EnterpriseOne Server Used for User Authentication

1. In the Quick Links section of the Management Console, click the Server Manager Users link.



2. In the Server Manager User Authentication pane, in the *Server Name* field, enter the name of the Enterprise Server to use for security services. The server must be running and listening on the same JDENET port that this instance is configured to use for outgoing connections.
3. In the Outgoing JDENET Port field, enter the TCP port to use for outgoing JDENET communications with a JD Edwards EnterpriseOne Enterprise Server. This value must match the JDENET Incoming Port (ServiceNameListen) defined for the Enterprise Server(s) with which this web server will communicate.
4. Click the *Save* button.

Note: It may be necessary to restart the management console application for the new settings to take effect.

21.1.2 Change the jde_admin User Password

The jde_admin user password is the only password that you can change in the Management Console. All other Management Console users use their JD Edwards EnterpriseOne user ID and password to sign in to the Management Console and these passwords are changed in JD Edwards EnterpriseOne.

1. In the Quick Links section of the Management Console, click the *Server Manager Users* link.

2. In the jde_admin Password section in the left pane, complete the Old Password, New Password, and Verify New Password fields to change the jde_admin password.

Note: If you lose the jde_admin password, there is no way to recover it. You will have to reinstall the Management Console.

21.2 Manage Management Console Users

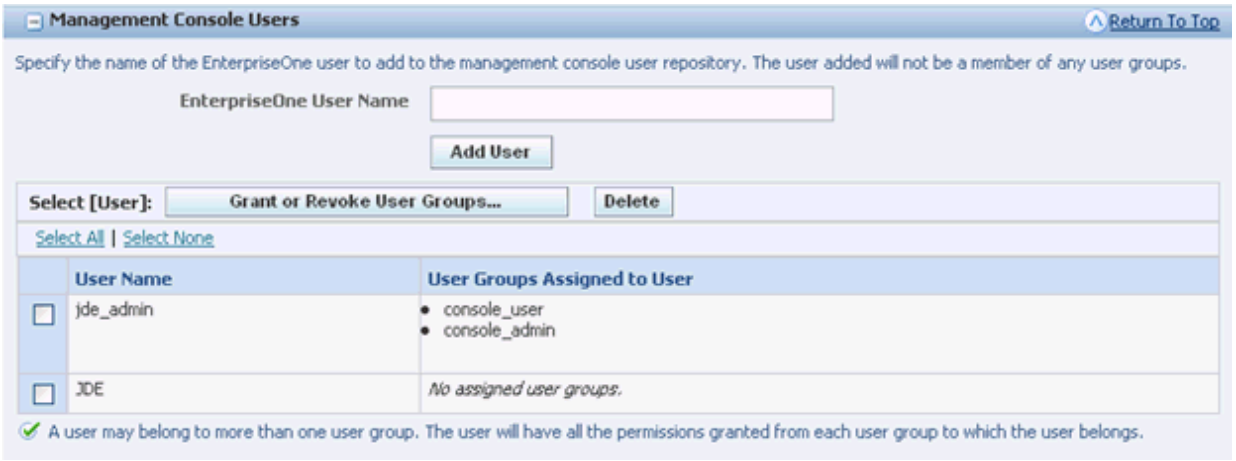
All users that you add to the Management Console are displayed in a grid in the interface. The Management Console displays the name of the user along with the user groups that are assigned to the user. You can sort each column alphabetically by clicking a column heading. All changes made to Management Console users and user groups take effect immediately.

This section describes:

- Add a User
- Remove a User

21.2.1 Add a User

1. In the Quick Links section of the Management Console, click the *Server Manager Users* link.



2. On *Server Manager Users*, in the *Management Console Users* pane, enter the name of the JD Edwards EnterpriseOne user in the EnterpriseOne *User Name* field.
3. Click *Add User*.

   The Management Console adds the user to its user repository. The added user will not belong to any user groups.

21.2.2 Remove a User

1. On Server Manager Users, in the Management Console Users pane, select the check box next to the user that you want to delete.
2. Click the *Delete* button.

21.3 Manage User Groups

This section describes:

- Create a User Group
- Delete a User Group

- Assign Users to a User Group
- Remove Users from a User Group

The Management Console employs user groups to manage permissions and group together users who perform similar tasks. Permissions are assigned to user groups, not individual users. A user may belong to zero or more user groups and will be authorized to perform the actions that are granted to each user group to which the user belongs.

See Assign Server Manager Permissions for a list of all the permissions that you can assign to user groups in Server Manager.

The Management Console displays each user group that you add in a grid. You can sort alphabetically on each column of the grid by clicking the column heading. The Management Console displays this information for each user group:

- User Group Name
- User Group Description
- Users Belonging to User Group
- Granted Permissions

The Management Console is delivered with the following predefined groups:

- console_user

  Any user who successfully authenticates and possesses this role may utilize the management console. If users do not belong to this user group, they cannot access any of the management console pages. You must have this permission to sign into the Management Console.

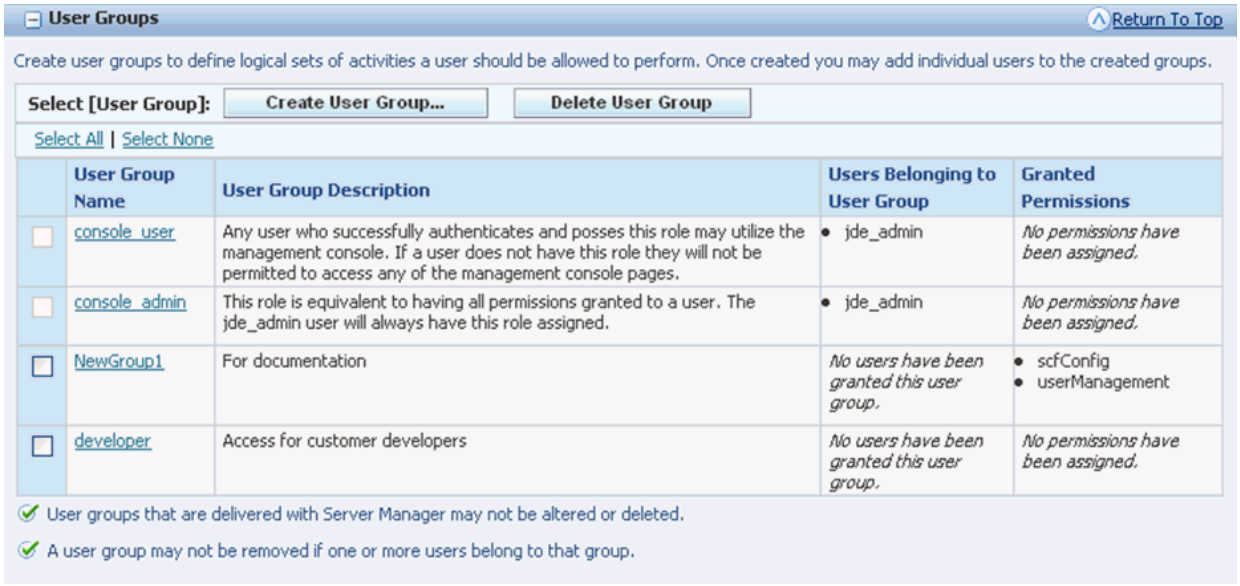
- console_admin

  This role is equivalent to having all permissions granted to a user. Users who belong to this user group automatically assume the rights of the console_user user group; it is not necessary to assign them to the console_user user group. The jde_admin user is always a member of the console_admin user group.

Note: The user groups that are delivered with Server Manager cannot be altered or deleted.

21.3.1 Create a User Group

1. In the Quick Links section of the Management Console, click the *Server Manager Users* link.



2. In the User Groups pane, click the Create User Group button.
3. Complete the User Group Name and Description fields and then click the Add User Group button.

The Management Console adds the new user group and displays the details about the user group in the grid.

21.3.2 Delete a User Group

Note: You cannot delete a user group if one or more users belong to that group.

1. In the User Groups pane, select the check box of the row that contains the user group that you want to delete.
2. Click the *Delete User Group* button.

21.3.3 Assign Users to a User Group

1. On the Server Manager Users page, scroll down to the Management Console Users pane and select the check box next to the user that you want to add to a user group.
2. Click the Grant or Revoke User Groups button.
3. In the User Group Name drop-down menu, select the user group to which you want to assign the user and then click the Grant User Group button.

21.3.4 Remove Users from a User Group

1. On the Server Manager Users page, select the check box next to the user that you want to remove from the user group.
2. Click the Grant or Revoke User Groups button.

21.4 Assign Server Manager Permissions

This section provides an overview of Server Manager permissions and discusses how to:

- Assign Global Permissions
- Assign Server Group Permissions

21.4.1 Understand Server Manager Permissions

Server Manager contains two types of permissions that you can assign to user groups global permissions and server group permissions. Both types of permissions are only assigned to user groups, not individual users. Server Manager follows Oracles secure by default security model. Management Console users cannot perform any functions unless they are authorized and have been assigned the appropriate permission to do so.

Global permissions allow users to perform administrative tasks in the Management Console that do not pertain to a particular server group, such as updating the Management Console software, distributing software components to managed homes, and granting other JD Edwards EnterpriseOne users access to the Management Console.

Server group permissions allow users to perform certain tasks on a particular server group. When you assign a server group permission, the permission applies to all servers that belong to the server group.

See Administer Server Groups for information about setting up and managing server groups.

21.4.2 Assign Global Permissions

Global permissions include:

- Application Server Management appServerConfig

  This permission is required to perform management tasks on an application server (Oracle Application Server or IBM WebSphere). A user who has this permission may register new application server instances, create new J2EE servers within the application server, start and stop application server components, and modify the configuration of the application server components. Users without this permission may see the application servers within the management console but may not perform any actions directly on those servers.

- Manage Software Components managedComponents

  This permission allows users to manage software components within Server Manager. With this permission, users can add software components to the Management Console User Repository, distribute or copy those components to managed homes, and delete software components both from the managed homes and from the management consoles.

- Monitor Configuration monitorConfig

  This permission allows users to manage the monitoring components of Server Manager. With this permission, users can create, delete, and start or stop configured monitors. Any user allowed to use Server Manager may view the contents of a running monitor; however, this permission is required to make any changes to the configuration of an existing monitor. In addition, users with this permission may remove any monitor reports from the monitor history.

- Console Configuration and Administration consoleConfig

  This permission allows users to manage the configuration of Server Manager. With this permission, users can update the Server Manager release, update deployed managed home agents, remove managed homes, configure the TCP/IP ports used by Server Manager, and download managed home agent installers. This permission is not required to manage the

Management Console user repository; that permission is granted by the userManagement permission.

- Server Manager User Management userManagement

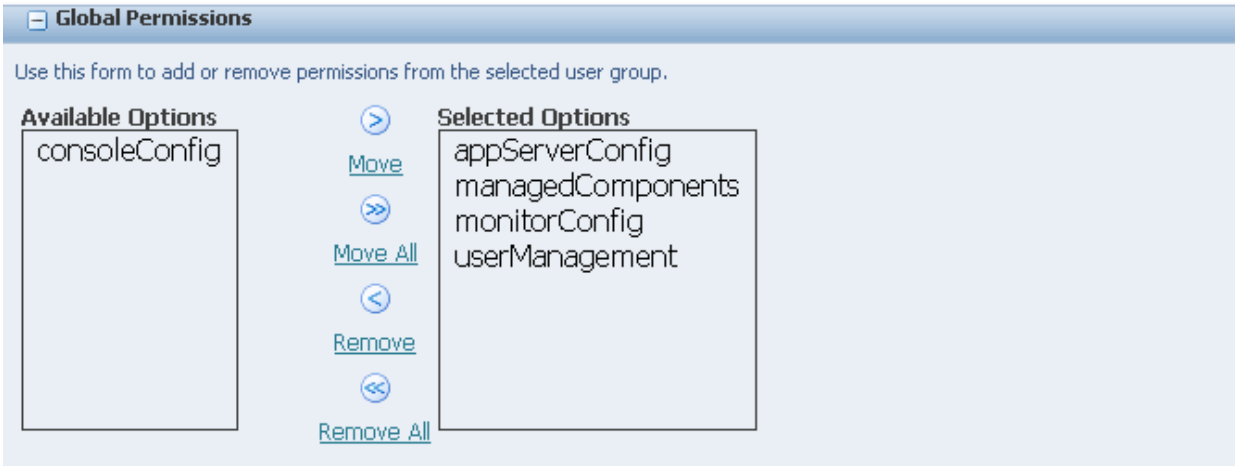
  This permission allows users to administer the Server Manager user management repository. With this permission, users can add additional JD Edwards EnterpriseOne users as Management Console users and assign permissions.

- Web Product User Session Management

  This permission allows users to manage web product user sessions. It allows users to terminate OWVirtual sessions, terminate user sessions including any running OWVirtual sessions, broadcast messages to OWVirtual clients, and temporarily disable logins to a web product.

To assign global permissions to a user group:

1. In the Quick Links section of the Management Console, click the Server Manager Users link.
2. In the User Groups pane, click the link of the user group to which you want to add permissions. For example, if you chose Global Permissions you would have these available options:



3. On Modify a User Group, in the Global Permissions pane, select a permission from the Available Options box.
4. Click the Move link (single right arrow) to move the permission to the Selected Options box.

   You can also grant the user group all global permissions by clicking the Move All link (double right arrow).

To remove global permissions from a user group:

1. In the User Groups pane, click the link of the user group to which you want to remove permissions.
2. In the Global Permissions pane, select the permission that you want to remove from the Select Options box.
3. Click the Remove link (single left arrow).

   You can also remove all permissions in the Selected Options box by clicking the Remove All link (double left arrow).

21.4.3 Assign Server Group Permissions

Server group permissions include:

- Permit Clearing JDBj Caches clearCache

  This permission allows users to clear the JDBj caches that are maintained with the JD Edwards EnterpriseOne web products.

- Enterprise Server Instance Management - enterpriseServerInstance

  This permission allows users to create new Enterprise Servers, remove existing Enterprise Servers, configure Enterprise Servers, and start or stop Enterprise Servers. This permission also allows users to change the JD Edwards EnterpriseOne Tools release of a corresponding server. This permission is required to manage a JD Edwards EnterpriseOne Enterprise Server.

- View Group Members viewGroupMembers

  This permission allows users to view the JD Edwards EnterpriseOne servers that are members of a server group. Without this permission, users cannot view the server group members in the Management Console. You must explicitly grant this permission to each desired server group; no other permission implies or inherits this permission.

- Web Product Instance Management webProductInstance

  This permission allows users to create new web product instances, remove existing web product instances, configure web products, register/de-register application servers, configure application servers, and start or stop application servers and web products. This permission also allows users to change the JD Edwards EnterpriseOne Tools release of a corresponding server. This permission is required to allow users to manage JD Edwards EnterpriseOne web products including HTML servers, Transaction Servers, Business Service servers, and the corresponding application servers (Oracle Application Server and IBM WebSphere).

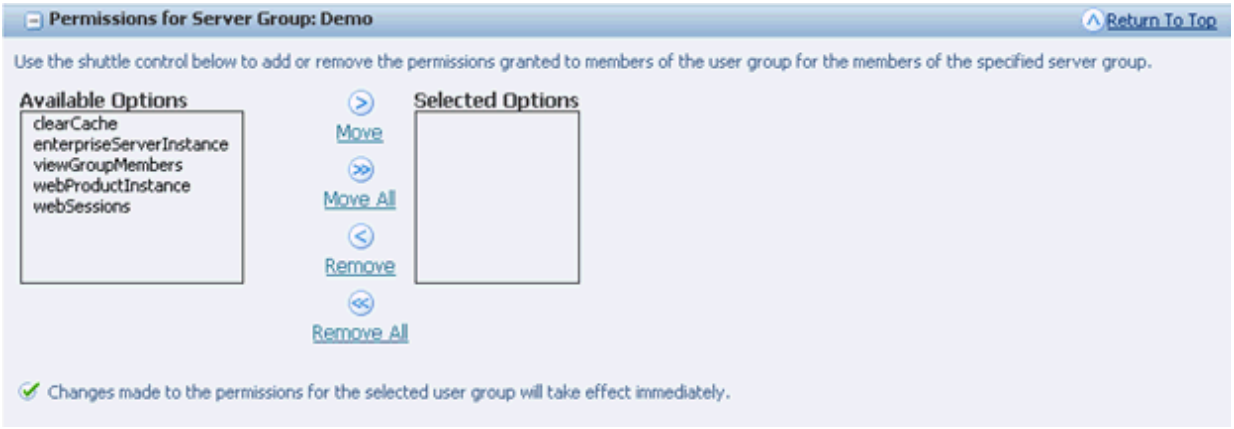
- Web Product User Session Management webSessions

  This permission allows users to manage web product user sessions. With this permission, users can terminate OWVirtual sessions and user sessions (including any running OWVirtual sessions), broadcast messages to OWVirtual clients, and temporarily disable anyone from signing onto a web product.

To assign server group permissions to a user group:

1. In the Quick Links section of the Management Console, click the Server Manager Users link.
2. In the User Groups pane, select the user group to which you want to assign server group permissions.

   The Management Console displays a separate pane for each server group in the Management Console. Each pane displays the permissions for that particular server group.



3. On Modify A User Group, scroll to the server group to which you want to add server group permissions for the user group.
4. Select the permission from the Available Options box and then click the Move link (single right arrow) to move the permission to the Selected Options box.

   You can also grant the user group all server group permissions by selecting the Move All link (double right arrow).

To remove server group permissions from a user group:

1. In the User Groups pane, select the user group to which you want to remove server group permissions.
2. On Modify A User Group, scroll to the server group to which you want to remove server group permissions from the user group.
3. On Modify A User Group, in the Server Group pane, select the permission from the Selected Options box and then click the Remove link (single left arrow) to remove the permission.

   You can also remove all server group permissions from the user group by selecting the Remove All link (double left arrow).

21.5 Run the User Access Report

The User Access Report generates a list of all the Management Console users and lists the following information for each user:

- The user groups that a user is a member of
- Global permissions assigned to each user group of which a user is a member
- Server group permissions assigned to each user group of which a user is a member

Use this report to verify that you have added users to the appropriate user groups and that you have applied the appropriate permissions to each user group.

You must have the userManagement global permission to be able to view the report.

To run the User Access Report:

1. In the Quick Links section of the Management Console, click the Server Manager Users link.
2. In the User Management Tasks section, click the User Access Report link.

User Access Report

User: jde_admin

Assigned User Groups	Non-Group Permissions	Server Group: default	Server Group: Demo
	All Permissions Granted	All Permissions Granted	All Permissions Granted

User: JDE

Assigned User Groups	Non-Group Permissions	Server Group: default	Server Group: Demo
	No permissions granted.	*No permissions granted.*	*No permissions granted.*

22

Monitor JD Edwards EnterpriseOne Servers

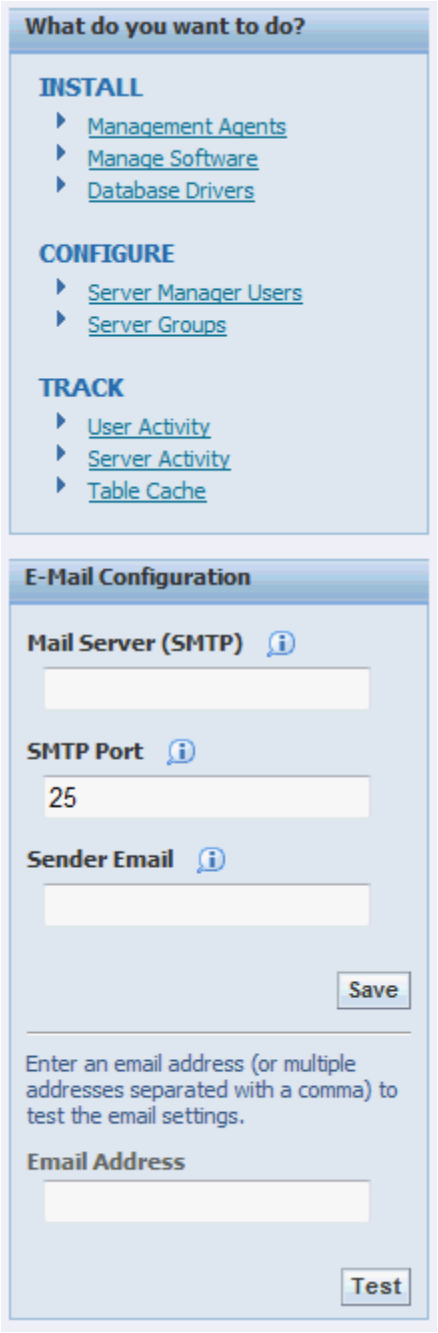
This chapter discusses:

- Section 22.1, "E-Mail Configuration"
- Section 22.2, "Monitors"

22.1 E-Mail Configuration

When you click the *Server Activity* link in the *What do you want to do?* pane, the Management Console displays another pane under *What do you want to do?* called *E-Mail Configuration*.

E-Mail is sent through SMTP and is SMS/pager friendly.



To configure e-mail notification for monitors:

1. Complete these fields:

   - *Mail Server (SMTP)*

     Defines the name of the SMTP mail server Server Manager will utilize for sending e-mails.

   - *SMTP Port*

     The TCP/IP port to use when connecting to the SMTP mail server for sending e-mails. The default value is 25, though some mail servers may be configured to use an alternate port.

- *Sender Email*

  The e-mail address to use as the sender for e-mail notifications sent by Server Manager.

- *Email Address*

  Enter an email address (or multiple addresses separated with a comma).

2. Click the *Save* button to save your settings.
3. To verify your settings and email address for use by Monitors, click the *Test* button. If the test is not successful, an error appears.

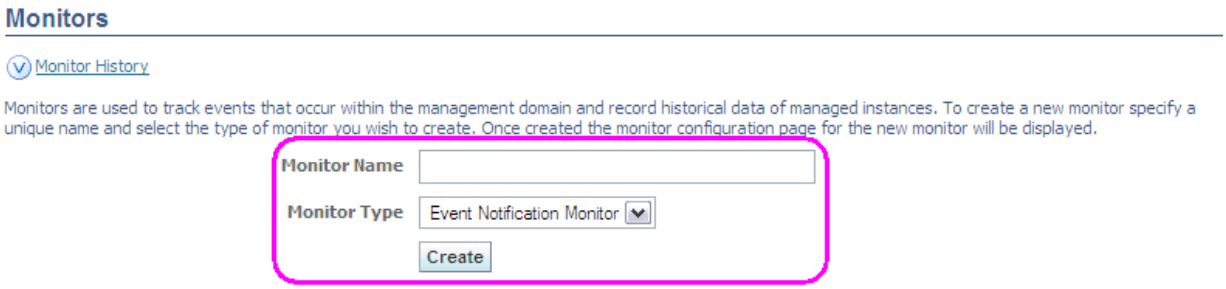
22.2 Monitors

This section describes:

- Create a Monitor
- Monitor Configuration
- Available Monitors
- Monitor History

22.2.1 Create a Monitor

You use monitors to track events that occur within the management domain and record historical data of managed instances. Once you create the monitor, the configuration page for the new monitor will be displayed. Multiple monitors can be created with different parameter settings to monitor various aspects of managed instances. An email can then be sent to the appropriate person or group alerting them to specified status changes in the managed instances.



To create a new monitor:

1. Complete these fields:

   - *Monitor Name*

     Defines the name of the new monitor. The monitor name must be unique.

   - *Monitor Type*

     Defines the type of the new monitor. The available monitor types appear in the drop down selection.

2. Click the *Create* button to create your new monitor. When the new monitor has been created a monitor configuration page is displayed.

22.2.2 Monitor Configuration

All configuration items for the new monitor are displayed on this page.

This section describes:

- General Properties
- Managed Instances
- Monitored Events
- Notification Hours
- E-Mail Subscriptions

22.2.2.1 General Properties

To configure *General Properties* for monitors:

1. Complete these fields:

   - *Query Interval (Seconds)*

     Specifies the number of seconds between collections. Some monitored events are pushed to the management console, in which case the corresponding notifications will be sent soon after the event occurs. Other events require periodic polling to identify. This value specifies the amount of time between those polls. Use caution when setting this to a low value (such as under a minute), as this may negatively impact performance of the managed instances.

   - *Automatically Start Monitor*

     You select this to automatically start the new monitor. If the Management Console should stop and restart, the monitor will start automatically if this has been selected.

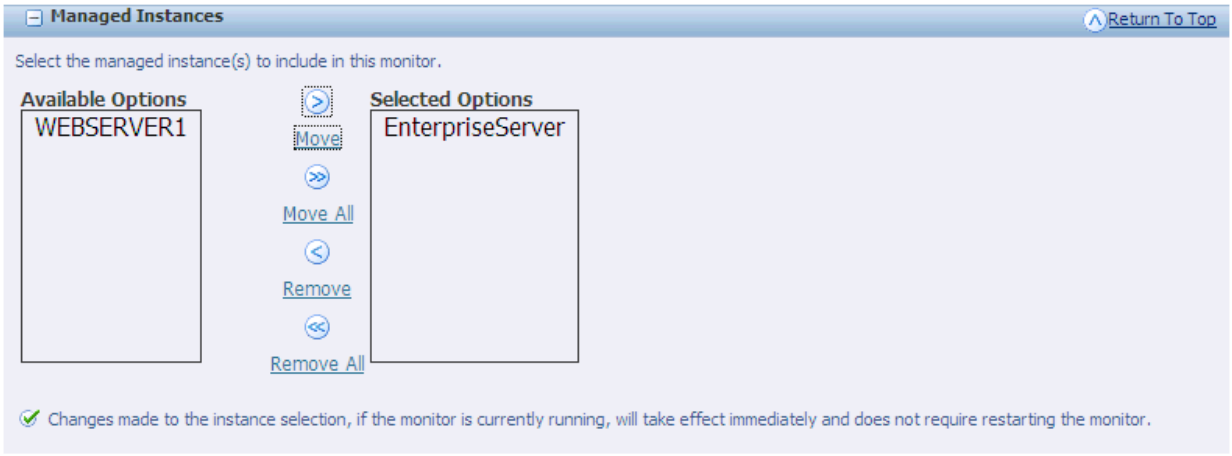
2. Click the *Save* button to save your settings.

Note: The Save button applies only to the pane where the Save button is located. It does not save the entire page. The Save button must be clicked within each pane for changes made within that pane.

22.2.2.2 Managed Instances

This section describes:

- Include a Managed Instance(s) in a Monitor
- Remove a Managed Instance(s) from a Monitor



22.2.2.2.1 Include a Managed Instance(s) in a Monitor One or more managed instances may be selected to be monitored.

To include a managed instance(s) in a monitor, either:

1. Select an instance from *Available Options* and click *Move*, or
2. Click *Move All* to include all managed instances.

22.2.2.2.2 Remove a Managed Instance(s) from a Monitor To remove a managed instance(s) from a monitor, either:

1. Select an instance from *Selected Options* and click *Remove*, or
2. Click *Remove All* to remove all managed instances.

Note: Changes made to the instance selection, if the monitor is currently running, will take effect immediately and does not require restarting the monitor.

22.2.2.3 Monitored Events

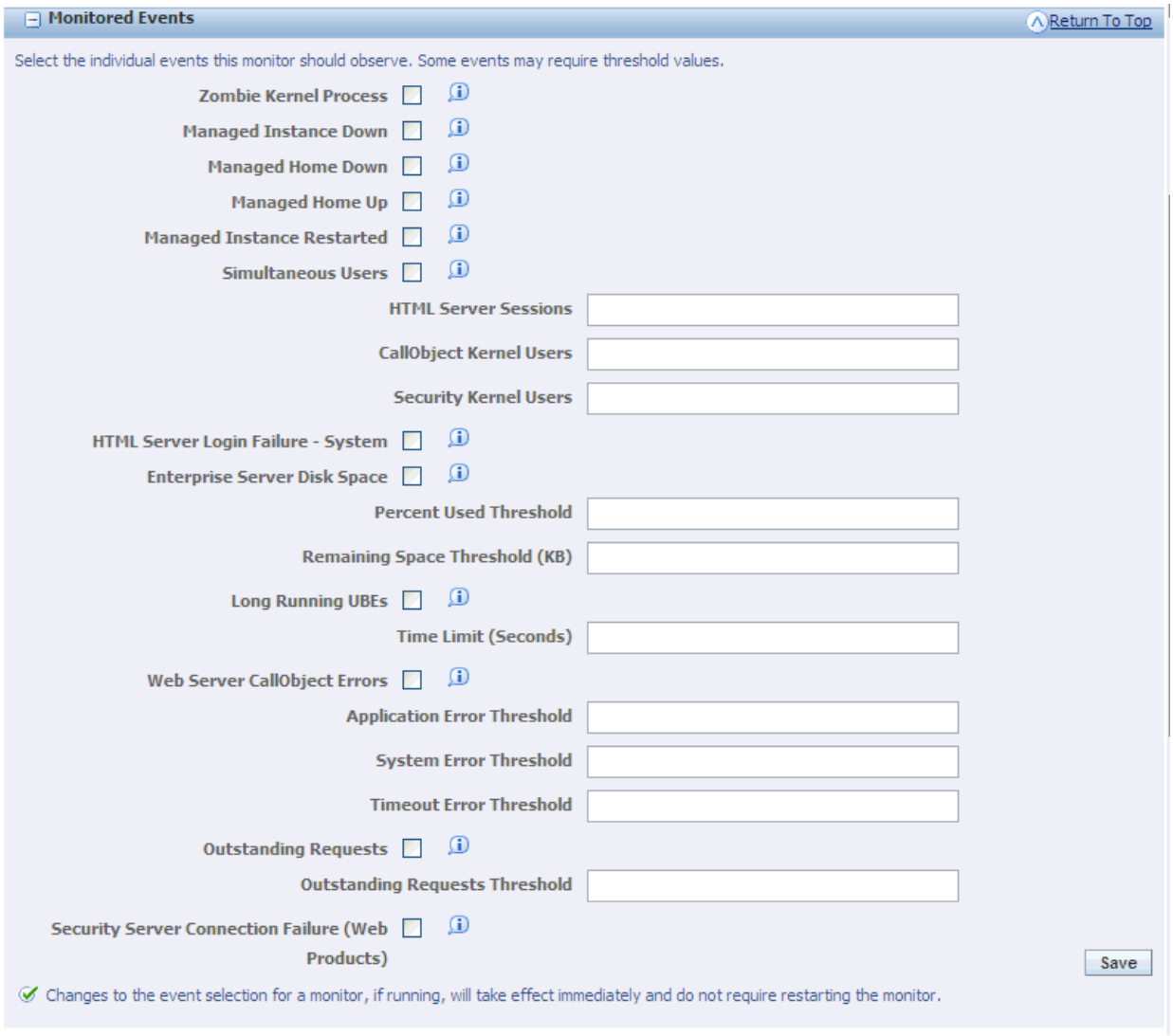
You can select the individual events that a specific monitor should observe that will trigger an e-mail alert.

Examples include:

- Enterprise server kernel crashes
- Web user unable to sign in due to system error
- Security server down
- Simultaneous users exceeding specified thresholds
- Low disk space on enterprise server
- Managed instance down
- Managed home down

Note: Some events may require threshold values.

To specify the events to monitor:



Events may be dynamically enabled or disabled for a particular monitor.

1. On Monitored Events, select from these fields:

   - *Zombie Kernel Process*

     This event occurs when an enterprise server process (including network, kernel, and runbatch processes) unexpectedly terminates.

   - *Managed Instance Down*

     This event occurs when a matching instance was in the running state on the previous collection but is no longer running.

   - *Managed Home Down*

     This event occurs if the connection between the management console and a connected managed home is lost. This could be because the management agent within the managed home is down, or the network connection was severed.

   - *Managed Home Up*

     This event occurs if when the connection between a managed home and the management console is established.

- *Managed Instance Restarted*

  This event occurs when a managed instance is stopped and restarted within the last sampling interval. If a server is stopped and restarted but the operation does not complete within the sleep interval of this monitor the notification will be handled as a managed instance down rather than restart.

- *Simultaneous Users*

  This event is triggered when the specified threshold of users is reached. This event is checked on the timed interval specified for the monitor. You may set thresholds for the number of simultaneous users active in an EnterpriseOne HTML server, connected to a single CallObject kernel on the enterprise server, or connected to a security server kernel on the enterprise server. This notification will be sent the first time the threshold value is met, and each time thereafter when the value is larger than any previously sent notification.

- *HTML Server Sessions*

  Specifies the threshold when the event will be triggered.

- *CallObject Kernel Users*

  Specifies the threshold when the event will be triggered.

- *Security Kernel Users*

  Specifies the threshold when the event will be triggered.

- *HTML Server Login Failure - System*

  This event occurs when a user cannot sign onto a HTML server due to a system related failure. It does not include login failures caused by incorrect user activity, such as supplying incorrect login credentials.

- *Enterprise Server Disk Space*

  This event occurs when a physical disk on a monitored enterprise server meets the specified threshold value(s). You may specify the 'Percent Used Threshold', in which an event will be triggered if the usage on the disk/volume reaches or exceeds the specified percentage. An event may also be specified when the disk has less than a specified number of kilobytes available. The enterprise server must be running at the time of collection for this metric to be evaluated.

- *Percent Used Threshold*

  Specifies the threshold when the event will be triggered.

- *Remaining Space Threshold (KB)*

  Specifies the threshold when the event will be triggered.

- *Long Running UBEs*

  Allows you to specify, in seconds, a threshold value for the duration of UBEs. If a UBE takes longer than the specified threshold to complete a notification will be sent.

- *Time Limit (Seconds)*

  Specifies the threshold when the event will be triggered.

- *Web Server CallObject Errors*

  This event enables receiving notification whenever a problem occurs while performing a CallObject (business function) request from an EnterpriseOne HTML server to an enterprise server. You may specify a threshold for each of the error types that may occur. Once reached notifications will be sent for the corresponding CallObject error.

- *Application Error Threshold*

  Specifies the threshold when an event will be triggered.

- *System Error Threshold*

  Specifies the threshold when the event will be triggered.

- *Timeout Error Threshold*

  Specifies the threshold when the event will be triggered.

- *Outstanding Requests*

  This event occurs when a kernel process reaches the supplied threshold value for outstanding request. Outstanding requests are requests that are queued for the kernel but have not yet executed to do current work. The notification will be sent each time outstanding requests are greater than the last sample period and above the specified threshold value.

- *Outstanding Requests Threshold*

  Specifies the threshold when the event will be triggered.

- *Security Server Connection Failure (Web Products)*

  This event occurs if a user attempts to sign on to a web product and the configured security server did not successfully respond to the authentication request.

2. Click the *Save* button to save your settings.

Note: Changes to the event selection for a monitor, if running, will take effect immediately and do not require restarting the monitor.

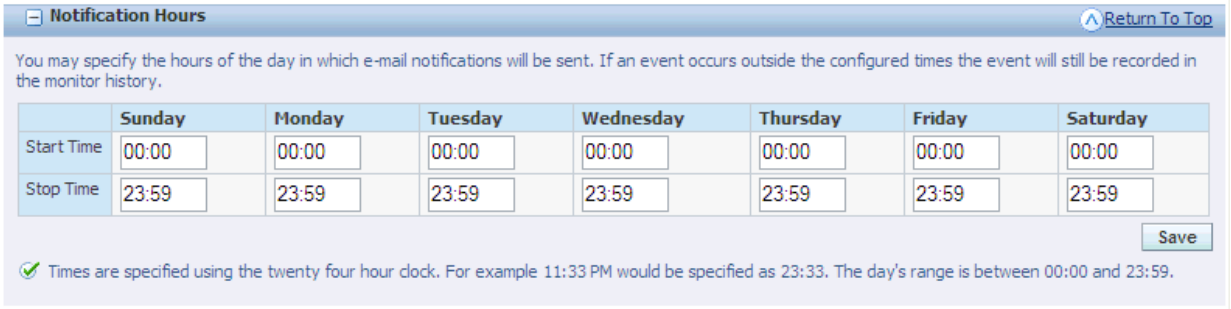
Note: If input values are used in the enterable fields, the parameter field immediately above the input section must have the check box selected in order for the input values to be applied.

22.2.2.4 Notification Hours

You may specify the hours of the day in which e-mail notifications will be sent. If an event occurs outside the configured times the event will still be recorded in the monitor history. An email per event, per threshold, per duration will be sent.

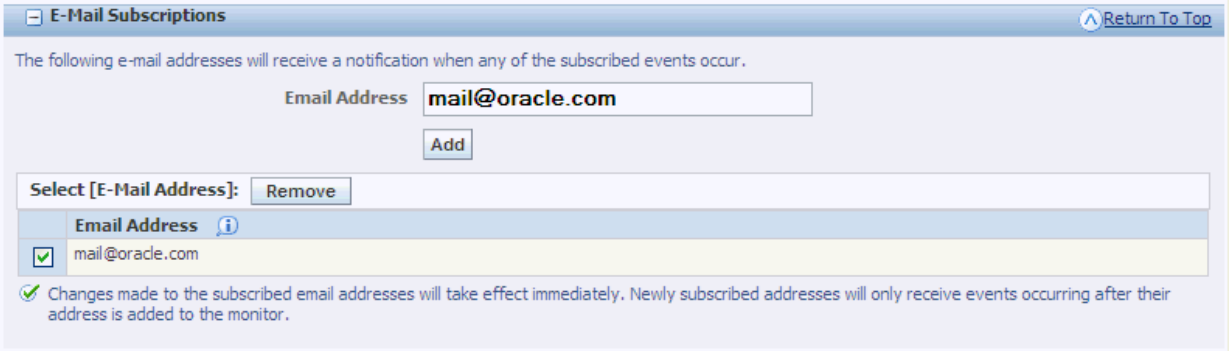
You may have identical monitors assigned to different time frames to notify different people. A monitor may be set up to notify a person during prime hours, and a different identical monitor to notify a different person for non-prime hours.

To specify notification hours, enter start and stop times using the twenty four hour clock. For example 11:33 PM would be specified as 23:33. The day's range is between 00:00 and 23:59.



22.2.2.5 E-Mail Subscriptions

Specified e-mail addresses, including distribution lists, will receive a notification when any of the subscribed events occur. An unlimited amount of e-mail addresses may be added to a monitor.



To add e-mail subscriptions:

1. Enter an email address (or multiple addresses separated with a comma).
2. Click the *Add* button.

To remove e-mail subscriptions:

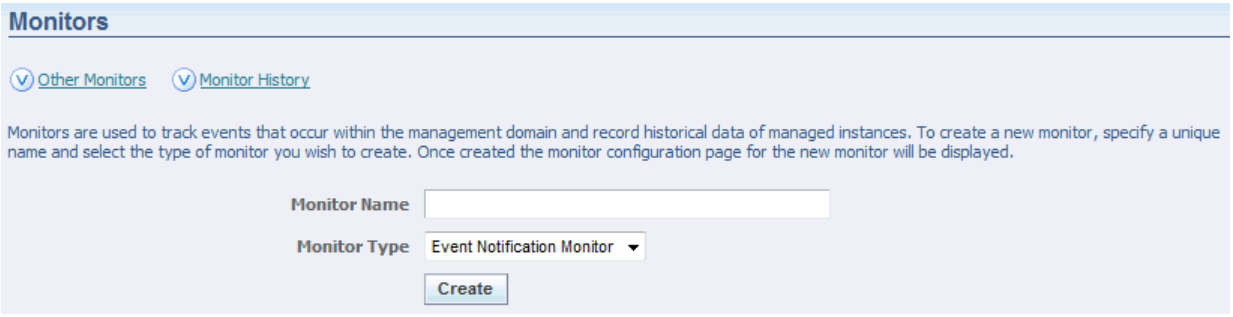
1. Select the check box for an email address(es).
2. Click the *Remove* button.

22.2.3 Available Monitors

Displays each of the monitors. Use the links to modify the configuration of the individual monitor. If the monitor is currently running or has been run since the management console was started you may view the monitor results.

This section describes:

- Start a Monitor
- Stop a Monitor
- Delete a Monitor
- Modify the Monitor Configuration
- View a Monitor Report
- Create a Duplicate Monitor



22.2.3.1 Start a Monitor

To start a monitor:

1. Select the check box for a monitor(s).
2. Click the *Start* button.

22.2.3.2 Stop a Monitor

To stop a monitor:

1. Select the check box for a monitor(s).
2. Click the *Stop* button.

22.2.3.3 Delete a Monitor

To delete a monitor:

1. Select the check box for a monitor(s).
2. Click the *Delete* button.

22.2.3.4 Modify the Monitor Configuration

To modify the monitor configuration, click the icon in the *Configure* column for the monitor.

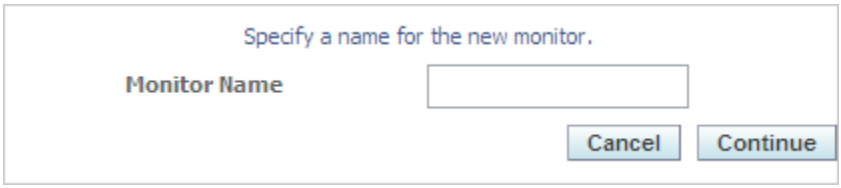
22.2.3.5 View a Monitor Report

To view a monitor report, click the icon in the *View Report* column for the monitor. The icon will change if the report has run.

22.2.3.6 Create a Duplicate Monitor

To create a duplicate monitor:

1. Click the icon in the *Create Duplicate* column for the monitor.
2. Specify a name for the new monitor, by completing the *Monitor Name* field.



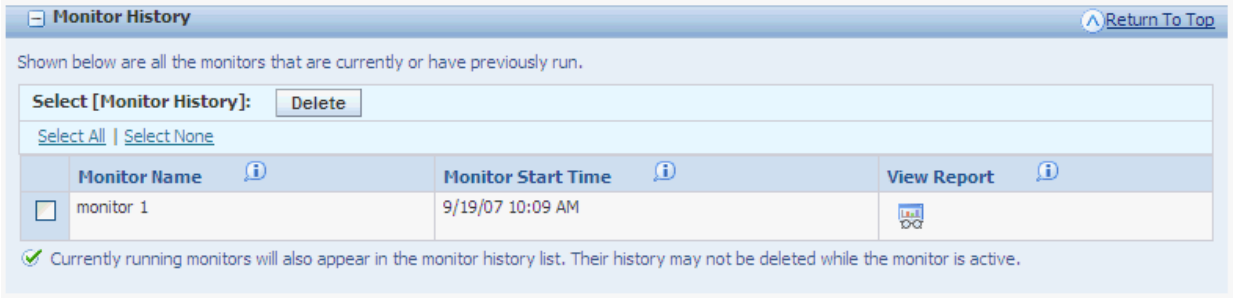
3. Click the *Continue* button.
4. Complete the *Monitor Configuration* page.
5. Click the *Save* button for every pane.

22.2.4 Monitor History

The Monitor History section displays all monitors that are currently or have previously run.

This section describes:

- Delete Monitor History
- View the Monitor Start Time
- View Report



22.2.4.1 Delete Monitor History

To delete monitor history:

1. Select the check box for a monitor(s).
2. Click the *Delete* button.

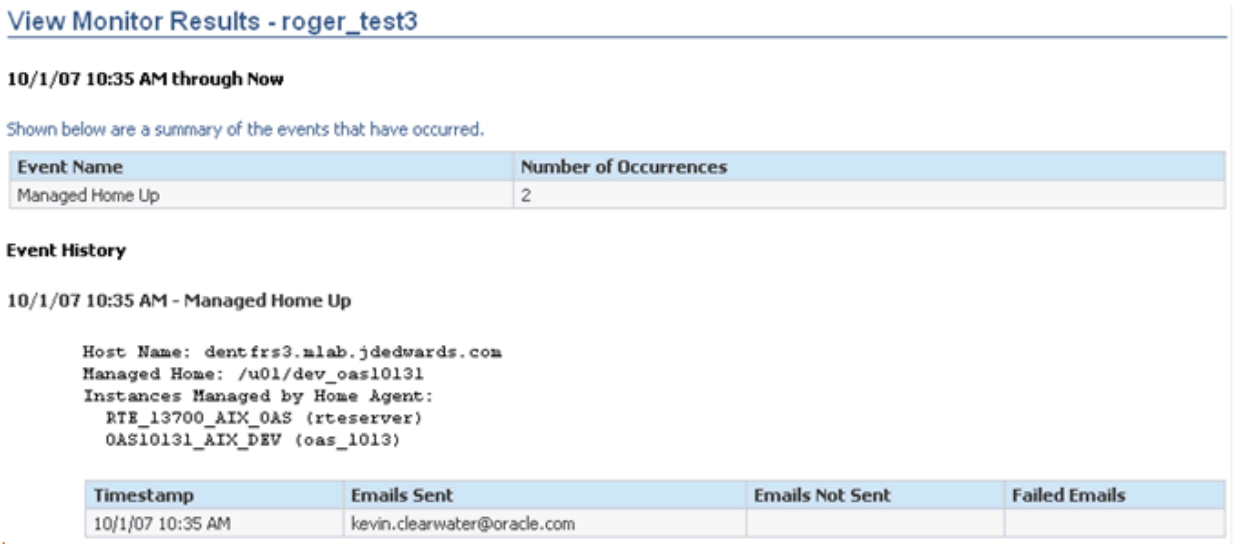
22.2.4.2 View the Monitor Start Time

To view a monitor start time look in the *Monitor Start Time* column for the monitor.

22.2.4.3 View Report

To view a monitor history report:

1. Select the check box for a monitor(s) history.
2. Click the icon in the *View Report* column.



The report provides information for the event and email. The Emails Not Sent field will report the number of emails accumulated outside the Notification Hours designated in the configuration settings for the monitor. The Failed Emails field will report the number of emails not delivered due to any issues with the email system, such as an email server being down.

Note: Currently running monitors will also appear in the monitor history list. Their history may not be deleted while the monitor is active.

23

Available Log Files

This chapter discusses:

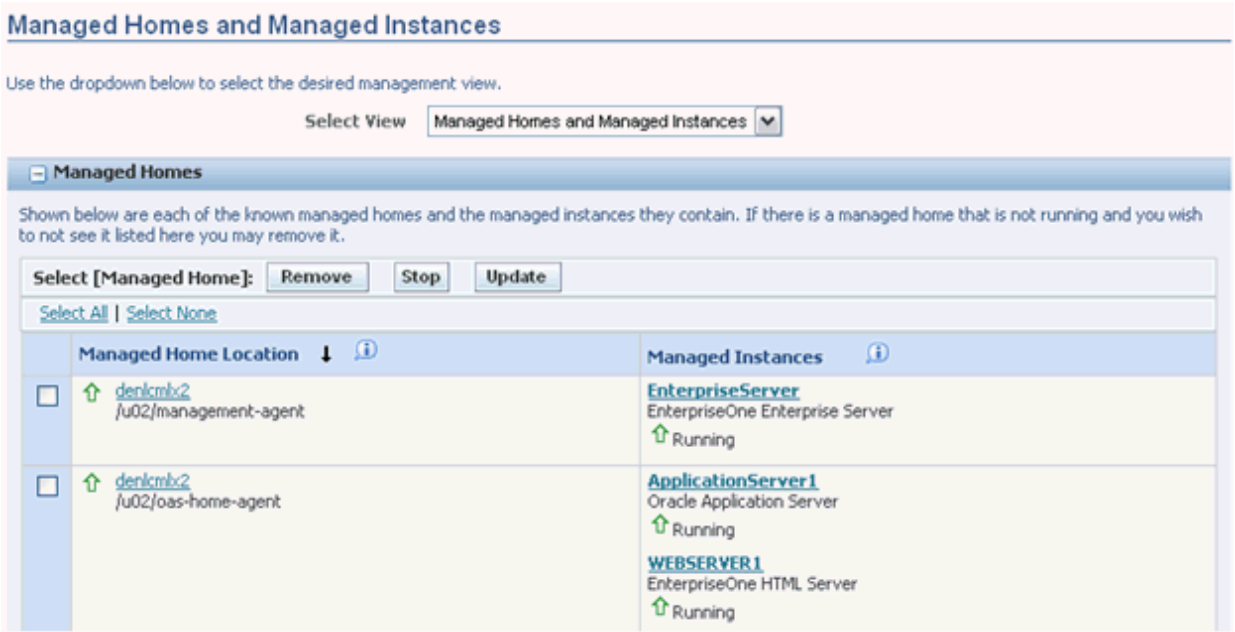
- Section 23.1, "Managed Home Log Files"
- Section 23.2, "Managed Instance Log Files"
- Section 23.3, "jde.properties Logging"

23.1 Managed Home Log Files

This section describes:

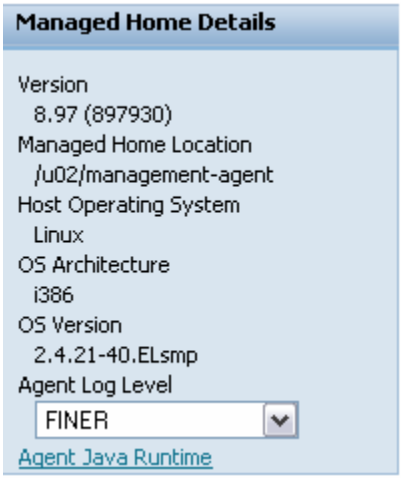
- Managed Home Details
- Agent Log Level

Server Manager generates log files detailing its activity within the Managed Homes. Managed Home logging can be accessed from the main menu. Upon logging into Server Manager, find the Managed Home that you want to access by selecting the view in the *Select View* field called Managed Homes and Managed Instances. In the grid field called *Managed Home Location*, select the Managed Home Location with the logs that you want to view.



23.1.1 Managed Home Details

When a Managed Home Location has been selected, the *Managed Home Details* section appears on the next screen. This section provides selection options for configuring the messaging level for the Management Agent logs.



23.1.2 Agent Log Level

The Management Agent generates log messages at various log levels. Use the *Agent Log Level* dropdown to change the level of the messages are written to the Management Agent logs. Any changes to the log level are stored in the Managed Home configuration and are used even after the Management Agent is restarted.

The log file receives all messages that are at or above the selected log level. For example, if the log level is configured to Fine the log files will receive all generated messages at the Fine, Config, Info, Warning, and Severe level.

The default and recommended level is Fine. The finer and finest log levels should only be used for troubleshooting a specific Server Manager issue.

- *Off*

  This setting prevents any log messages from being written. It is not recommended to disable logging.

- *Severe*

  This level is for errors from which the system is not able to recover. Severe events are very rare for Server Manager and indicate a significant problem that needs to be addressed.

- *Warning*

  This level is for errors from which the system can recover; however these errors indicate a deviation from the expected path of least resistance scenario and are indicative of failure points in overall system health.

- *Info*

  This level receives messages that indicate the high-level tasks the agent is performing.

- *Config*

  This level includes information about the configuration or environment used by the Management Agent.

- *Fine*

This level includes trace-level logging messages used to understand not just which actions the Management Agent is performing but also details about how it is performing those tasks.

- *Finer*

  This level contains more detailed messages.

- *Finest*

  This level contains the most detailed messages and may generate large log files.

- *All*

  At this level all log messaging levels are displayed; it is equivalent to selecting Finest.

The Management Agent writes log files to a subdirectory named logs on its the installation path. The log files may be viewed using the Server Manager log file viewer.

The Management Agent maintains up to ten log files with a maximum size of 10MB each. The most recent log file always has _0 in the filename. As the current log file reached the 10MB limit, the last log file is removed, the log index file for existing log files is increased, and the logging continues with a new file using the zero log index.

23.2 Managed Instance Log Files

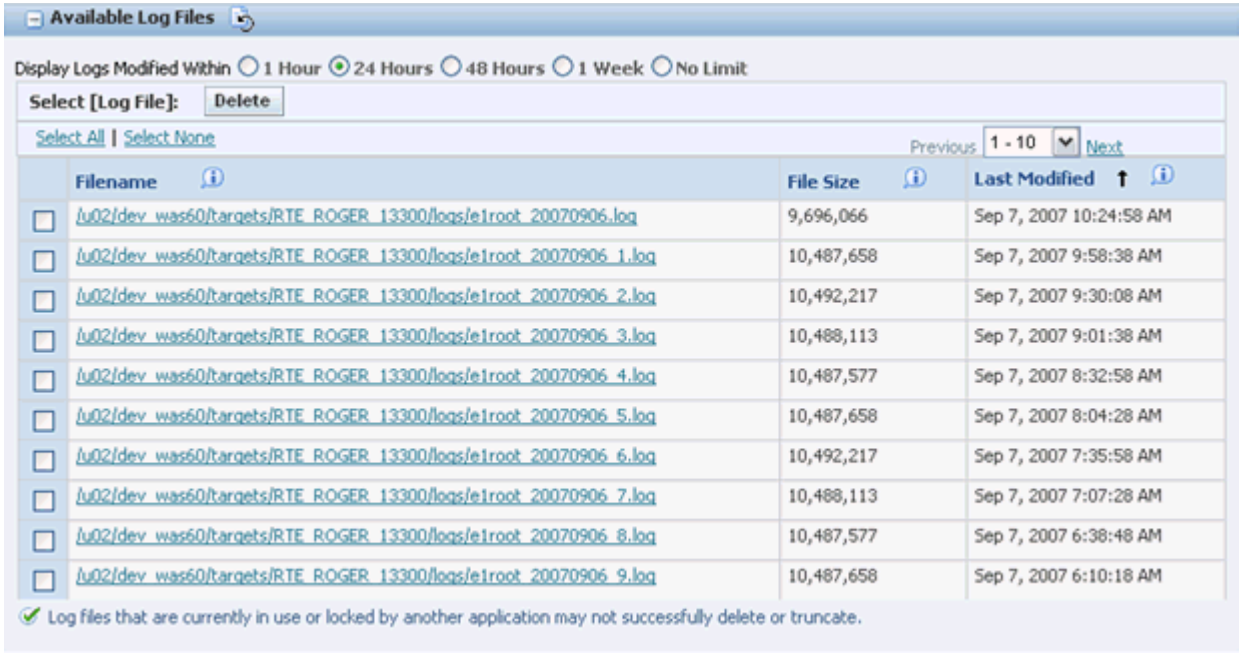
Log files for all Managed Instances, including the Management Agent, are viewable through Server Manager. Log files for the Managed Home are available by selecting the Managed Home from the Management Dashboard page. Log files for Managed Instances, including EnterpriseOne servers, Oracle application servers, and third party application servers, are available by selecting the corresponding Managed Instance anywhere throughout the Management Console. In all cases the management page contains an *Available Log Files* section.

This section describes:

- View Available Log Files
- Write Log Message [Web Products Only]
- Delete Log Files
- Log File Viewer

23.2.1 View Available Log Files

The log files for the managed instance or Managed Home are listed in a table in this section. A filter is provided to limit the list of log files based on the last time they were updated. By default only logs modified with the last 24 hours are displayed. You can use the available options to expand or narrow the subject of log files to be displayed.



- *Filename*

  The complete path and name of the log file.

- *File Size*

  The size of the log file, in bytes.

- *Last Modified*

  The date and time the log file was last modified as reported by the operating system.

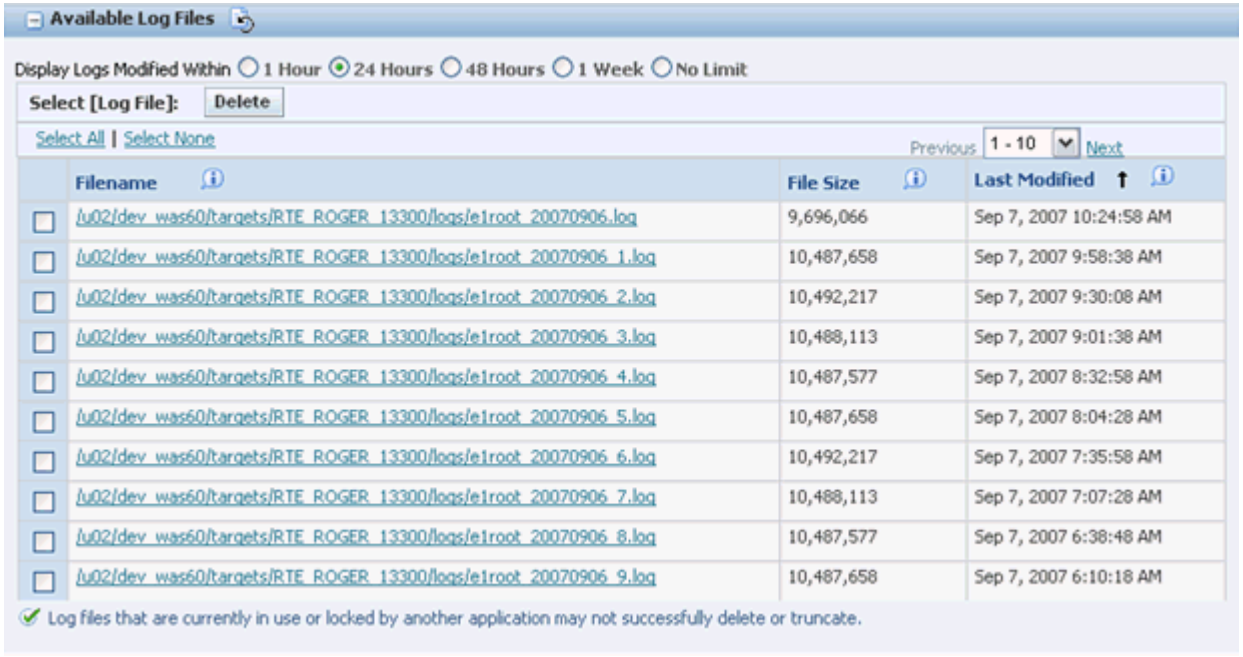
23.2.2 Write Log Message [Web Products Only]

Server Manager provides a mechanism for adding messages to the active log files. This mechanism is available only for the web-based JD Edwards EnterpriseOne servers and only when the instance is running. A free-form text message can be entered that is written to all the active log files for the Managed Instance. After entering the message, click the *Write Log Message* button to post the message to the active log files.

- *Message to Write*

  A free-form text message can be entered that is written to all the active log files for the managed instance.

23.2.3 Delete Log Files



Log files that are no longer of interested can be deleted using Server Manager. To remove a log file select the check box next to the desired log file(s) and click the *Delete* button. The selected log files are removed from the file system and no longer appear in the *Available Log Files* section.

Log files that are currently in use cannot be deleted. A warning indicates which log files cannot be deleted because they are in use.

On UNIX-based operating systems it might be possible to delete a log file while it is still in use. The file is removed from the file system and no additional log messages are written to the file.

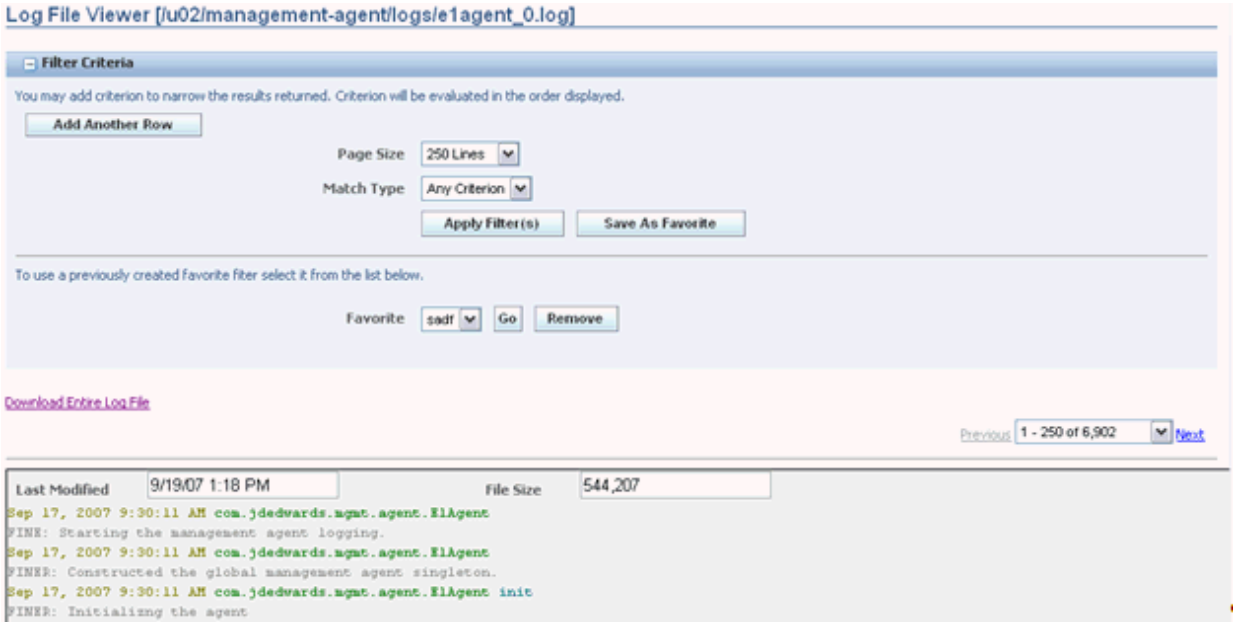
Log files should be deleted only if you are sure they are no longer needed.

23.2.4 Log File Viewer

Selecting a log file from the *Available Log Files* transfers the file to the Management Console and display the contents using the integrated log file viewer. Transferred log files are cached by the Management Console and only fetched again if the contents of the file have changed. On IBM i machines, the EBCDIC conversion is performed automatically.

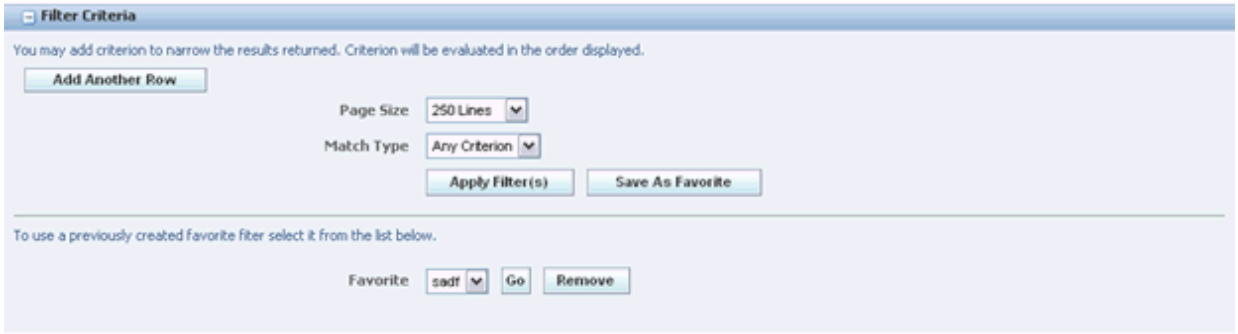
This section describes:

- Filter Log Files
- Criteria
- Apply Filter
- Save As Favorite
- Download
- Results



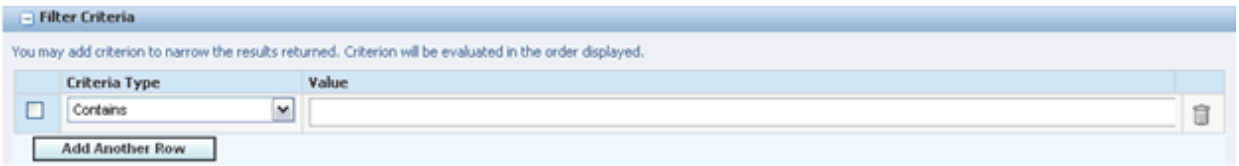
23.2.4.1 Filter Log Files

The first segment of the log file viewer is the *Filter Criteria*. Advanced filtering capabilities are provided for locating only the log entries of interest. Any number of filter criteria may be added to limit the log lines displayed. Filter criteria may be saved as a favorite for reuse at a later time.



23.2.4.2 Criteria

Criterion may be added to narrow the results that are returned. Additional rows can be added by clicking the *Add Another Row* button.



- *Criterion Type*

  The *Criterion Type* field has a dropdown list with the following filter criteria:

  Contains

  Does Not Contain

  Matches regex

Does Not Match regex

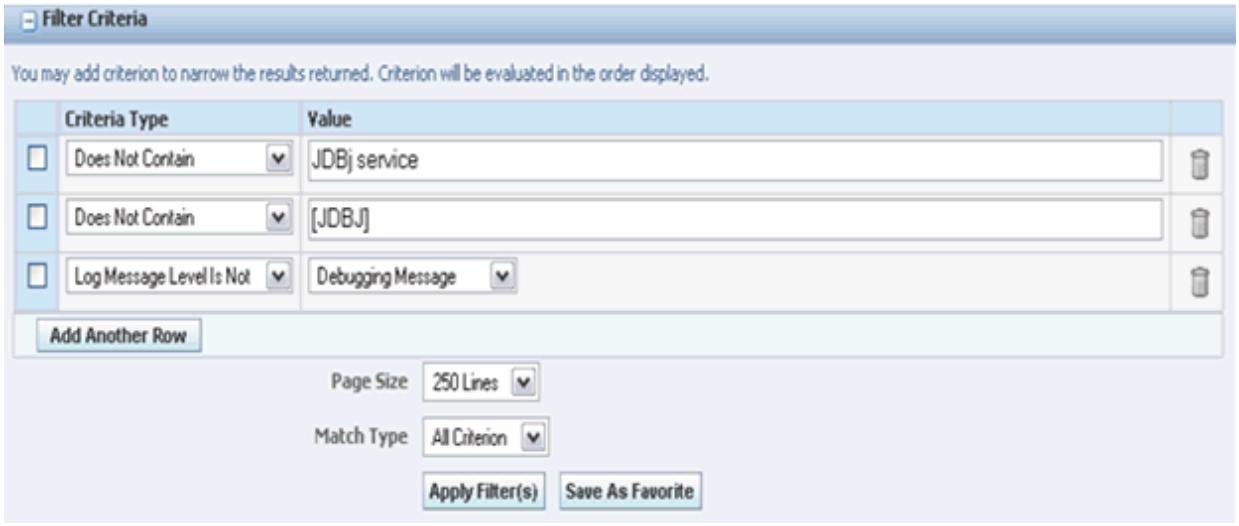
Log Level Message Is

Log Level Message Is Not

- *Value*

  The Value field is a free-form text input field.

Note: Multiple criteria are evaluated in the order listed.



23.2.4.3 Apply Filter

Available filter fields are:

- *Page Size*

  Log file contents are displayed using finite page lengths. Use this dropdown to customize the maximum number of lines that may be displayed in a single returned page. Select from these options:

  250 Lines

  500 Lines

  1000 Lines

- *Match Type*

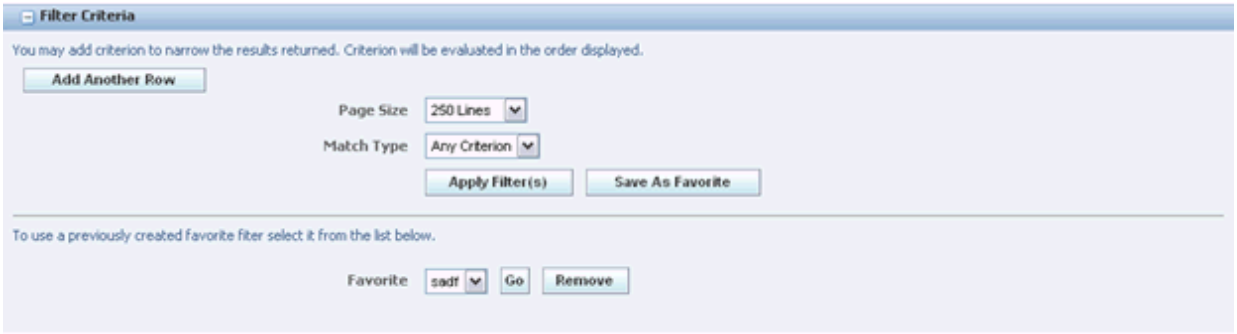
  Select how multiple criteria will be evaluated. Selecting Any Criterion returns log lines that match one or more of the supplied filter criteria. Selecting All Criterion (should be criteria, but if its that way in the software, then leave it of course) returns only those lines that match all of the supplied criteria.

After selecting the filtering preferences, click the *Apply Filter(s)* button to apply the filtering.

23.2.4.4 Save As Favorite

This section describes:

- Save a Favorite
- Run a Favorite
- Remove a Favorite



23.2.4.4.1 Save a Favorite

To save a favorite:

1. Click the *Save As Favorite* button.
2. Specify a name for the save criteria.
3. Click the *OK* button.

The favorite appears in the Favorite field drop down list for selection. These filter favorites are saved to the user account used to sign in to the management console.

23.2.4.4.2 Run a Favorite

To run a favorite:

1. Click the *Favorite* dropdown arrow.
2. Select a favorite from the list.
3. Click the *Go* button.

23.2.4.4.3 Remove a Favorite

To remove a favorite:

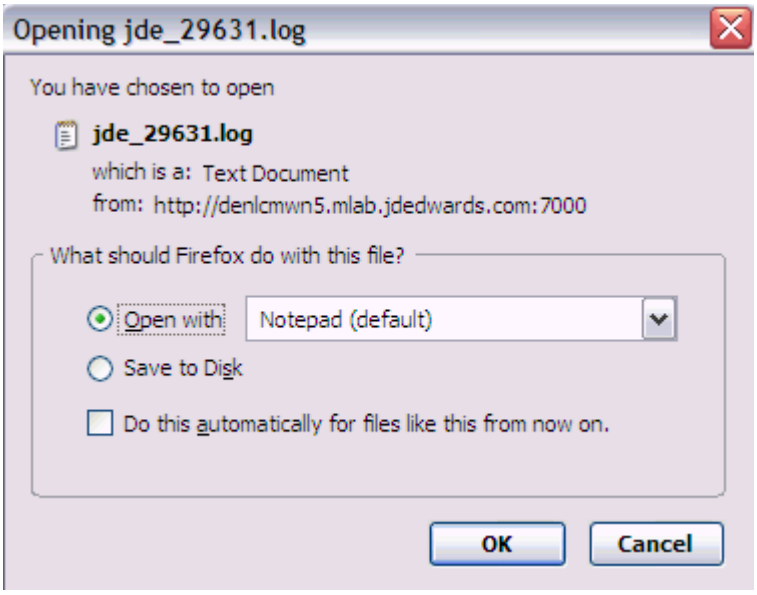
1. Click the *Favorite* dropdown arrow.
2. Select a favorite from the list.
3. Click the *Remove* button.

23.2.4.5 Download

You can download log files for viewing or parsing using other tools.

To download a log file:

1. Click the *Download Entire Log File* link or

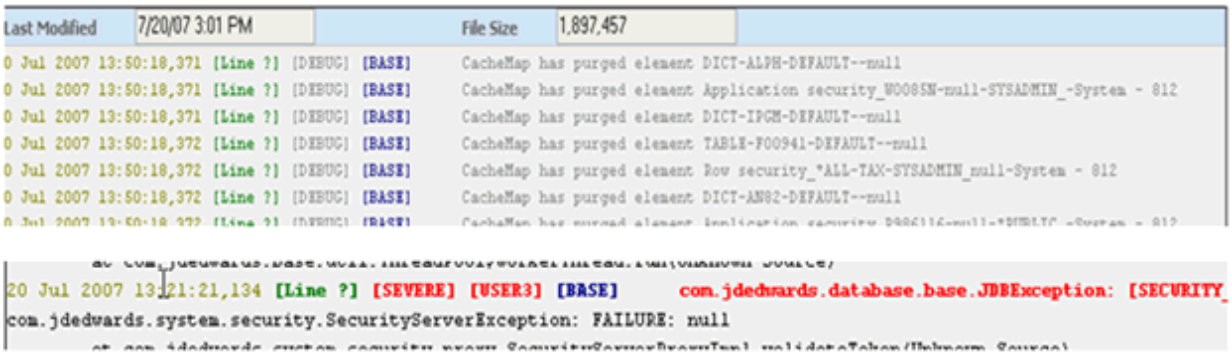


2. Select one of these options:
   - Open with
   - Save to Disk
3. Click the *OK* button.

Some very large log files might not be displayed properly within the log file viewer. If a file is too large for viewing using the integrated viewer, an appropriate message appears. You can still download these large log files for viewing with tools more suited to handling large text files.

23.2.4.6 Results

The second segment of the log file viewer is the log file. Results are color-coded and displayed in pages. EnterpriseOne log files are color coded for improved readability. The last date modified and file size information appears in the *Last Modified* and *File Size fields*.

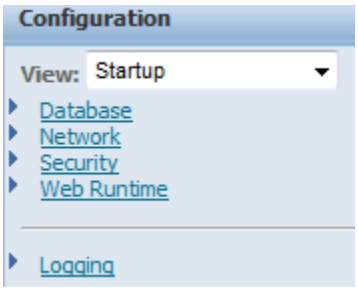


If the log file contains more lines than the current page size a dropdown appears on the upper and bottom right of the log contents. Use the dropdown or Previous/Next links to view the page of interest.

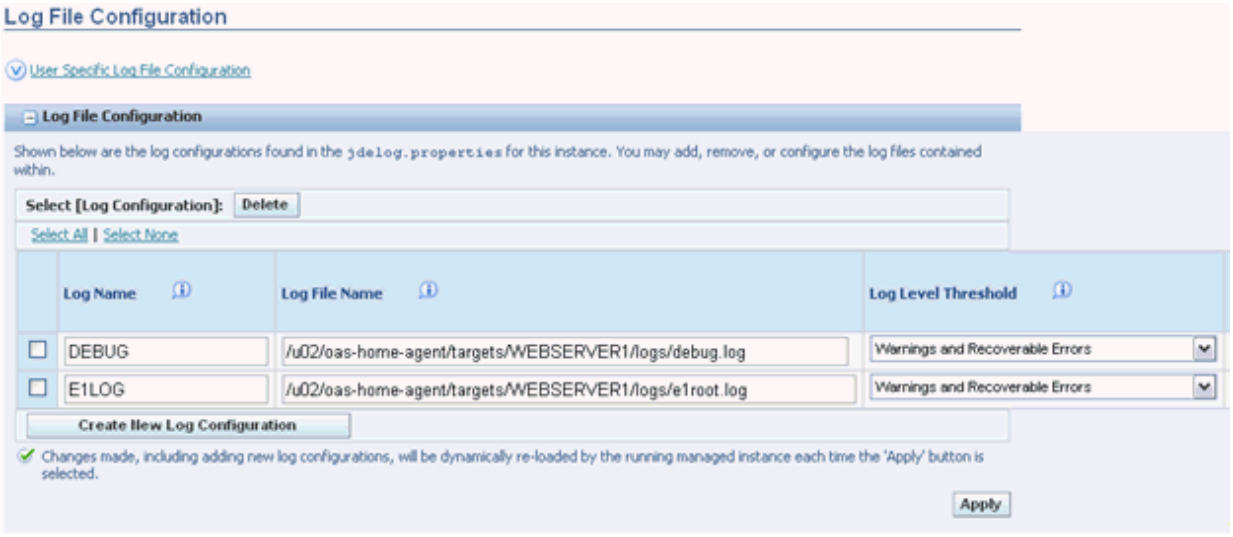
23.3 jde.properties Logging

The web based EnterpriseOne servers use the jdelog.properties file to configure their logging activity. The Java-based Enterprise Server kernels also utilize the `jdelog.properties` file to

configure their own logging activity. Server Manager provides an interface to configure these log files without having to directly modify the corresponding properties file.



From the management page for an EnterpriseOne server select the *Database* link in the *Configuration* pane. A page appears that provides details about the current configuration defined within the properties file.



Each configured log file appears as a row in the *Log File Configuration* section.

The grid fields in this section are:

- *Log Name*

  A unique identifier for this logging configuration. It is used as the section name in the jdelog.properties log configuration file.

- *Log File Name*

  The file name used to construct the actual file name. The actual log file is in the directory specified. The log file name is appended with the date the file was created and possibly the backup index of the file if the maximum size has been reached. For web products running using multiple JVMs a JVM specific identifier may also be appended to the generated log filename.

- *Log Level Threshold*

  Defines the threshold of log messages that should be written to the file. The order is Critical Errors, Warnings and Recoverable Errors, Application Level Activity, and Low Level Troubleshooting Messages (Verbose). Selecting Application Level Activity, for example, will receive all Critical Errors, Warnings and Recoverable Errors, and Application Level Activity level messages and Low Level Troubleshooting Messages (Verbose is ignored).

The available values are:

- Critical Errors
- Warnings and Recoverable Errors
- Application Level Activity
- Low Level Troubleshooting Messages (Verbose)

- *Log Format*

  There are three different formats available that differ in the amount of technical information included with each log message.

  The recommended format is Applications Format. The technical format contains the same information but adds the line number of the originating logging call. Line number information is not included in the EnterpriseOne products. Technical with Threads adds the name of the thread in which the log message originated.

- *Append Log Files*

  If TRUE, log files will append to existing log files with the same name. If FALSE, existing log files with the same name is truncated prior to writing the first log message.

- *Max. Log Size*

  This value defines the maximum size a log file may reach before it is renamed to a backup file and new log is created. The value should be specified in xxMB, where xx is a number specifying the number of Megabytes. Example: 10MB.

- *Max. Backup Index*

  The maximum number of backup files to retain. When a log file reaches the maximum allowed file size it is archived to another log file. This value specifies the maximum number of those backup entries to keep.

- *Log Components*

  Specifies the components within the EnterpriseOne product to log. You may specify ALL or the individual components (such as Runtime, JDBJ, etc.) that should be logged.

23.3.1 Remove Log Definitions

You can delete the log file definition by selecting the check box in the desired row and clicking the *Delete* button.

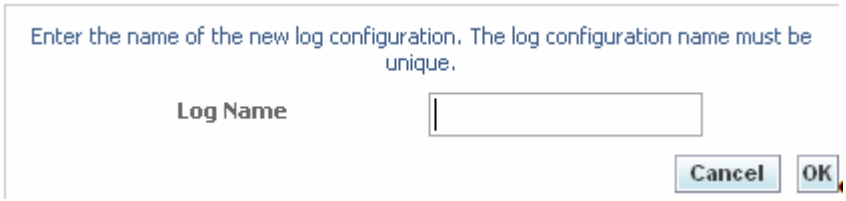
23.3.2 Apply Changes

After making changes, click the *Apply* button to save any modifications. Changes including adding new log configurations are dynamically re-loaded by the running managed instance each time the *Apply* button is selected.

For the web-based server products adding, modifying, or removing log files takes effect immediately after pressing *Apply* if the corresponding server is running. Java based enterprise server kernels will take up the modifications the next time the server is started.

23.3.3 New Log Configuration

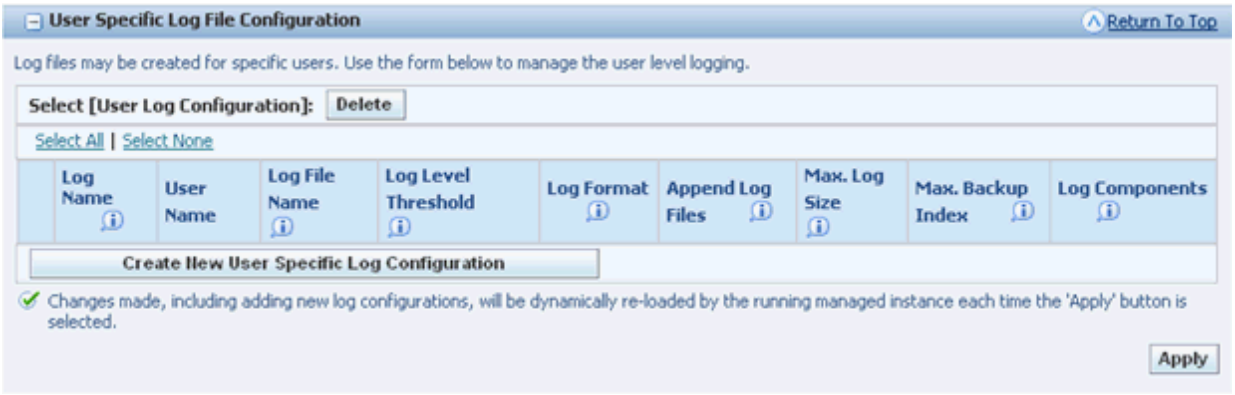
New log definitions may be created by selecting the *Create New Log Configuration* button. The application prompts for a name for the new definition. The supplied name contains only characters and must not already be used by an existing log configuration. Select *OK* to create the new definition.



Server Manager creates a new log definition using default values based on the E1LOG definition, if present. The log file path is created based on the log definition name supplied. You can change any of the default values created just as you would modify any of the log configurations.

23.3.4 User Specific Log File Configuration

The JD Edwards EnterpriseOne HTML Web Server supports user-specific log definitions. Any activity by the configured user is logged to the corresponding file as configured. Creating and modifying a user-specific log definition is nearly identical to creating a regular log definition.



23.3.5 Create New User Specific Log File Configuration

Rather than prompt for the name of the log definition the application prompts for the user name instead.

24

Install an Oracle Configuration Manager (OCM) Instance

This chapter discusses:

- Section 24.1, "Overview"
- Section 24.2, "Prerequisites"
- Section 24.3, "Oracle Configuration Manager Manual Install"
- Section 24.4, "Oracle Configuration Manager Install Using Server Manager"

24.1 Overview

Oracle Configuration Manager is an Oracle product that is used to collect data about your JD Edwards EnterpriseOne configuration and upload the data to a central repository at the Oracle site. It comes as part of Server Manager and can be installed and accessed from the Management Console in Server Manager.

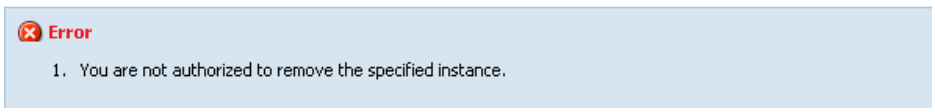
Oracle Configuration Manager is included as part of the Management Agent installation. However, you must complete the installation by registering each Oracle Configuration Manager instance using your Oracle customer ID and MetaLink ID Number.

The Oracle Configuration Manager installation provides you with the option to set up a proxy server to use for communication between Oracle Configuration Manager and Oracle. If a proxy server is used to connect to the Internet, the proxy connection details must be supplied to Oracle Configuration Manager as part of the installation procedure.

Oracle Configuration Manager can be installed only on Microsoft Windows and Unix platforms; you cannot install Oracle Configuration Manager on IBM i.

Note: Oracle Configuration Manager can be installed only by Oracle customers who have an Oracle Customer ID and an ID for My Oracle Support.

Note: You cannot remove an OCM instance. If you attempt to do so, the Management Console displays this error:



See Chapter 25, "Administer Oracle Configuration Manager (OCM)" for more information about Oracle Configuration Manager.

24.2 Prerequisites

Before you can install Oracle Configuration Manager on a managed home, you must:

- Have an Oracle Customer Identification Number and Oracle MetaLink-ID Number.

  Note: JD Edwards EnterpriseOne customers who do not use Oracle database or application software cannot install Oracle Configuration Manager.

- Install a managed home.

24.3 Oracle Configuration Manager Manual Install

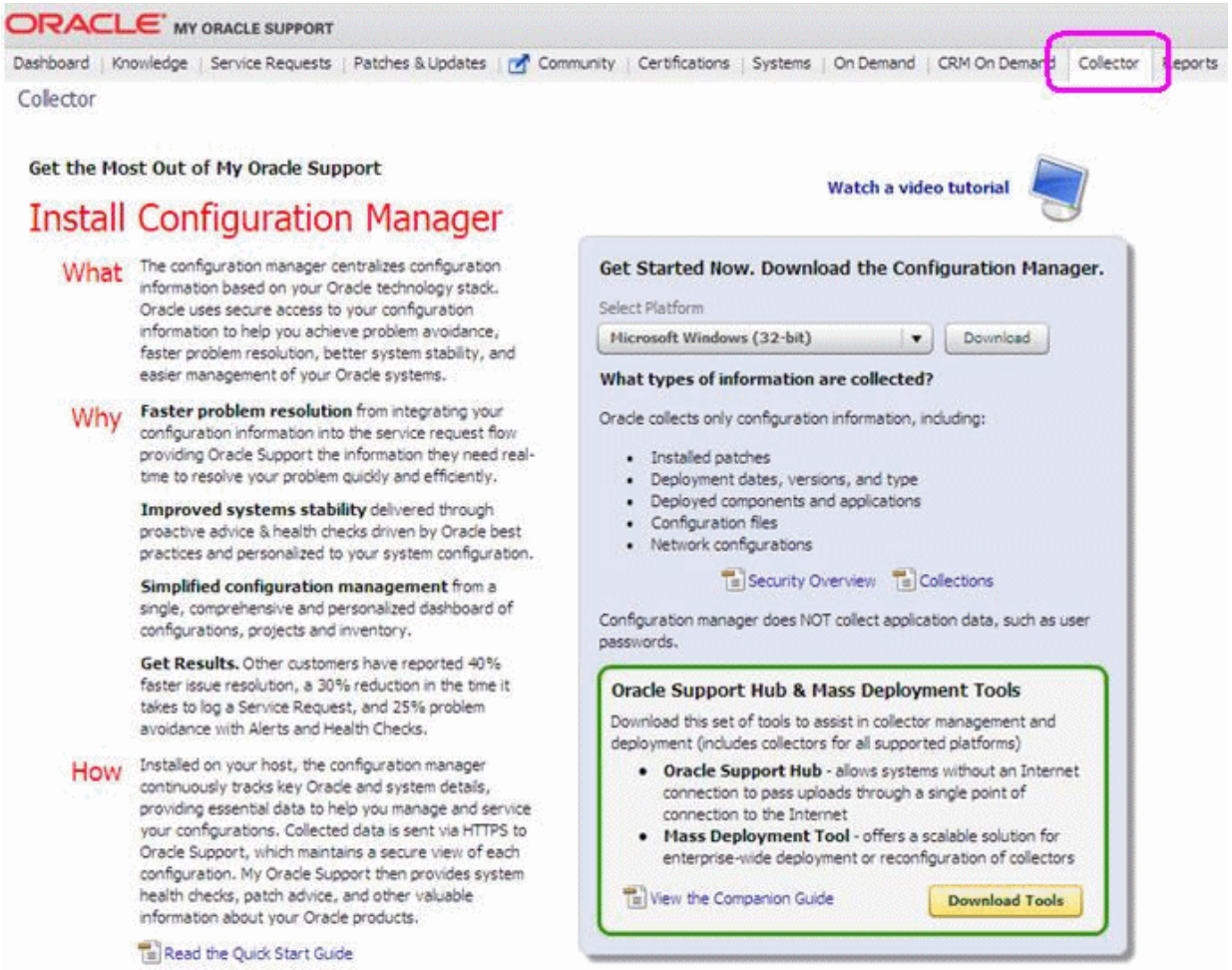
For Existing Installations of Server Manager. If previous to JD Edwards Enterprise Release 8.98.4 you have used Server Manager to install Oracle Configuration Manager, you must use the procedure in this section to manually deinstall your existing down-level version. Once the down-level OCM is deinstalled as described in this section, you can manually install the latest version as described in this section, or optionally you can install it using Server Manager as described in the next section of this guide entitled: Oracle Configuration Manager Install Using Server Manager.

For New Installations of Server Manager. The current release of Server Manager includes the current release of Oracle Configuration Manager. As a result, you must install Oracle Configuration Manager from Server Manager as described in the next section of this guide entitled: Oracle Configuration Manager Install Using Server Manager.

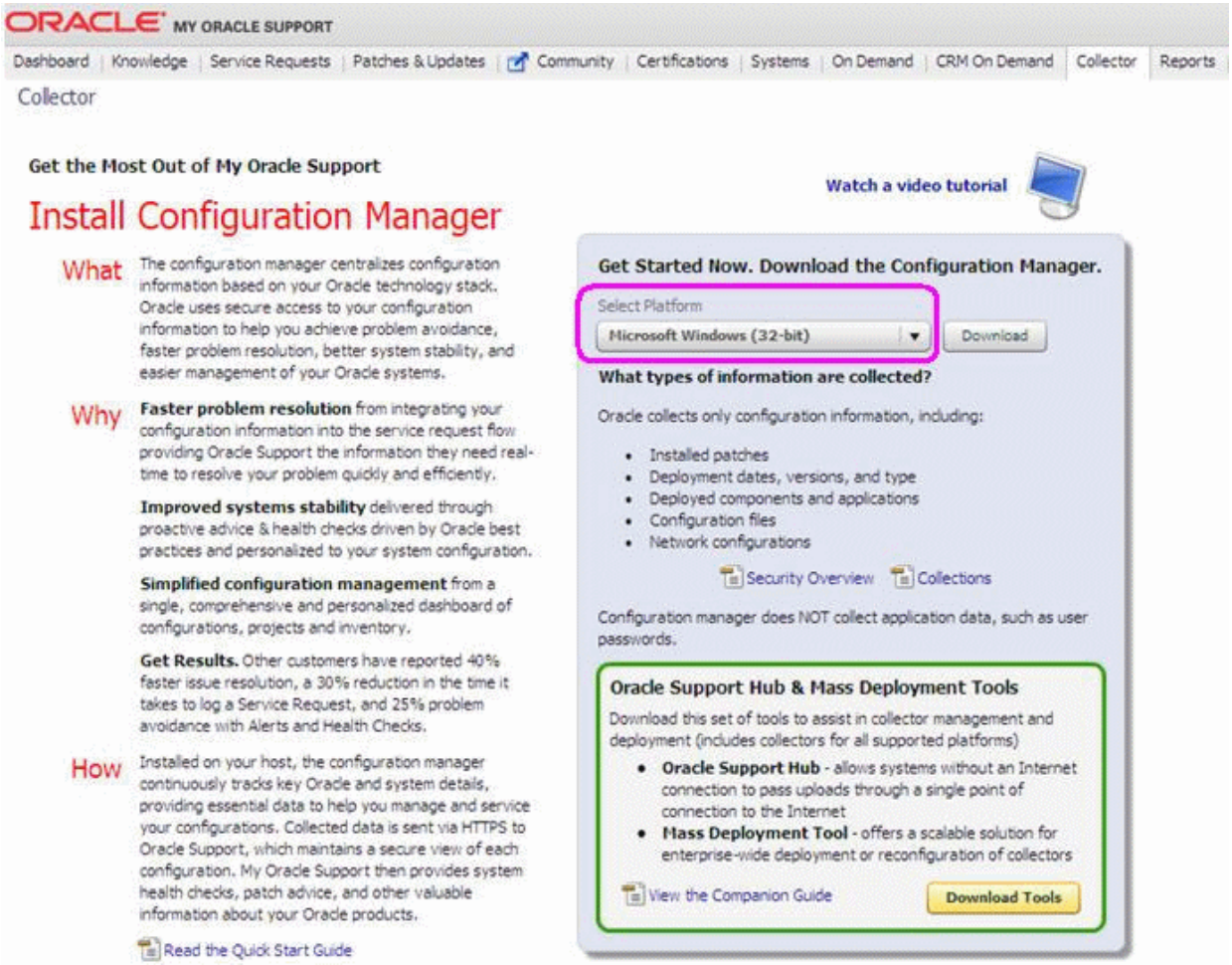
To install Oracle Configuration Manager:

1. Navigate to My Oracle Support:

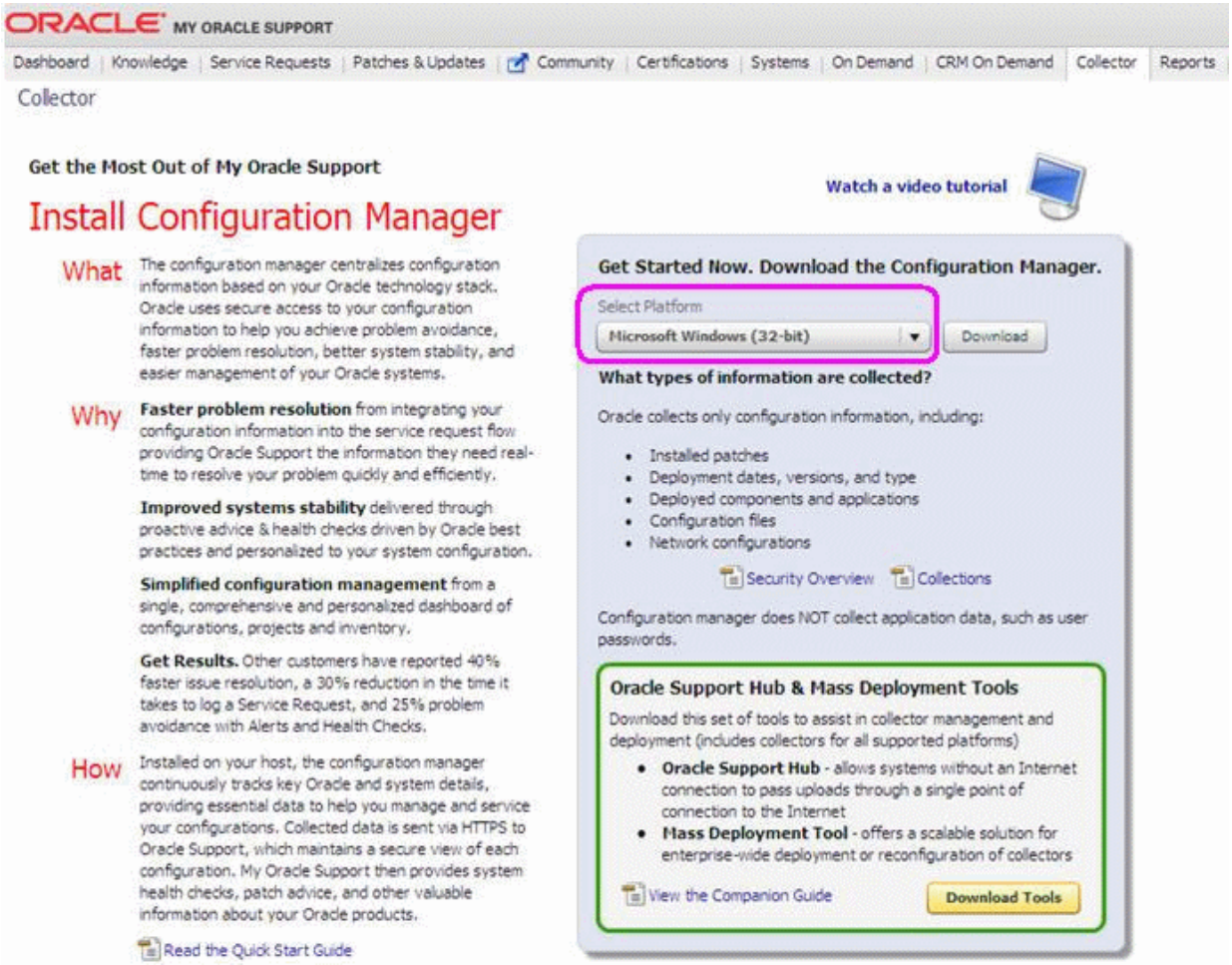
   `https://support.oracle.com`



2. On My Oracle Support, select the *Collector* tab.



3. On Install Configuration Manager, in the pane for Get Started Now, select the platform on which the Oracle Configuration Manager will be installed. Typically this is your JD Edwards EnterpriseOne Deployment Server, which must run on a Microsoft Windows (32-bit) machine.



4. Once you have selected the platform, click the *Download* button.
5. On your Server Manager machine, navigate to the folder where Server Manager Agent is installed. For example:

   ```
   C:\JDE_HOME
   ```

   Note: If OCM (also called CCR at the code level) has never been installed, only put in place by a Server Manager Agent install, you can skip to Step 9.

6. If Oracle Configuration Manager is running, navigate to the CCR bin folder. For example:

   ```
   C:\JDE_HOME\ccr\bin
   ```

7. Run this command to stop the Oracle Configuration Manager (CCR):

   ```
   emCCR stop
   ```

8. Once stopped, you must uninstall Oracle Configuration Manager (CCR) using this command:

   ```
   configCCR -r
   ```

9. Delete this folder:

   ```
   ccr
   ```

10. Extract downloaded zip file into agent folder:

```
C:\JDE_HOME
```

This extracts a `ccr` folder and `Readme.txt` into the Server Manager Agent installation folder.

Note: You can install the downloaded Oracle Configuration Manager (CCR) manually using the following step. Alternatively, you can install CCR from Server Manager Console. For the later method, refer to the next section in this chapter entitled: Oracle Configuration Manager Install Using Server Manager

---

11. Navigate to the `ccr\bin` folder. For example:

```
C:\JDE_HOME\ccr\bin
```

12. Run this command to manually install the Oracle Configuration Manager (CCR):

```
setupCCR -s Customer_Identification_Number MetaLink_ID Country_Code
```

Note: You must supply valid values in place for the `Customer_Identification_Number` and `MetaLink_ID` parameters. The parameter for `Country_Code` is optional.

The `-s` option in the command indicates acceptance of the license agreement found at this link:

`http://www.oracle.com/support/policies.html`

See Administer Oracle Configuration Manager (OCM) for more information about log files and Oracle Configuration Manager configuration settings.

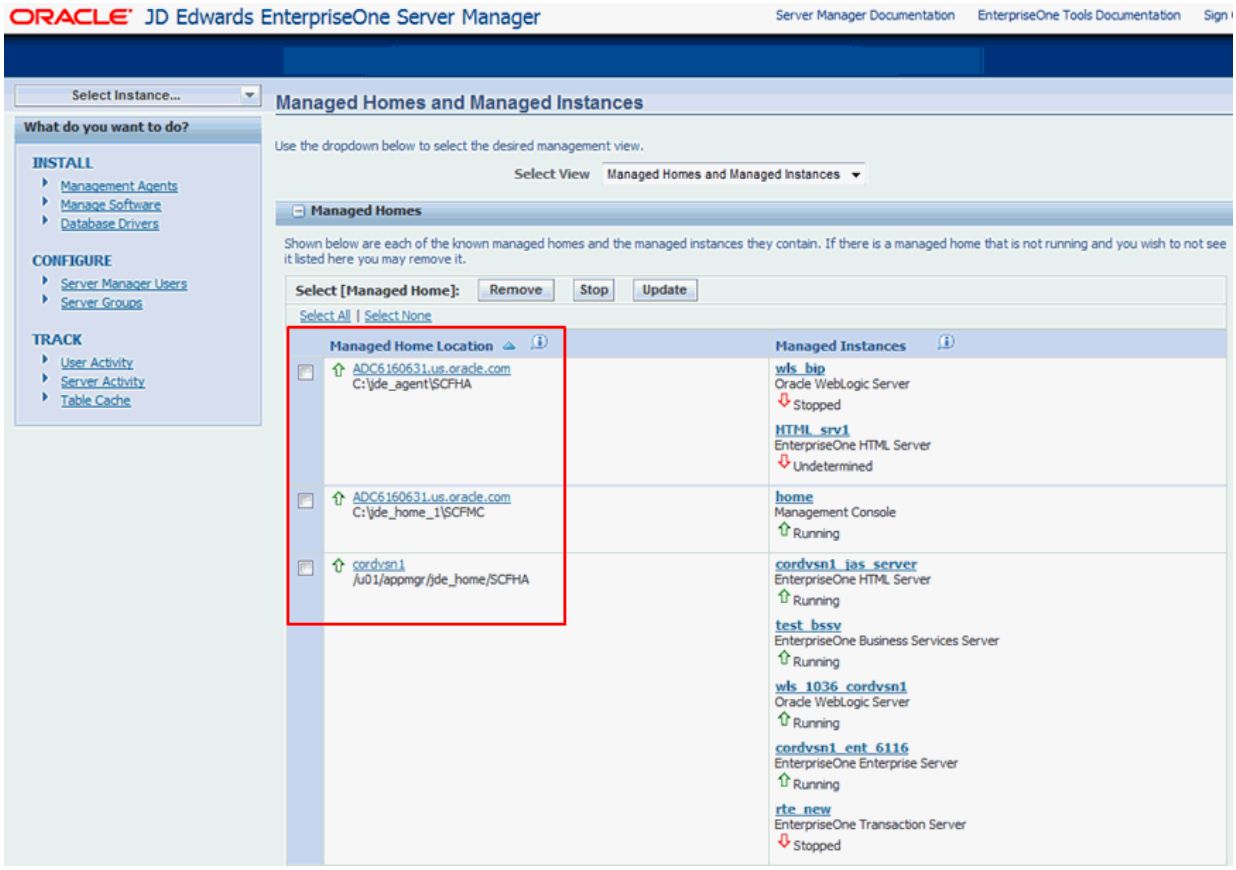
24.4 Oracle Configuration Manager Install Using Server Manager

For Existing Installations of Server Manager. If previous to JD Edwards Enterprise Release 8.98.4 you have installed OCM using Server Manager, you must use the procedure in the previous section of this guide to manually deinstall your existing down-level version. Once the down-level OCM is deinstalled as described in this section, you can manually install the latest version as described in the previous section, or optionally you can install it using Server Manager as described in this section.

For New Installations of Server Manager. The current release of Server Manager includes the current release of Oracle Configuration Manager. As a result, you must install Oracle Configuration Manager from Server Manager as described in this section.

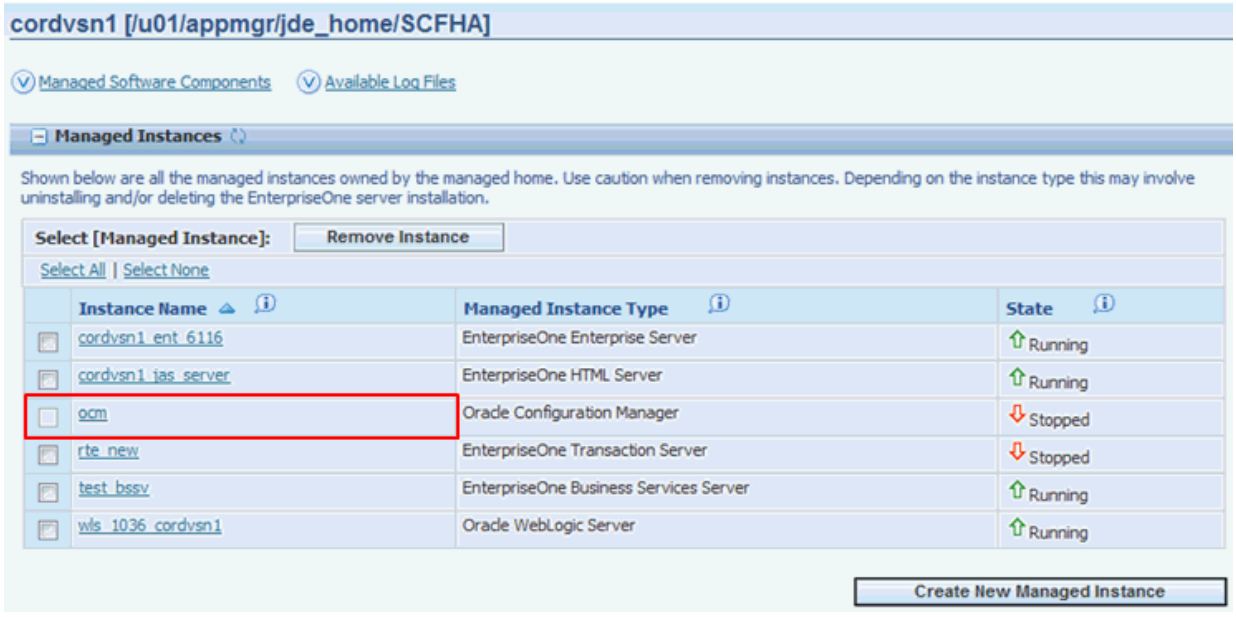
To install Oracle Configuration Manager:

1. In the Management Console, select the managed home location where you want to install Oracle Configuration Manager.



2. Select the “ocm” link in the instance.

Note: You can also click a managed home link on the Management Console home page and install the Oracle Configuration Manager (ocm) instance from the managed home location.

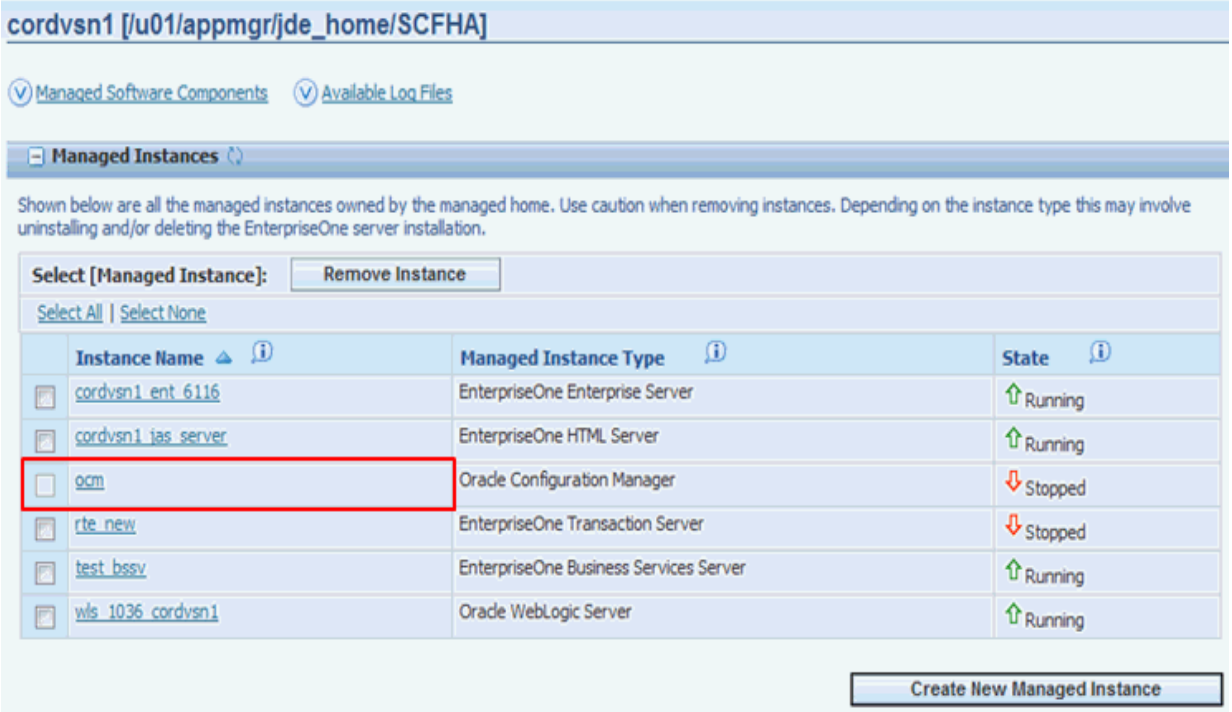


The Oracle Configuration Manager Instances page shows each Oracle Configuration Manager instance, the managed home it resides on, and the status of each instance, which include:

- Running. The ocm instance is installed.
- Stopped. The ocm instance is not installed.
- Undetermined. Cannot install due to incompatibility with the managed home platform.

3. In the Management Console, select the managed home location where you want to install Oracle Configuration Manager click the *Oracle Configuration Manager* link in the *Quick Links* section.

Note: You can also click a managed home link on the Management Console home page and install the Oracle Configuration Manager (ocm) instance from the managed home location.



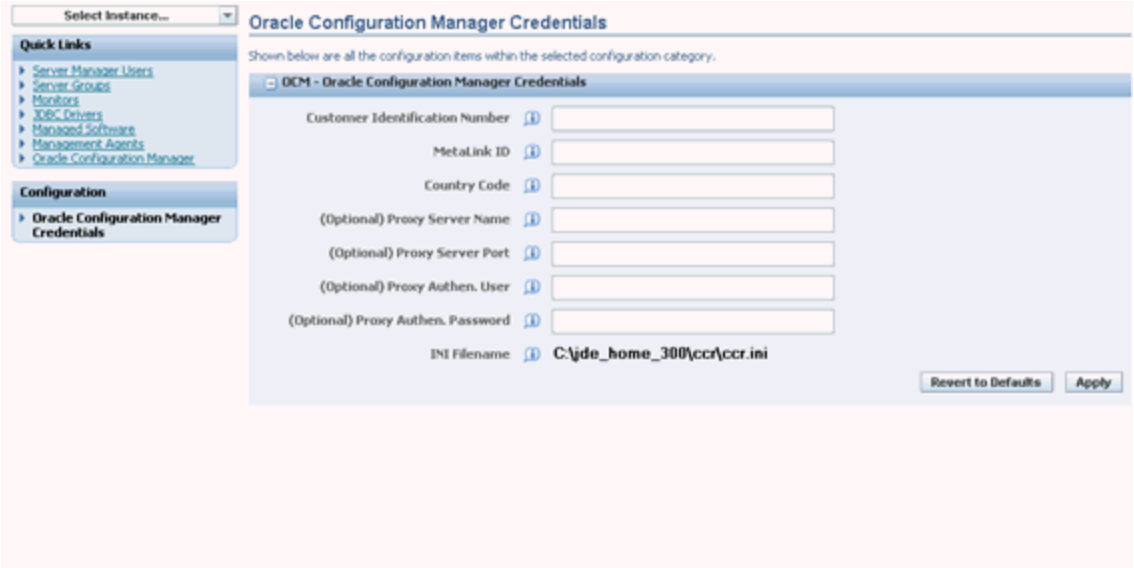
The Oracle Configuration Manager Instances page shows each Oracle Configuration Manager instance, the managed home it resides on, and the status of each instance, which include:

- Running. The ocm instance is installed.
- Stopped. The ocm instance is not installed.
- Undetermined. Cannot install due to incompatibility with the managed home platform.

4. In the License agreement section, click the *Oracle Configuration Manager License Agreement* link to read the license agreement and then click the *Accept License Agreement* option to proceed.

   If you click the Decline License Agreement option, you cannot proceed with the installation.

5. In the Configuration section, click the *Oracle Configuration Manager Credentials* link.

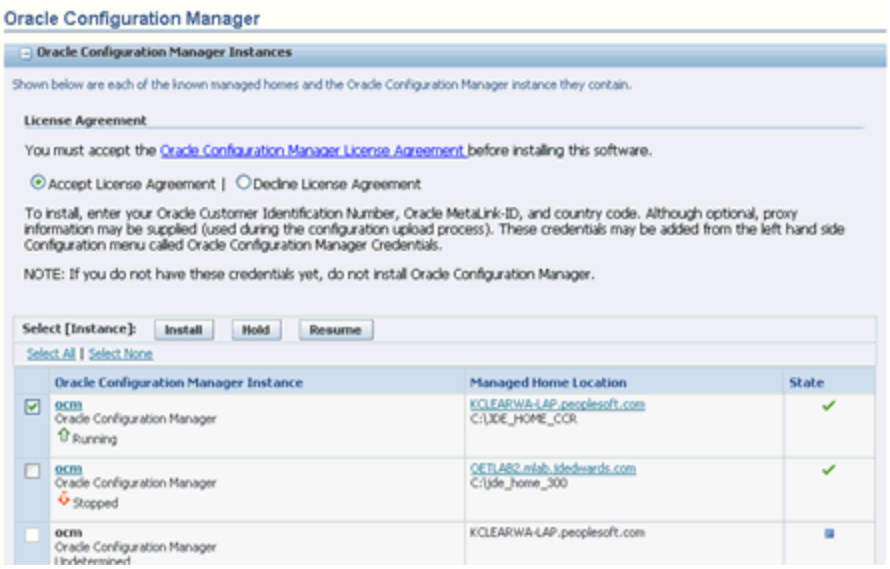


6. In the OCM Oracle Configuration Manager Credentials section, complete these fields and then click the *Apply* button:

   - Customer Identification Number
   - MetaLink ID
   - Country Code
   - (Optional) Proxy Server Name
   - (Optional) Proxy Server Port
   - (Optional) Proxy Authen. User
   - (Optional) Proxy Authe. Password
   - INI Filename. The system displays the physical file location where the credential information is stored. Sensitive data is encrypted.

     You can click the Revert to Defaults button if you are modifying these fields and want to return to the original values that you entered.

     Note: If a proxy server is used to connect to the Internet, you must complete the proxy connection fields.



7. Click the check box next to the ocm instance that you want to install. You can install an Oracle Configuration Manager instance on multiple managed homes at the same time by clicking additional check boxes

   Note: If the status below the ocm link is Undetermined, you cannot install an Oracle Configuration Manager instance due to an incompatibility with the platform of the managed home, or if the managed home is down.

8. Click the Install button. Once Oracle Configuration Manager is installed, the status below the ocm link changes to Running.

   The Management Console verifies the credentials that you entered and automatically downloads the latest Oracle Configuration Manager from Oracle. If necessary, it runs its first collection and sends the data to the Oracle repository.

9. Click the ocm link of an instance that is running to view additional information about the Oracle Configuration Manager instance, such as status, log file settings, and so on.

   See Administer Oracle Configuration Manager (OCM) for more information about log files and Oracle Configuration Manager configuration settings.

25

Administer Oracle Configuration Manager (OCM)

This chapter discusses:

- Section 25.1, "Overview of Oracle Configuration Manager"
- Section 25.2, "Secure Communication Through Oracle Configuration Manager"
- Section 25.3, "Data Collected by Oracle Configuration Manager"
- Section 25.4, "Prerequisite"
- Section 25.5, "Check the Status of Oracle Configuration Manager"
- Section 25.6, "Test the Connection to Oracle"
- Section 25.7, "Modify the Collection Interval Settings"
- Section 25.8, "Run a Manual Collection"
- Section 25.9, "Hold or Resume Oracle Configuration Manager on a Managed Home"
- Section 25.10, "View Configuration Data and Log Files"
- Section 25.11, "Manually Download Updates to Oracle Configuration Manager"
- Section 25.12, "Examples of Data Collected by Oracle Configuration Manager"

25.1 Overview of Oracle Configuration Manager

Oracle Configuration Manager is an Oracle product that is used to collect data about your JD Edwards EnterpriseOne configuration and upload the data to a central repository at the Oracle site. When configuration data is uploaded on a regular basis, support analysts can analyze this data and provide better service to customers.

Some of the benefits of Oracle Configuration Manager include:

- Reduced time for resolution of support issues
- Proactive problem avoidance
- Improved access to best practices and the Oracle knowledge base
- A better understanding of customers business needs and a mechanism to help provide consistent responses and services

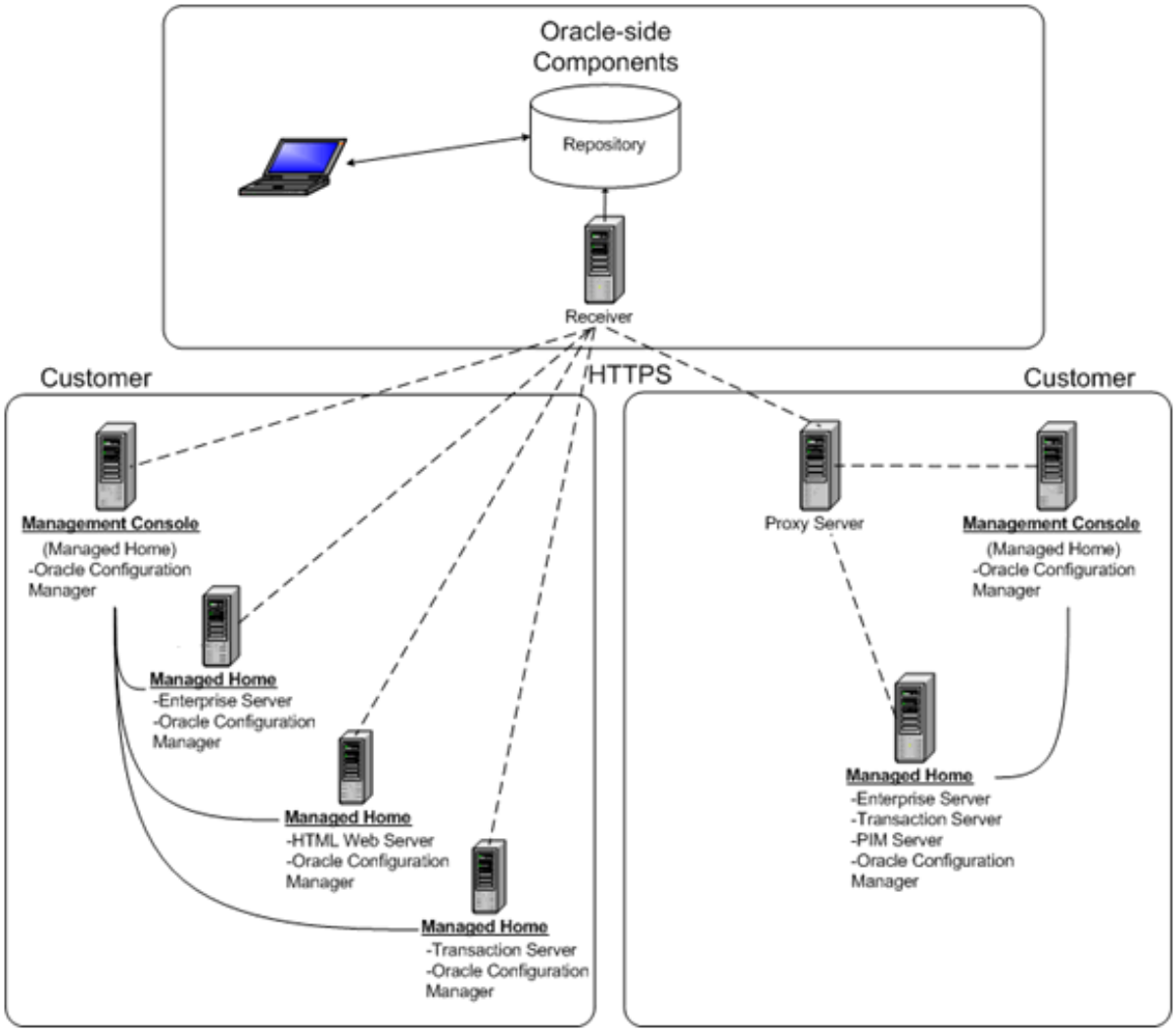
Oracle Configuration Manager comes as part of Server Manager and can be installed and accessed from the Management Console in Server Manager. The EnterpriseOne Management Console is the central hub for installing, configuring, and administering JD Edwards

EnterpriseOne components, such as the HTML Web Server, transaction server, PIM server, and so forth.

25.1.1 How Oracle Configuration Manager Works

Oracle Configuration Manager consists of both customer-side and Oracle-side components. The customer-side components collect the configuration data from each managed home and send the data to Oracle. The Oracle-side components receive the configuration data and store it in a central repository from which Oracle support staff can view the data.

The following diagram is a high-level depiction of the Oracle Configuration Manager architecture, with two different customer configurations: one that connects directly to the Internet and another that uses a proxy server to connect to the Internet:



Oracle Configuration Manager architecture

25.1.1.1 Customer-Side Components

The JD Edwards EnterpriseOne Management Console on the customer side provides the interface through which you can install and administer Oracle Configuration Manager on each managed home. Likewise, the JD Edwards EnterpriseOne Management Console is also a

managed home and you can install an instance of Oracle Configuration Manager on the Management Console managed home as well.

On each managed home, Oracle Configuration Manager uses a script to create a target list of components on the managed home and then collects data based on the target list. For example, a managed home might contain two JD Edwards EnterpriseOne components, a transaction server and an HTML web server. Oracle Configuration Manager collects data regarding the configuration of these components, houses the data in a collection, and then automatically uploads the collection to the Oracle repository.

A scheduling service (or daemon on UNIX platforms) determines how often collections are made on the managed home. The scheduling service uses default interval settings set by Oracle to determine when collections are made. However, you can modify the interval settings to a time that will minimize or alleviate any disruption in system performance. The scheduling service automatically starts when the host machine is restarted. You can use the administration tools on your operating system to start or stop this service. You can also use the EnterpriseOne Management Console to place an instance of Oracle Configuration Manager on hold or resume it.

Oracle Configuration Manager updates the collection only if the configuration on the managed home has been modified. Before a collection is created, Oracle Configuration Manager performs a delta process that updates the target list to reflect the current state of the managed home. If there are no changes to the target list, the collection is not updated.

25.1.1.2 Oracle-Side Components

The Oracle-side components authenticate and collect data received from each Oracle Configuration Manager on a customer site. Oracle stores the configuration data in a repository.

In addition, when receiving data, a component on the Oracle side checks the version of the Oracle Configuration Manager that it is receiving data from and automatically sends software updates to Oracle Configuration Manager if available. If you prefer, you can disable automatic updates and download updates manually.

25.2 Secure Communication Through Oracle Configuration Manager

Oracle Configuration Manager uses the features of the Secure Socket Layer (SSL) and makes use of HTTPS for all Oracle-side component communications.

25.2.1 Direct Access to the Internet

The Oracle-side components are exposed by way of a website. This website has a certificate that can be validated so that the customer-side component can ensure that it is communicating with Oracle. If you have direct connectivity to the Internet from your machine, no additional configuration is required.

25.2.2 Access Through a Proxy Server to the Internet

If a proxy server is used to connect to the Internet, the proxy connection details must be supplied to Oracle Configuration Manager as part of the installation procedure.

One potential way of determining these parameters is looking at the settings in your local web browser. This may or may not be the same for the server that you are configuring for Oracle Configuration Manager. To view these settings in Internet Explorer, go to Tools, Internet Options, Connections, LAN Settings, Advanced.

See Install an Oracle Configuration Manager (OCM) Instance for information about how to install Oracle Configuration Manager with a proxy server.

25.2.3 Automatic Updates

During its initial contact with Oracle, Oracle Configuration Manager uses HTTPS and will interrogate the Oracle-side server certificate to make sure that it is communicating with Oracle. When the connection is made, Oracle Configuration Manager downloads digitally signed JAR files. When the JAR files reside on the customer machine, Oracle Configuration Manager verifies the digital signature of the JAR file to ensure that it has been signed by Oracle and that the contents have not been altered. If the verification succeeds, Oracle Configuration Manager deploys the update.

25.3 Data Collected by Oracle Configuration Manager

Oracle Configuration Manager places configuration data in xml files and creates log files that provide information about the collection process. You can view all data that is collected and sent to Oracle by accessing the xml files in the Management Console.

Oracle Configuration Manager collects the following system level data about each managed home:

- The machine name of the managed home
- Oracle software that is installed on the machine, including all JD Edwards EnterpriseOne components
- jde.ini file settings
- jas.ini file settings
- jdbj.ini file settings
- A list of other non-JD Edwards EnterpriseOne components on each managed home.

The following table lists the configuration data that Oracle Configuration Manager collects from each component of a JD Edwards EnterpriseOne configuration:

Component	Configuration Data
EnterpriseOneConfiguration	Path codes
	Environments
	Datasource definitions
	Machine key
	Updates
	Note: A management agent must be installed on your deployment server to obtain this data. If the Management Console is not installed on the deployment server, you must install a separate management agent to obtain this data.
EnterpriseOneManagement Console	Management Console attributes
	Managed homes
	Managed instances
EnterpriseOneManaged Home	Managed homeattributes
	Managed home managed instances

Component	Configuration Data
EnterpriseOne WebServer (JAS)	Web server(JAS) attributes
	Web server (JAS) JAS.INI
	Web Server (JAS) JDBJ.INI
EnterpriseOneEnterprise Server	EnterpriseOne enterprise server attributes
	EnterpriseOne enterprise server JDE.INI
EnterpriseOne PIMSynch Server	EnterpriseOnePIM Synch Server attributes
	EnterpriseOne PIM Synch Server JAS.INI
	EnterpriseOne PIM Synch Server JDBJ.INI
EnterpriseOneTransaction Server	EnterpriseOne Transaction Server attributes
	EnterpriseOne Transaction Server JAS.INI
	EnterpriseOne Transaction Server JDBJ.INI
EnterpriseOneCollaborative Portal	EnterpriseOne Collaborative Portal attributes
	JAS.INI
	JDBJ.INI
	JDE.INI

This table contains a list of the files generated by Oracle Configuration Manager and a description of the contents of each file:

File	Description
Sched.log	Contains information about the scheduling process activities alongwith information about errors.
Collector.log	Contains information about collection activities along withinformation about errors.
Config.xml	Contains the raw host configuration data. Oracle ConfigurationManager generates an xml file for each target type and then sends theinformation to Oracle. You can directly view the configuration data in thisfile.
targetMap.xml	Lists the targets found through discovery process.
Upgrade.log	Contains information regarding upgrade activities, including anyerrors.

See Examples of Data Collected by Oracle Configuration Manager

25.4 Prerequisite

Install Oracle Configuration Manager on each managed home. See Install an Oracle Configuration Manager (OCM) Instance

Note: Oracle Configuration Manager is not compatible with IBM i platforms, including enterprise and application servers. For each managed home on IBM i, the check box and link for the OCM install are disabled. The EnterpriseOne Management Console provides a list of the components installed on IBM i, but it does not provide information about the settings or configuration for each component.

25.5 Check the Status of Oracle Configuration Manager

You can view information about the status and state of each Oracle Configuration Manager instance on a managed home. Statuses include:

- Running. Indicates that Oracle Configuration Manager is installed and running on the managed home.
- Stopped. Indicates that Oracle Configuration Manager is not installed.
- Undetermined. Indicates that Oracle Configuration Manager cannot be installed on the managed home due to an incompatibility with the platform of the managed home. This can also indicate that the managed home is down.

The state provides further details about an installed Oracle Configuration Manager instance, such as the date and time of the next scheduled collection and the collection interval frequency.

To check the status of Oracle Configuration Manager:

1. In the Quick Links section of the Management Console, click the Oracle Configuration Manager link.

   The Oracle Configuration Manager Instance column displays the status of each instance under the ocm link.

   Note: You can only check the state of Oracle Configuration Manager if the ocm link is active; that is the status is stopped or running. If the status is Undetermined (uninstalled), information about its state is unavailable.

2. Click the ocm link of the managed home to view details about its state.

   The Oracle Configuration Manager page for that instance appears and displays information about its state in the Overview section.

3. Alternatively, you can access an Oracle Configuration Manager instance from the Management Dashboard home page. If you know the managed home location of the instance that you want to access, click the link of the managed home location, and then click the ocm link on the managed home page.

25.6 Test the Connection to Oracle

You can test the Oracle Configuration Manager connection to the Oracle-side components to ensure the proper transfer of configuration data.

To test the connection to Oracle:

1. Access the Oracle Configuration Manager on the managed home for which you want to test the connection.
2. On the Oracle Configuration Manager: ocm page, click the Operations link at the top of the page or scroll down to the Test Connection section, and then click the Test Connection button.

   The system displays a detailed message about the connection and states whether the connection was successful.

25.7 Modify the Collection Interval Settings

The collection interval settings in the Oracle Configuration Manager scheduling service determine how often collections are made. By default, the scheduling service is set to generate

collections on a daily basis. If you prefer, you can modify the interval settings. However, Oracle recommends that collections occur daily.

To modify the collection interval settings:

1. In the Quick Links section of the Management Dashboard, click the Oracle Configuration Manager link.
2. On the Oracle Configuration Manager page, click the ocm link of the managed home location in which you want to modify the collection interval.
3. On the Oracle Configuration Manager: ocm page, click the Settings link, or scroll down to the Settings section.
4. In the Settings section, complete these fields under the Set Collection Interval heading:
   - Frequency. Settings include Daily, Weekly, Monthly. If you select Weekly, then select a day in the By Day field. If you select Monthly, then select a day in the By Month Day field.
   - By Day
   - By Month Day
   - By Hour
   - By Minute

25.8 Run a Manual Collection

You can manually generate a collection of configuration data in Oracle Configuration Manager. After the data is collected, Oracle Configuration Manager automatically uploads the configuration data to the Oracle repository.

To run a manual collection:

1. In the Quick Links section on the Management Dashboard home page, click the Oracle Configuration Manager link.
2. On the Oracle Configuration Manager page, click the ocm link for the managed home location on which you want to run a manual collection.
3. On the Oracle Configuration Manager: ocm page, click the Operations link, or scroll down to the Operations section.
4. Click the Collect button.

25.9 Hold or Resume Oracle Configuration Manager on a Managed Home

You can place an instance of Oracle Configuration Manager on hold and resume it as necessary.

To hold or resume Oracle Configuration Manager on a Managed Home

1. In the Quick Links section on the Management Dashboard home page, click the Oracle Configuration Manager link.
2. To place an Oracle Configuration Manager instance on hold, select the OCM check box of the appropriate managed home location and click the Hold button.
3. To resume an Oracle Configuration Manager instance, click the OCM check box of the appropriate managed home location and then click the Resume button.

25.10 View Configuration Data and Log Files

All configuration data obtained by Oracle Configuration Manager can be viewed only by Oracle and the customer that has Oracle Configuration Manager installed. You can view the raw configuration data that is stored in an xml file through the Oracle Configuration Manager instance in Server Manager.

In addition, Oracle Configuration Manager produces log files that contain information about the scheduling, collection, and upgrade processes that occur in Oracle Configuration Manager, as well as information about errors.

See Also: Examples of Data Collected by Oracle Configuration Manager and Data Collected by Oracle Configuration Manager

25.10.1 View Raw Configuration Data and Log Files on the Managed Home

On each Oracle Configuration Manager home page, you can access configuration data in xml files, as well as log files that are generated each time Oracle Configuration Manager creates a collection.

To view raw configuration data and log files on the managed home:

1. In the Quick Links section on the Management Dashboard home page, click the Oracle Configuration Manager link.
2. On the Oracle Configuration Manager page, click the ocm link for the managed home location on which you want to view configuration data and log files.
3. Click the Available Log Files link at the top of the page or scroll down to the Available Log Files section.
4. Click the appropriate link to the xml or log file to view the data.
5. To delete any of these files, select the check box associated with a file and then click the Delete button.

25.11 Manually Download Updates to Oracle Configuration Manager

Each time a collection is uploaded to the Oracle repository, Oracle automatically checks the version of the customers Oracle Configuration Manager instance and sends an update, if available.

You can control whether updates are automatically downloaded to Oracle Configuration Manager. By default, the Auto Update option is enabled. If you prefer, you can disable this setting and manually download an update.

Note: If a mandatory update to Oracle Configuration Manager is required, an upload of configuration data will not occur until that update has been applied.

To manually download updates to Oracle Configuration Manager

1. In the Quick Links section on the Management Dashboard home page, click the Oracle Configuration Manager link.
2. On the Oracle Configuration Manager page, click the ocm link for the managed home location on which you want to download an update to Oracle Configuration Manager.

3. On the Oracle Configuration Manager: ocm page, click the Operations link or scroll down to the Operations section. Click the Updates button to manually download an update.
4. To disable automatic updates, scroll to the Settings section and select Off in the Set Auto Update field, and then click the Set Auto Update button.

25.12 Examples of Data Collected by Oracle Configuration Manager

This section contains examples of the information that is provided in these files:

- Sched.log
- Collector.log
- Collection .xml File
- Targetmap.xml
- Upgrade.log

Note: The acronyms CCR and SCF that appear in the log files and examples in this section are synonymous with Oracle Configuration Manager and Server Manager respectively.

25.12.1 Sched.log

In this example of the Sched.log, the collection is scheduled to run every four days; however, Oracle Configuration Manager has been manually placed on hold and will not perform a collection:

```
2007-01-04 19:53:04, [WARN]: Not starting scheduled
  collection as OCM is on hold 2007-01-08 19:53:02, [WARN]: Not starting
  scheduled collection as OCM is on hold
```

25.12.2 Collector.log

This is an example of the Collector.log:

```
2006-12-12 13:52:45,468 [main] ERROR - Mandatory updates
  for scripts (10.2.4.0.0), core (10.2.4.0.0), metricdata (10.2.4.0.0) available.
  Please execute "emCCR getupdates" to download/apply the updates. 2006-12-12
  13:52:45,468 [main] ERROR - Mandatory updates available. Please execute "emCCR
  getupdates" to download/apply the updates.
```

25.12.3 Collection .xml File

This is an example of an .xml file that contains the raw collection data:

```
<?xml-stylesheet type="text/xsl"
  href="../../admin/xsl/preview_collection.xsl"?> <ROWSET
  OMS_PROTOCOL_VERSION="10.2.0.0.0" SINGLE_ROW="TRUE" TABLE="MGMT_TARGETS">
  <ROW>
  <TARGET_GUID>ED0211AADF3494E7EB4AD173B78632E0</TARGET_GUID>
  <TARGET_NAME>ED0211AADF3494E7EB4AD173B78632E0</TARGET_NAME>
  <ORG_ID>123456</ORG_ID>
  <HOST_NAME>user1-pc1.company.com</HOST_NAME>
  <AGENT_TARGET_NAME>c:\jde_home</AGENT_TARGET_NAME>
```

```
<TARGET_TYPE>oracle_e1_scf_mc</TARGET_TYPE>
<ORACLE_HOME>c:\jde_home</ORACLE_HOME>
<TIMEZONE_REGION>America/Denver</TIMEZONE_REGION> </ROW>
</ROWSET> <ROWSET OMS_PROTOCOL_VERSION="10.2.0.0.0"
TABLE="MGMT_E1_MC_MANAGED_INSTANCES" META_VER="1.0" INCREMENTAL="FALSE"
CONFIG="TRUE"> <ROW> <MIINLOC>c:\jde_home</MIINLOC>
<MIMHHOST>user1-PC1.company.com</MIMHHOST>
<MIMHINLOC>c:\jde_home</MIMHINLOC>
<MIINSTNM>home</MIINSTNM>
<MITRGTYP>mgmtconsole</MITRGTYP> <MITTDESC>JD Edwards
Management Console</MITTDESC> </ROW> </ROWSET> <ROWSET
OMS_PROTOCOL_VERSION="10.2.0.0.0" TABLE="MGMT_E1_MC_AGENT" META_VER="1.0"
INCREMENTAL="FALSE" CONFIG="TRUE"> <ROW>
<AGINLOC>c:\jde_home</AGINLOC> </ROW> </ROWSET>
<ROWSET OMS_PROTOCOL_VERSION="10.2.0.0.0" TABLE="MGMT_E1_MC_MANAGED_HOMES"
META_VER="1.0" INCREMENTAL="FALSE" CONFIG="TRUE"> <ROW>
<MHINLOC>c:\jde_home</MHINLOC>
<MHMHHOST>user1-PC1.company.com</MHMHHOST>
<MHMHINLOC>c:\jde_home1</MHMHINLOC> </ROW> <ROW>
<MHINLOC>c:\jde_home</MHINLOC>
<MHMHHOST>user1-PC2.company.com</MHMHHOST>
<MHMHINLOC>c:\jdehome2</MHMHINLOC> </ROW> <ROW>
<MHINLOC>c:\jde_home</MHINLOC>
<MHMHHOST>user1-PC3.company.com</MHMHHOST>
<MHMHINLOC>/u01/jdehome3</MHMHINLOC> </ROW> </ROWSET>
```

25.12.4 Targetmap.xml

This is an example of the Targetmap.xml file:

```
<?xml-stylesheet type="text/xsl"
  href="../../admin/xsl/preview_targets.xsl"?> <Targets
  collection_time="2007-01-03 19:53:27" host_name="user1-pc1.company.com">
  <Target name="E90_8.97" type="EnterpriseOne Configuration Data">
  <Collection name="oracle_e1_config" file="313EDABD749A480395F60E3ED2E1CE1F-
  oracle_e1_config.xml" collection_timestamp="2007-01-03 19:53:27
  America/Denver"/> </Target> <Target name="UnknownName:c:\jde_home"
  type="Oracle Home"> <Collection name="oracle_home_config"
  file="8329DAC3A760C2C9A009EC96D724B0C3- oracle_home_config.xml"
  collection_timestamp="2007-01-03 19:57:01 America/Denver"/> </Target>
  <Target name="user1-pc1.company.com" type="Host"> <Collection
  name="ll_host_config" file="7A23AE3E2D86C990D231050392630000-ll
  _host_config.xml" collection_timestamp="2007-01-03 19:57:02
  America/Denver"/> </Target> <Target name="c:\jde_home"
  type="EnterpriseOne Management Console Data"> <Collection
  name="oracle_e1_scf_mc" file="ED0211AADF3494E7EB4AD173B78632E0-
  oracle_e1_scf_mc.xml" collection_timestamp="2007-01-03 19:59:36
  America/Denver"/> </Target> <Target name="Oracle Configuration
  Manager" type="Oracle Configuration Manager"> <Collection
  name="livelink_config" file="2EB5B050A63E1AFC25CBDDB2113E15BF-
  livelink_config.xml" collection_timestamp="2007-01-03 19:59:39
  America/Denver"/> </Target> </Targets>
```

25.12.5 Upgrade.log

This is an example of the Upgrade.log file:

```
Scheduler restarting for upgrade. Oracle Configuration
```

```
Manager - Release: 10.2.3.0.0 - Production Copyright (c) 2005, 2006, Oracle.
All rights reserved.
------------------------------------------------------------------- Deploying
core - Version 10.2.4.0.0 Deploying metricdata - Version 10.2.4.0.0 Deploying
scripts - Version 10.2.4.0.0 Starting Oracle Configuration Manager... Waiting
for status from Oracle Configuration Manager.... Start Date 12-Dec-2006
19:53:46 Last Collection Time 11-Dec-2006 20:53:37 Next Collection Time
13-Dec-2006 19:53:00 Collection Frequency Daily at 19:53 Collection Status
scheduled collection running Log Directory c:\jde_home\ccr\log Oracle
Configuration Manager successfully started.
```

26

Update Server Manager

The Management Console and the Management Agents have codependent release levels. The Management Console constantly monitors the version levels of the registered Management Agents and if it determines that a registered Management Agent is out of sync (mismatched) with the Management Console's own release level, then it notifies the user that an update is required for a specific Management Agent. This can happen any time you change the release level of the Management Console, either to a newer release or to an older release.

You must manually update a Management Agent when notified, as described in this chapter. If you do not update the Management Agent, unpredictable and undesirable results can occur in the execution of Server Manager requests on the target machine on which the Management Agent resides.

This chapter discusses:

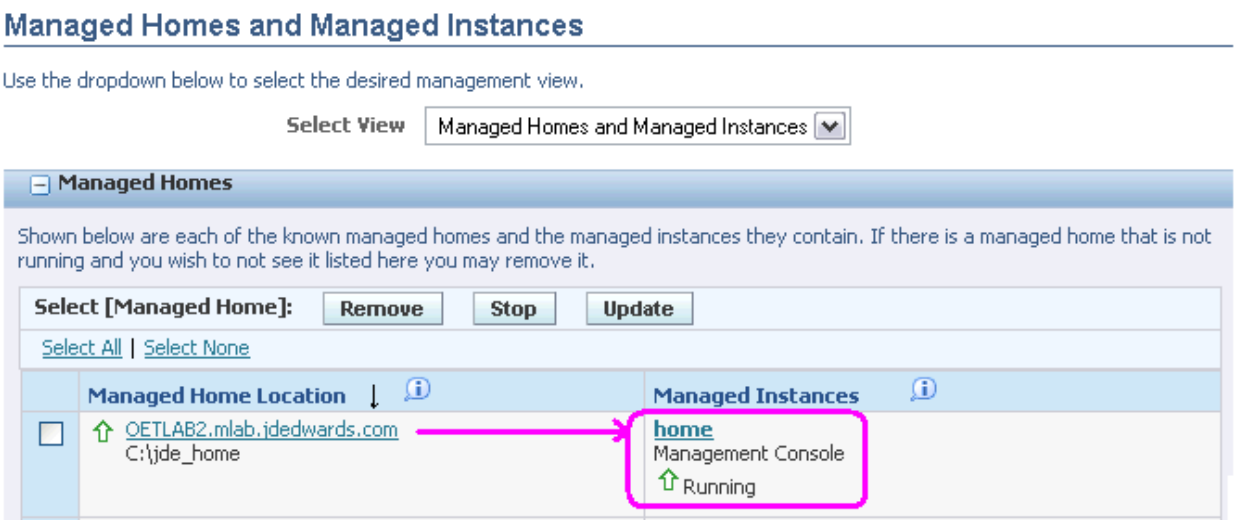
- Section 26.1, "Update the Management Console"
- Section 26.2, "Update a Management Agent"
- Section 26.3, "Troubleshooting an Unsuccessful Management Console Update"

26.1 Update the Management Console

If you update the Management Console to a new Tools Version (for example, 8.98.3), you must upgrade the Management Agents to the same version. Otherwise your Server Manager cannot communicate and operate with the target machines as expected.

You update the Management Console by changing its Software Component using the same method as changing any other Server Manager Managed Instance (refer to Managed Software Components).

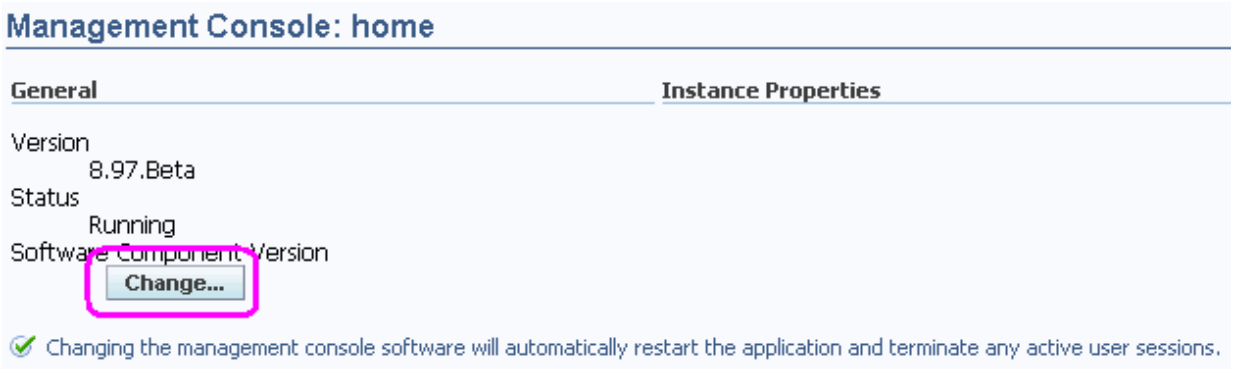
Caution: Changing the Software Component version for the Management Console will automatically restart the Management Console application and terminate any active user sessions.



To update the Software Component:

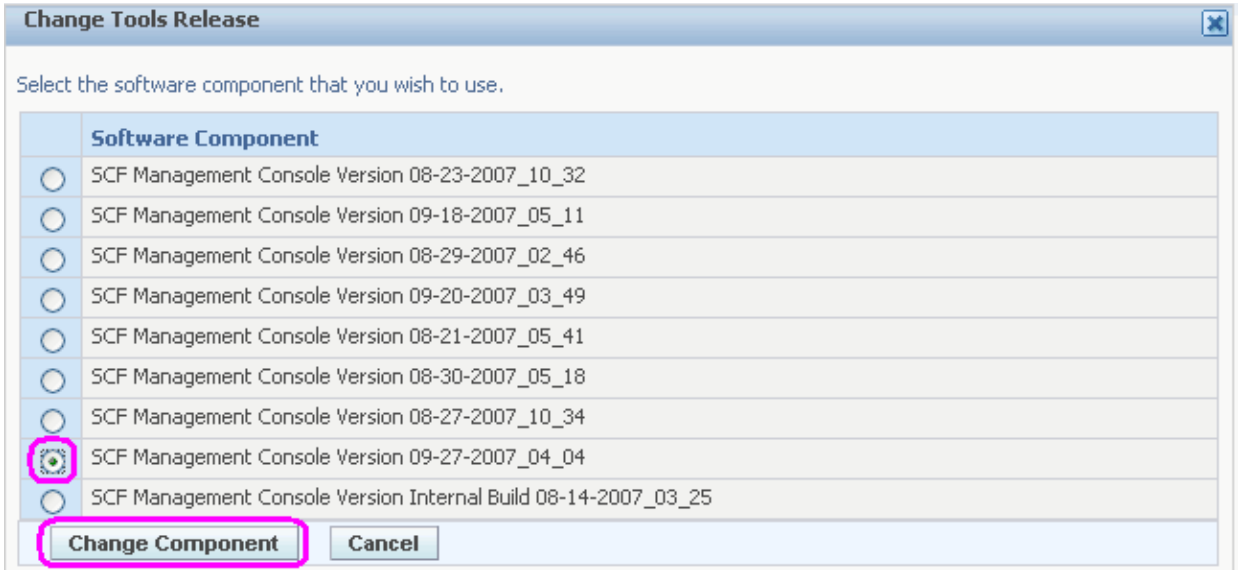
1. On Managed Homes and Managed Instances, locate the Managed Home Location for your Software Component and click the link for the associated Managed Instance for *home*.

   This is the location you specified when you installed the Software Component, where the default is `c:\jdehome`.



2. In the General section of the page, under Software Component Version, click the *Change ...* button.

   The Management Console displays a popup with a list of available Managed Software Components is displayed. For example:

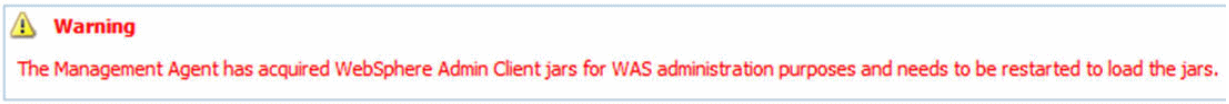


3. On the Change Tools Release popup, you can select a *Software Component* radio button and click the *Change Component* button to change to that version.

   The update process starts immediately and upon completion the Management Console application will automatically restart. If the Management Console fails to restart as expected, refer to Troubleshooting an Unsuccessful Management Console Update in this chapter for a description of symptoms and recovery.

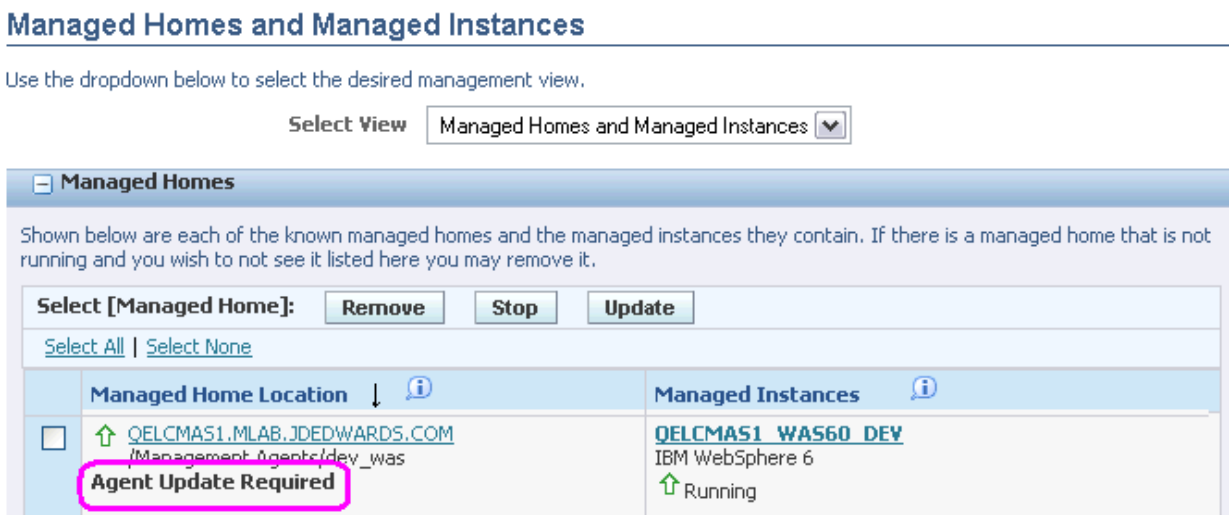
26.2 Update a Management Agent

After you update a Management Agent to a new tools version (for example, Tools Version 8.98.3), any existing WAS 6.x instances will display this message:



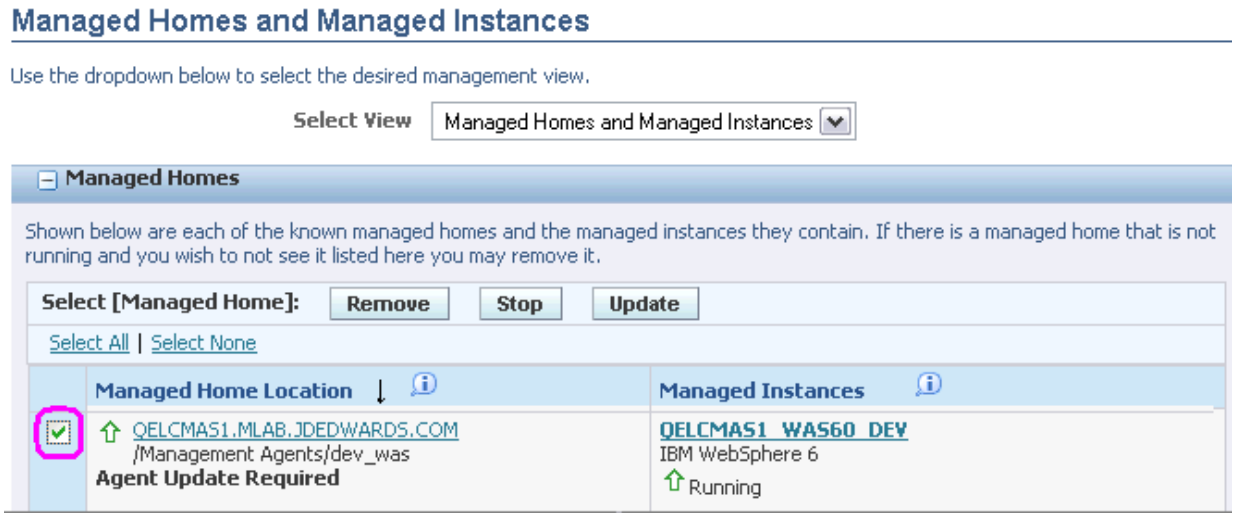
To resolve the Warning you must restart the Management Agent to complete the update process.

When the Management Console determines that a Management Agent version is out of sync (mismatched) with the version of the Management Console itself it displays a notification under the Managed Home Location of the applicable Management Agent. For example:

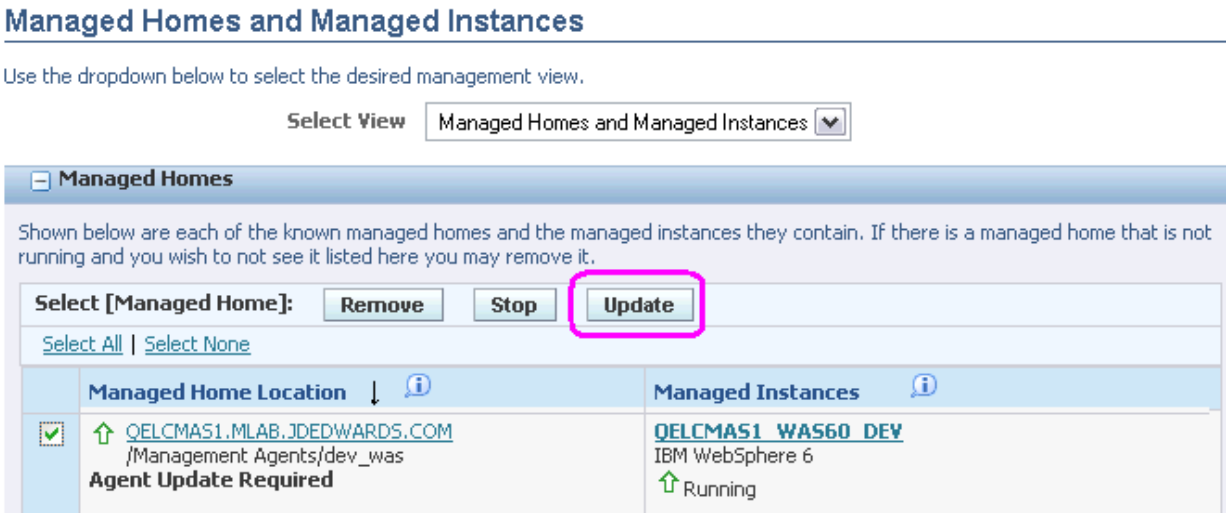


To update a Management Agent:

1. On Managed Homes, select the Managed Home Location for which indicates: *Agent Update Required*.



2. Use the check box to select the appropriate Managed Home Location.



3. Click the *Update* button.

   The Management Console displays this confirmation dialog:

4. Click OK to immediately begin updating the selected Management Agent. Once the update is complete, Server Manager will automatically restart the Management Agent.

26.3 Troubleshooting an Unsuccessful Management Console Update

There may be times when updating the Management Console application is not successful. The symptoms of a failed updated is the lack of a logon screen after the update completes, even after restarting the Management Console. Server Manager provides a fallback script that can be used to redeploy the application and recover the Management Console without any data loss. The script will deploy the intended (change-to) release.

To troubleshoot an unsuccessful Management Console update:

1. Stop the Management Console service.
2. Start the Management Console service.
3. Open a command prompt and navigate to this directory:

   `\jde_home\targets\home\_staging`

   where `jde_home` is the install path of the Management Console.
4. Invoke the `redeployManagementConsole.cmd` recovery script.

   The script takes one parameter, which is the password used to initially install the Management Console. For example

   `redeployManagementConsole.cmd password`

Upon successful execution of this script you can log on to the Management Console application.

27

Create a JD Edwards EnterpriseOne Data Access Server as a New Managed Instance

This chapter discusses:

- Section 27.1, "Prerequisites and Recommended Installation Sequence for Managed Instances for Data Access Server Instance"
- Section 27.2, "Create a Data Access Server as a New Managed Instance"

27.1 Prerequisites and Recommended Installation Sequence for Managed Instances for Data Access Server Instance

This list shows the prerequisites and recommended installation sequence for Managed Instances for JD Edwards EnterpriseOne Data Access Servers:

1. Prerequisite: Management Agent is installed on target machine.

   Refer to Chapter 5, "Install a Management Agent".

2. Prerequisite: The Data Access Server Software Component is uploaded to the Management Console.

   Refer to Section 11.1, "Upload Software Components".

3. Prerequisite: The Data Access Server Software Component is distributed to the target Managed Home.

   Refer to Section 11.2.1, "Distribute Software Components to Managed Homes".

4. Create a Data Access Server as a New Managed Instance

   Refer to Section 27.2, "Create a Data Access Server as a New Managed Instance".

See Also:

- Refer to the *JD Edwards EnterpriseOne Interoperability Guide* in the chapter *Using Java Database Connectivity* for additional tasks and topics related to the Data Access Server.
- *JD Edwards EnterpriseOne BI Publisher for JD Edwards EnterpriseOne Guide*
- Refer to various Red Papers in the Red Paper Library on Customer Connection.

  Navigation: Customer Connection > Implement, Optimize, and Upgrade > Implementation Guide > Implementation Documentation and Software > Red Paper Library

  http://www.peoplesoft.com/corp/en/iou/red_papers/index.jsp

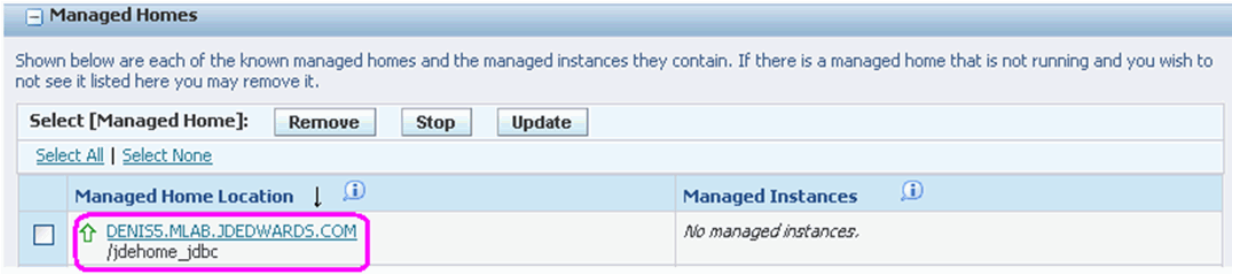
27.2 Create a Data Access Server as a New Managed Instance

You must use Server Manager to install a Data Access Server instance.

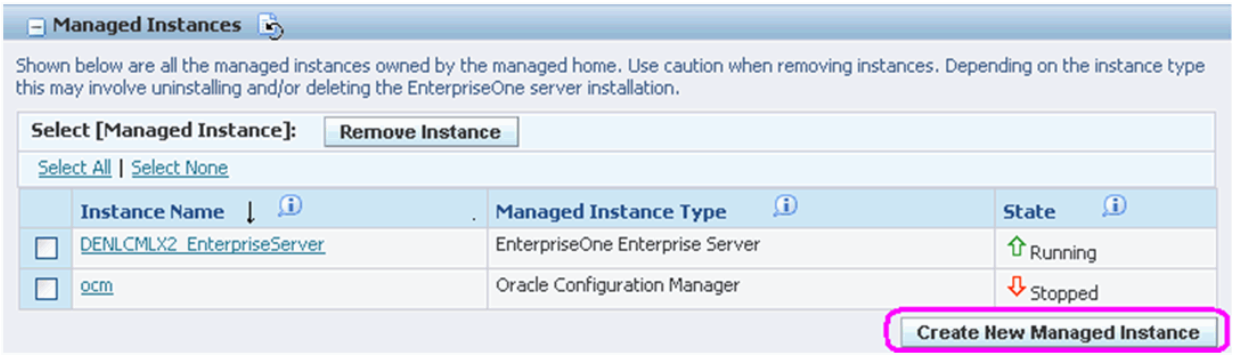
See Also:

- Prerequisites and Recommended Installation Sequence for Managed Instances for Data Access Server Instance

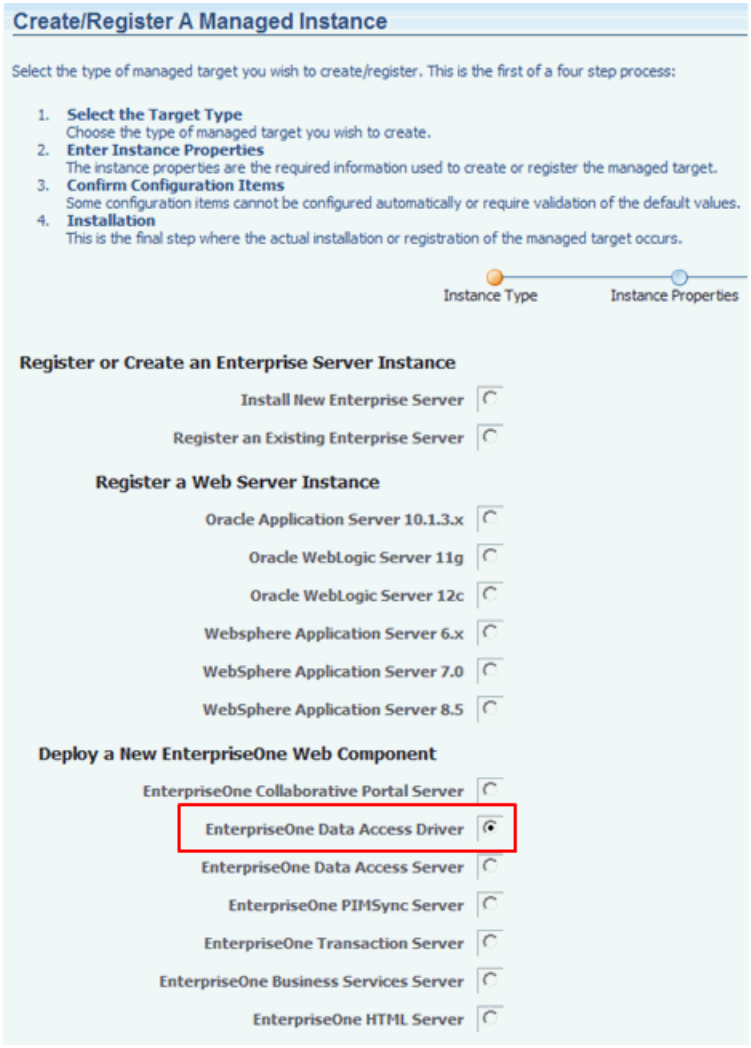
To install a JD Edwards EnterpriseOne EnterpriseOne Data Access Server instance:



1. Select the Managed Home in which you wish to install the Data Access Server.



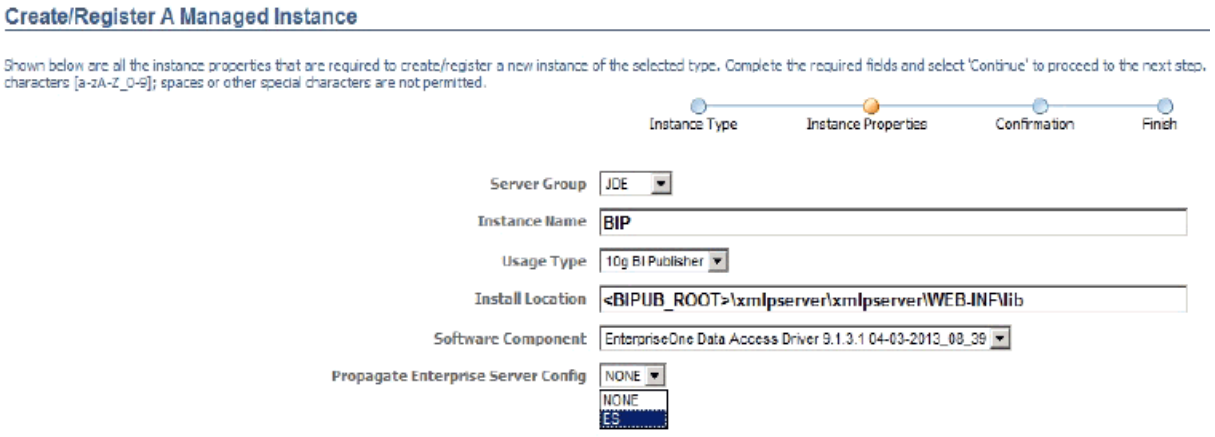
2. Click the *Create a New Managed Instance* button to create the Managed Instance in the Managed Home.



3. On Create/Register a Managed Instance, Instance Type, select this radio button:

   EnterpriseOne Data Access Server

4. Click Continue.



5. On Create/Register a Managed Instance, Instance Properties, complete these fields:

   - *Server Group*

Use the pulldown to select the Server Group to which you want this instance to belong.

Also refer to Chapter 31, "Administer Server Groups".

- *Instance Name*

  Enter a unique name for the instance name.

  Tip: A good business practice is to name your instances so that they are easily and consistently identifiable. For example:

  `PRODUCT_SERVER_PORT`

  where `PRODUCT` is the JD Edwards EnterpriseOne server type, such as `Data Access_Server`, and

  where `SERVER` is the machine on which the instance is installed, and

  where `PORT` is the HTTP port which is defined for use by this server.

- *Install Location*

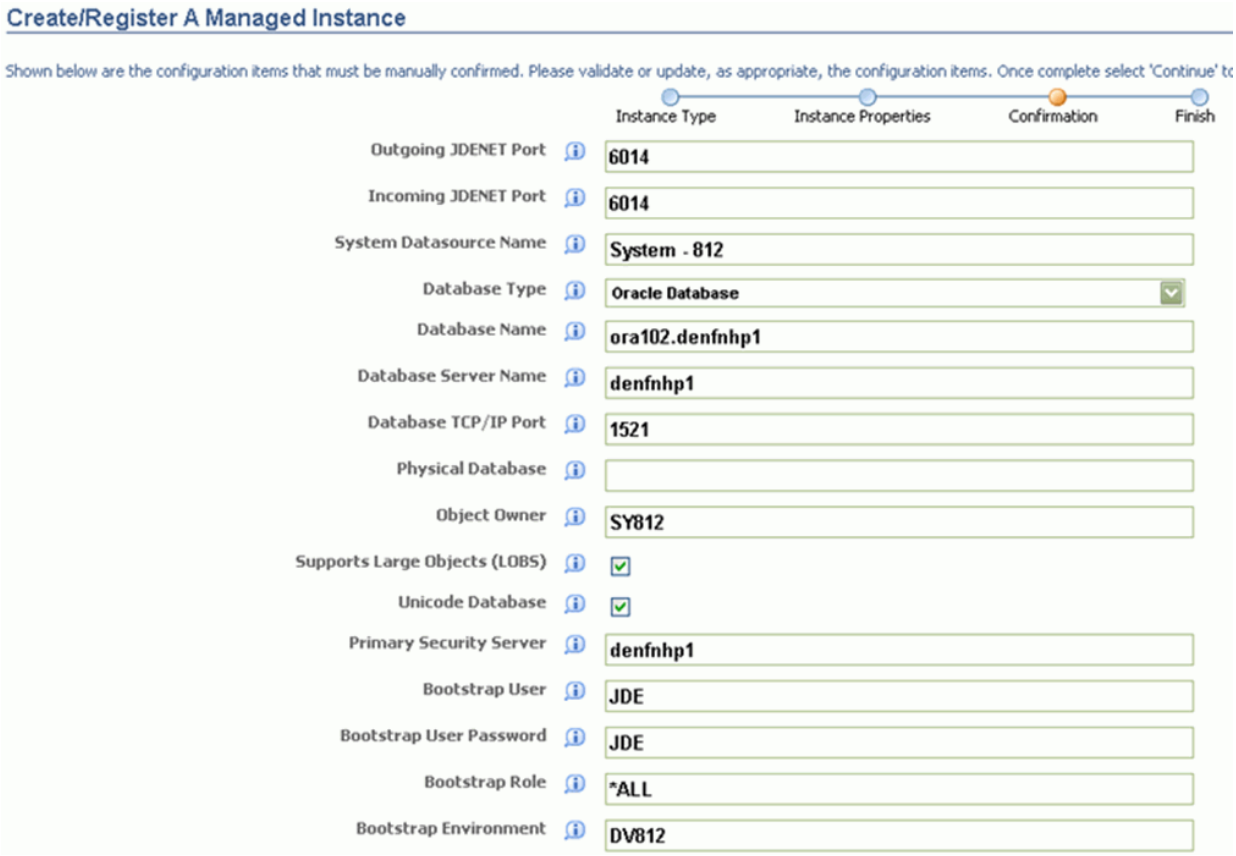
  Specify where the Data Access Server is to be installed.

  This location must be unique and *not* within the Management Agent directory structure.

- *Software Component*

  Use the dropdown to select the version of this Software Component that you wish to install.

6. Click Continue.



7. On Create/Register a Managed Instance, Confirmation, review the key configuration items. The values on this form must be manually confirmed. You must validate or update, as appropriate, all configuration items.

   Tip: For help, click the Information icon next to the title of a field.

   See Also:

   - Chapter 9, "Configure the Default Server Group Configuration Settings"

8. After you have validated and updated all configuration items, click Continue to proceed to the next installation step.

9. On Create/Register a Managed Instance, Finish, click the Create Instance button to complete the installation of the EnterpriseOne Data Access Server.

Once complete the browser is redirected to the Management Console page for the newly registered Data Access Server. This server also appears as a Managed Instance within the corresponding Managed Home.

For each registered Managed Instance, the Management Console displays appropriate information at the top of the page:

- *General*
  - *Status*

    Valid values are:

    Running

    When the status is Running, the *Stop* button is available.

    Stopped

    When the status is Stopped, the *Start* button is available.

See Also:

- Section 11.3, "Start or Stop a Managed EnterpriseOne Software Component"

- *Software Component Version*

  Displays the version of this Software Component.

See Also:

- Section 11.4, "Change a Managed EnterpriseOne Software Component"

- *Data Access Server Password*

  Allows you to change the Data Access Server Password when the Data Access Server is running. The new password is taken from the current configuration value for the Data Access Server Password.

- *Instance Properties*

  - *Install Location*

    The location Data Access Server was installed.

  - *Instance Name*

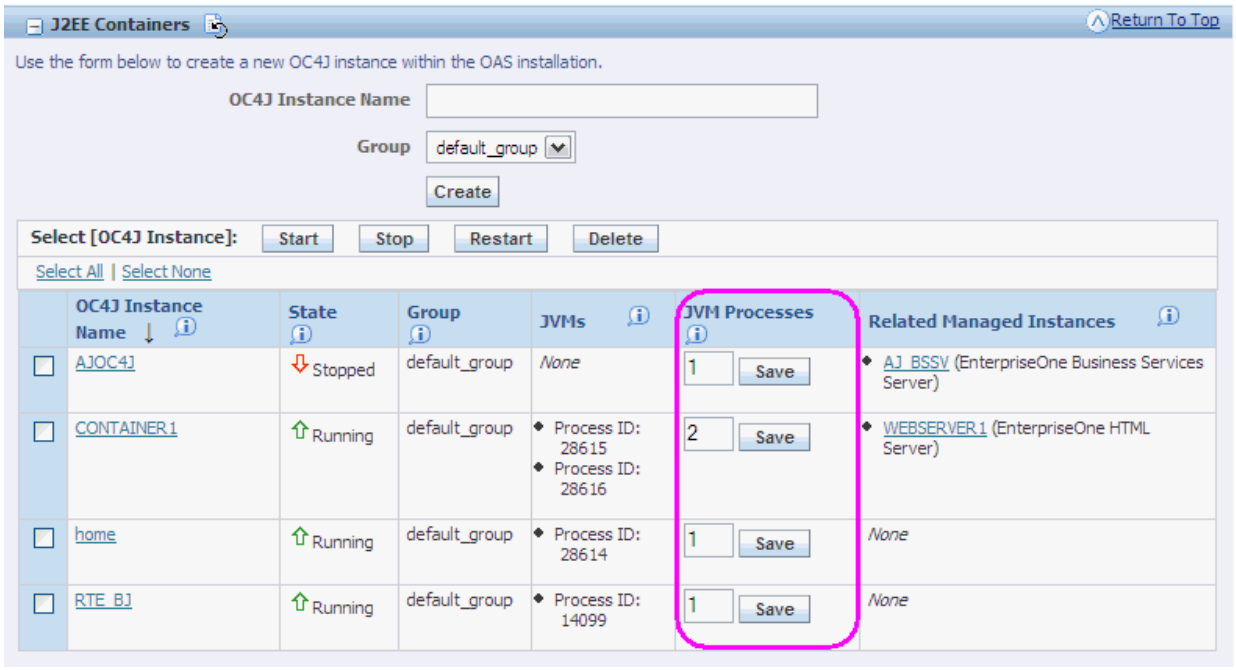
    The unique name assigned to the Managed Instance at the time it was created or registered.

For information on log files, refer to the chapter entitled: Chapter 23, "Available Log Files".

28

Configure an Oracle Application Server

When you click the *Oracle Application Server Name* link on the *Managed Homes* page, the Management Console displays another page called *Oracle Application Server Name*.



To configure Oracle Application Server:

1. In the *J2EE Containers* section, complete this field for the instance you want to configure:

   - *JVM Processes*

     Enter a numeric value specifying the number of JVM processes to simultaneously run within this container.

2. Click the *Save* button.

   Tip: Only the Oracle Application Server needs to be running in order for the Management Console to set this value. The OC4J instance does not need to be running.

29

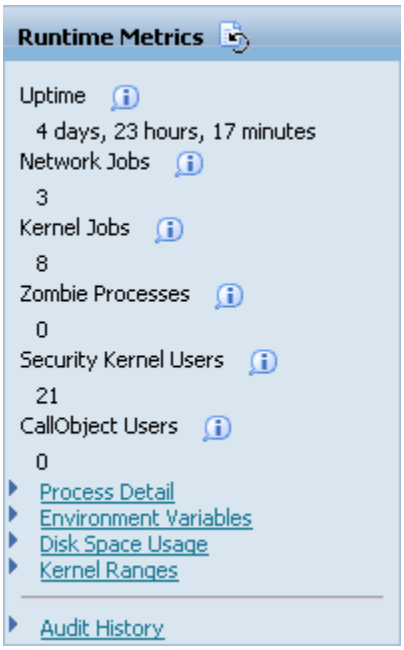
View Runtime Metrics for a Managed Instance

The runtime metrics provide operational information about insight to the EnterpriseOne servers. Runtime metrics are only available when the server is running.

This chapter discusses:

- Section 29.1, "Enterprise Server Runtime Metrics"
- Section 29.2, "EnterpriseOne Web-based Servers Runtime Metrics"
- Section 29.3, "Application Interface Services Server Runtime Metrics (Release 9.1 Update 5)"
- Section 29.4, "Transaction Server Administration"

29.1 Enterprise Server Runtime Metrics



A Runtime Metrics information summary and links to detailed information are available for each Enterprise Server that is running. Metrics are provided by an embedded variant of the management agent built into each EnterpriseOne server. A new kernel definition, the management kernel, was added in 8.97. A single management kernel process is created when the enterprise server is started. The management kernel is responsible for securely networking

between the enterprise server and the server manager management console while providing the runtime details of the enterprise server.

The following runtime metrics are available for a running enterprise server:

- General
- Process Detail
- Environment Variables
- Disk Space Usage
- Kernel Ranges
- Audit History

29.1.1 General

Runtime Metrics will display runtime information for these parameters:

- *Uptime*

  The amount of time the Enterprise Server has been running.

- *Network Jobs*

  The number of network listener processes (jdenet_n) that are currently running.

- *Kernel Jobs*

  The total number of kernel processes (jdenet_k) that are currently running.

- *Zombie Processes*

  Zombie status refers to an Enterprise Server process that has unexpectedly terminated without properly cleaning ups its resources. This value will display the total number of zombie processes that are tracked in the enterprise server shared memory segment.

- *Security Kernel Users*

  The number of EnterpriseOne users that have a currently active security server connection to the Enterprise Server.

- *Call Object Users*

  The number of EnterpriseOne users that have a currently active CallObject (business function) connection to the Enterprise Server.

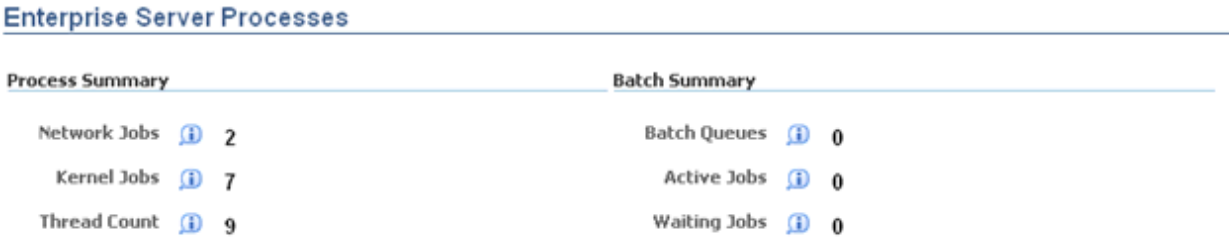
29.1.2 Process Detail

Information about all of the running network, kernel, and other enterprise server processes can be viewed by selecting the Process Detail hyperlink from the Runtime Metrics pane. The management kernel process will periodically query the enterprise server to retrieve the runtime information. This polling will occur approximately every thirty seconds; therefore it is possible that the information displayed through the server manager process detail pages may be up to 30 seconds old.

The process detail page includes:

- A Process Summary
- A Batch Summary
- A Process Table

The top of the page includes a Process Summary section providing a quick reference to the number of active enterprise server processes and provides a Batch Summary that displays the running batch queues, active batch jobs, and pending batch jobs.



29.1.2.1 A Process Summary

The status information fields for Process Summary are:

- *Network Jobs*

  The total number of network listener jobs active on the Enterprise Server.

- *Kernel Jobs*

  The total number of kernel jobs active on the Enterprise Server.

- *Thread Count*

  The total number of threads active on the Enterprise Server.

29.1.2.2 A Batch Summary

The status information fields for Batch Summary are:

- *Batch Queues*

  The number of batch queues that are managed by the queue kernel process on the Enterprise Server.

- *Active Jobs*

  The number of jobs that are currently being processed (running) in the batch queues.

- *Waiting Jobs*

  The number of jobs that are currently in the queue awaiting processing.

29.1.2.3 A Process Table

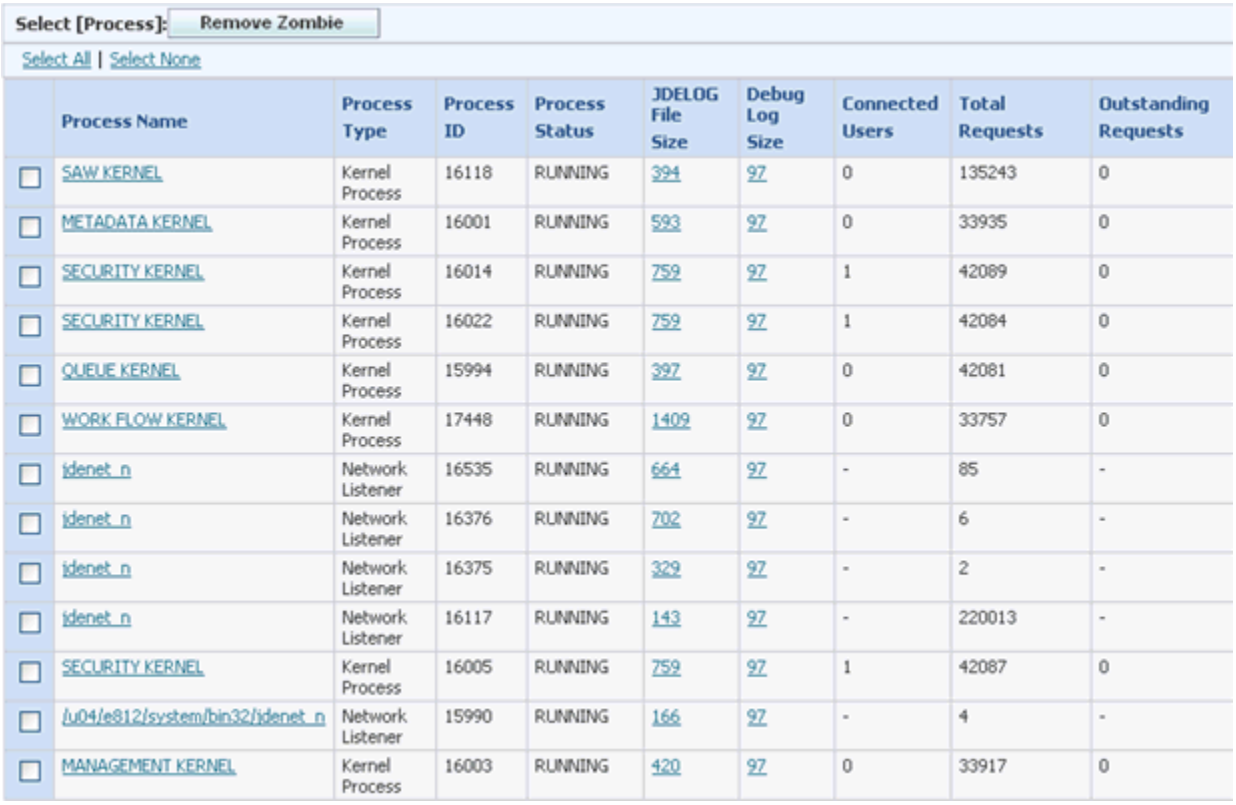
The process table contains a row for each EnterpriseOne server process contained within the shared memory segment. The shared memory segment is created by the first server process created during server startup. Each additional server process will register itself within that shared memory segment. Server Manager uses this shared memory to identify and display all the running server processes.

The process table lists each of the processes found. Each process is displayed along with some key columns. The table also provides links to directly view the associated JDE and JDEDEBUG log files.

Selecting the process name will display more detailed information.

This section describes:

- Remove Zombie
- Process Detail



Select [Process]: Remove Zombie

Select All | Select None

	Process Name	Process Type	Process ID	Process Status	JDELOG File Size	Debug Log Size	Connected Users	Total Requests	Outstanding Requests
☐	SAW KERNEL	Kernel Process	16118	RUNNING	394	97	0	135243	0
☐	METADATA KERNEL	Kernel Process	16001	RUNNING	593	97	0	33935	0
☐	SECURITY KERNEL	Kernel Process	16014	RUNNING	759	97	1	42089	0
☐	SECURITY KERNEL	Kernel Process	16022	RUNNING	759	97	1	42084	0
☐	QUEUE KERNEL	Kernel Process	15994	RUNNING	397	97	0	42081	0
☐	WORK FLOW KERNEL	Kernel Process	17448	RUNNING	1409	97	0	33757	0
☐	jdenet_n	Network Listener	16535	RUNNING	664	97	-	85	-
☐	jdenet_n	Network Listener	16376	RUNNING	702	97	-	6	-
☐	jdenet_n	Network Listener	16375	RUNNING	329	97	-	2	-
☐	jdenet_n	Network Listener	16117	RUNNING	143	97	-	220013	-
☐	SECURITY KERNEL	Kernel Process	16005	RUNNING	759	97	1	42087	0
☐	/u04/e812/system/bin32/jdenet_n	Network Listener	15990	RUNNING	166	97	-	4	-
☐	MANAGEMENT KERNEL	Kernel Process	16003	RUNNING	420	97	0	33917	0

29.1.2.3.1 Remove Zombie A zombie process is an enterprise server process registers itself within the shared memory segment then terminates without removing its registration information shared memory. The most likely cause of a zombie process is a process that performs an illegal operation and is terminated by the host operating system.

Zombie process may have their information removed from the shared memory segment. Removing the zombie process will prevent it from showing up in the process table. To remove a zombie process select the check box next to a process in the zombie state and click the Remove Zombie button. Selecting and attempting to remove a process that is not in the zombie state will have no effect.

29.1.2.3.2 Process Detail Selecting the process name in the process table section will display additional information about that process.

The additional detail includes:

- General Information
- Connected Users
- Log File Configuration
- Thread Detail

Process ID: 29517

Connected Users | Log File Configuration | Thread Detail

When an individual process is selected for viewing, a process detail screen will be displayed with the Process ID number in the heading of the page. The General Information section is always displayed followed by additional relevant sections. Hyperlinks will appear below the Process ID that will link to the additional sections.

29.1.2.3.3 General Information

The General Information section will provide information for these parameters:

- *Process Name*

  The name of the kernel process. The name indicates which kernel definition the kernel belongs to.

- *Process Type*

  The description of the Enterprise Server process type.

- *Kernel Range*

  The kernel definition index. The Enterprise Server is composed of kernels that process messages from other servers and clients. There are more than thirty different types of kernels. The range index indicates which kernel group this kernel belongs to.

- *Process ID*

  The operating system assigned process identifier for the kernel process.

- *Process Index In Shared Memory*

  An internal identifier used to locate the process position in the shared memory resources that track kernel and network processes.

- *Start Time*

  The time the process was created.

- *Last Active Time*

  The last time the kernel performed any activity such as processing incoming JDENET messages.

- *Messages Received*

  The total number of messages (requests) that have been processed by the kernel process.

- *Outstanding Requests*

  The number or requests that are queued and awaiting processing by the kernel process.

- *Parent Process ID*

  The operating system assigned process identifier of the parent process.

- *IBM i Job Number*

  The job number of the process, valid on the IBM i platform only.

- *Process User ID (OS)*

  The operating system user id under which the process is running.

- *OS Group ID*

  The group identifier of the os user running the process; valid only on unix based platforms.

- *OS Username*

  The operating system user name under which the process is running.

- *OS Status*

  The status of the process as reported by the operating system:

  0 = Sleeping

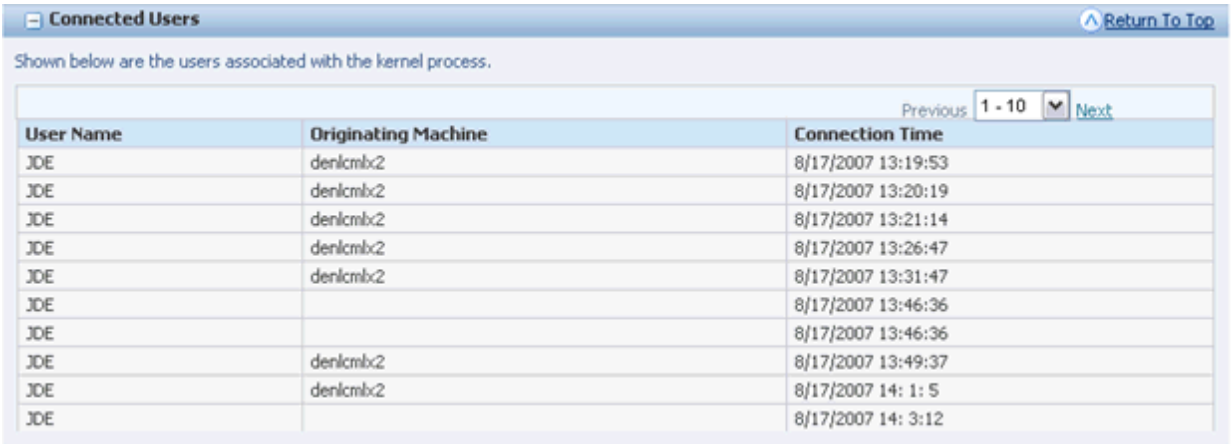
  1 = Running

  2 = Stopped

  3 = Zombie

  4 = Other

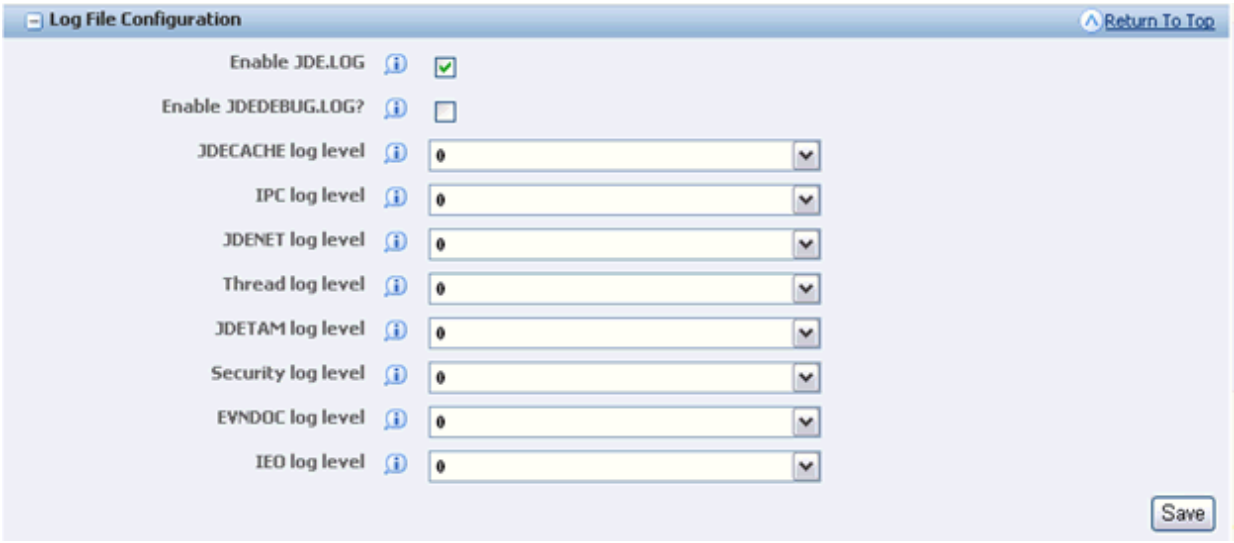
29.1.2.3.4 Connected Users



User Name	Originating Machine	Connection Time
JDE	denlcmlx2	8/17/2007 13:19:53
JDE	denlcmlx2	8/17/2007 13:20:19
JDE	denlcmlx2	8/17/2007 13:21:14
JDE	denlcmlx2	8/17/2007 13:26:47
JDE	denlcmlx2	8/17/2007 13:31:47
JDE		8/17/2007 13:46:36
JDE		8/17/2007 13:46:36
JDE	denlcmlx2	8/17/2007 13:49:37
JDE	denlcmlx2	8/17/2007 14: 1: 5
JDE		8/17/2007 14: 3:12

Security and CallObject kernel processes have active users associated with the process. The page will display a section containing the names, originating machine, and connection time of each remote user that is active on the kernel process.

29.1.2.3.5 Log File Configuration Logging may be dynamically enabled or disabled for an individual process.



The Log File Configuration section will contain up to three segments. The first segment allows for configuration enablement of the JDE.LOG and the JDEDEBUG.LOG, and for setting the log levels for different log files.

The parameters available to change log files are:

- *Enable JDE.LOG*

  This setting controls whether error and other significant messages are written to the jde.log. It is highly recommended this logging type always be enabled.

- *Enable JDEDEBUG.LOG*

  This setting controls whether debug and trace messages are written to the jdedebug.log. These messages are very useful when troubleshooting an Enterprise Server; however, enabling debug logging will impact performance.

- *JDECACHE log level*

  Configures the level of logging generated by the cache manager. This setting will have no effect if JDEDEBUG logging is disabled.

- *IPC log level*

  Configures the level of logging generated by the interprocess communication (IPC) related functionality. This setting will have no effect if JDEDEBUG logging is disabled.

- *JDENET log level*

  Configures the level of logging generated by the JDENET network related functionality. This setting will have no effect if JDEDEBUG logging is disabled.

- *Thread log level*

  Configures the level of logging generated by the thread handling functionality. This setting will have no effect if JDEDEBUG logging is disabled.

- *JDETAM log level*

  Configures the level of logging generated by the TAM specification access routines. This setting will have no effect if JDEDEBUG logging is disabled.

- *Security log level*

  Configures the level of logging generated by the security related functionality. This setting will have no effect if JDEDEBUG logging is disabled.

- *ENVDOC log level*

  Configures the level of logging generated by the EVNDOC (Interop) functionality. This setting will have no effect if JDEDEBUG logging is disabled.

- *IEO log level*

  Configures the level of logging generated by the IEO (Interop) functionality. This setting will have no effect if JDEDEBUG logging is disabled.

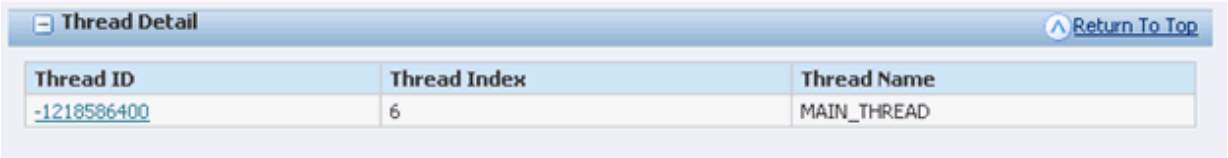
Click the Save button to save any changes made to the parameters.

The second segment will display the filename, size, and last modified date of the JDE.LOG file. Select the View button to retrieve and view the log file contents using the integrated log file viewer.

See Log File Viewer

The third segment will display the filename, size, and last modified date of the JDEDEBUG.LOG file. Select the View button to retrieve and view the log file contents using the integrated log file viewer.

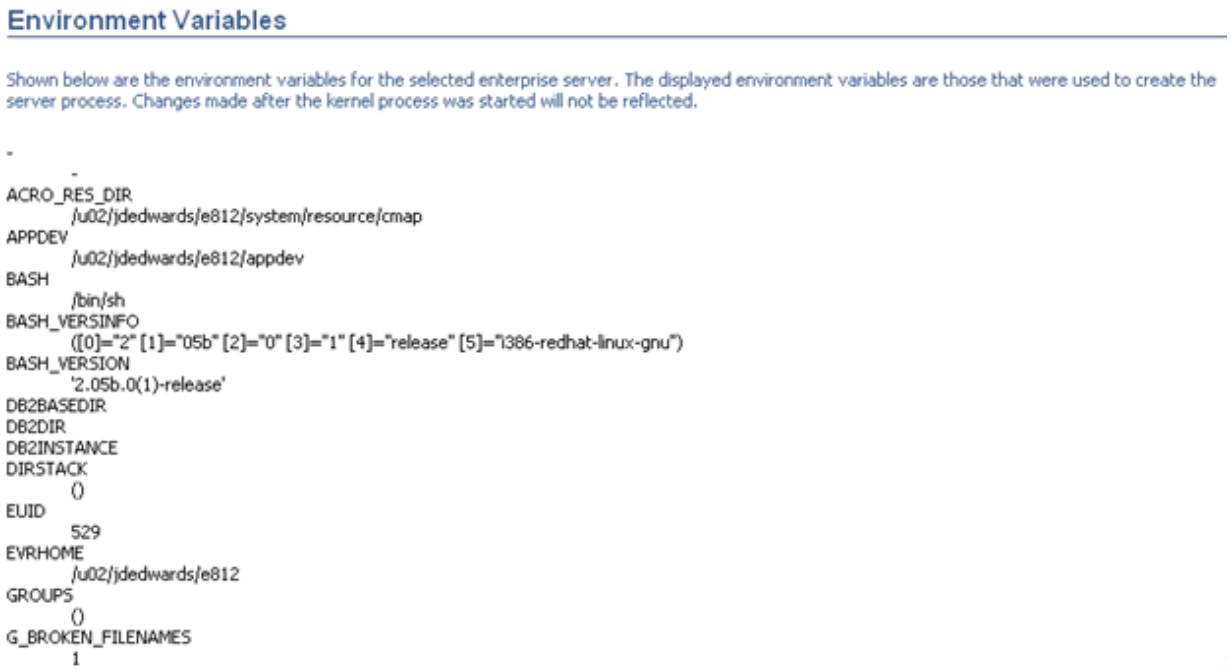
29.1.2.3.6 Thread Detail The active threads for the Enterprise Server process are displayed in the Thread Detail section. Each thread is displayed along with its thread identifier, index in shared memory, and thread name. If thread metrics are enabled selecting a thread identifier will display additional thread related metrics.



If Thread metrics has been enabled, then when the hyperlink for a Thread ID is clicked, then a Thread metrics screen will appear with additional information for the Thread ID. If Thread metrics has not been enabled, then this screen will appear:

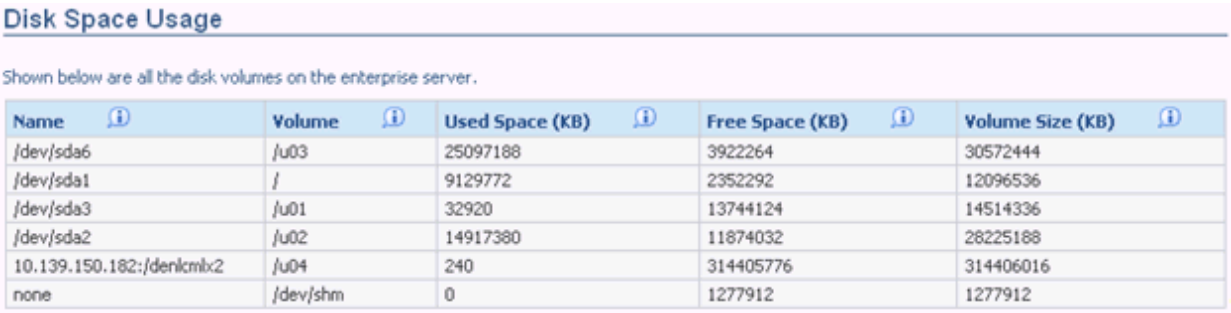
29.1.3 Environment Variables

The Environment Variables hyperlink, when selected, will display the environment variables that are active on the selected Enterprise Server. The displayed environment variables are those that were used to create the server process. Changes made after the kernel process was started will not be reflected.



29.1.4 Disk Space Usage

The Disk Space Usage hyperlink, when selected, displays this information on the disks that make up the Enterprise Server that you are monitoring.



Name	Volume	Used Space (KB)	Free Space (KB)	Volume Size (KB)
/dev/sda6	/u03	25097188	3922264	30572444
/dev/sda1	/	9129772	2352292	12096536
/dev/sda3	/u01	32920	13744124	14514336
/dev/sda2	/u02	14917380	11874032	28225188
10.139.150.182:/denlcmlx2	/u04	240	314405776	314406016
none	/dev/shm	0	1277912	1277912

The information available on the Disk Space Usage screen is:

- *Name*

  The name of the physical disk.

- *Volume*

  The volume, or mount point, of the disk.

- *Used Space (KB)*

  The amount of space that is currently in use on the disk, in kilobytes.

- *Free Space (KB)*

  The amount of space that is available on the disk, in kilobytes.

- *Volume Size (KB)*

  The total amount of space available on the disk, in kilobytes.

29.1.5 Kernel Ranges

Selecting the Kernel Ranges hyperlink will link to the Kernel Ranges screen. This screen has two sections:

- Network Listener Jobs (JDENET_N)
- Kernel Process Jobs (JDENET_K)

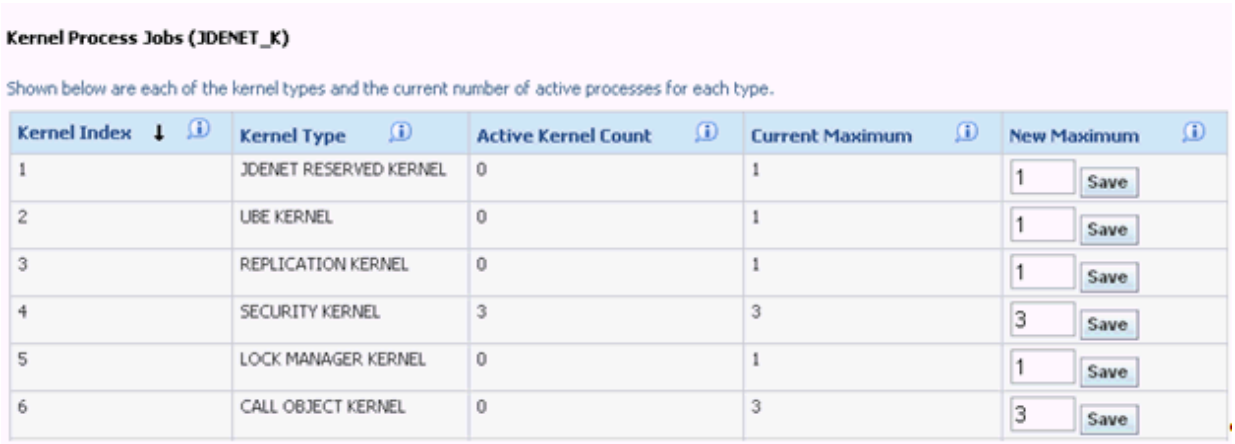
29.1.5.1 Network Listener Jobs (JDENET_N)

The first section of this screen is for Network Listener Jobs (JDENET_N). The maximum number of simultaneous network listener jobs can be designated by entering a number into the Maximum Net Listeners field.

- Maximum Net Listeners

  The maximum number of network listener jobs (jdenet_n) that may be active at any given time.

29.1.5.2 Kernel Process Jobs (JDENET_K)



This section will list each of the kernel types and the current number of processes for each type. The information in this section includes:

- *Kernel Index*

The kernel definition index. Each kernel type has a distinct value, which corresponds to the JDENET_KERNEL_DEF## section in the JDE.INI where ## represents the kernel index value.

- *Kernel Type*

  A textual description to the kernel process type.

- *Active Kernel Count*

  The number of kernel processes of the specified type that is running.

- *Current Maximum*

  The current maximum number of processes of the specified type that may simultaneously exist. This value is an in-memory value only; if the Enterprise Server is restarted the maximum processes will be reloaded from the INI configuration file.

- *New Maximum*

  You may specify a new maximum number of simultaneous processes for a particular kernel. The value must be equal to or greater than the current number of processes of the specified kernel type.

If the *New Maximum* has been changed, click the *Save* button next to the changed number to save the change.

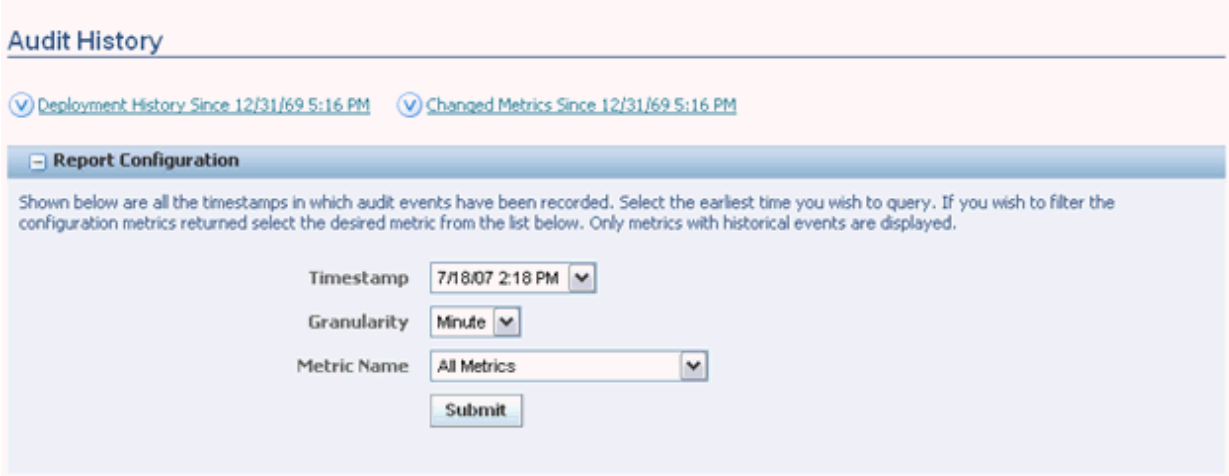
29.1.6 Audit History

You may view the configuration changes that have occurred over time by selecting the audit history link. Each configuration item that has changed will be listed in chronological order. You may also use the filter criteria to narrow down the results returned. Audit history will also contain a record for each start and stop of the server that was performed using server manager. This screen has three sections:

- Report Configuration
- Deployment History
- Changed Metrics

29.1.6.1 Report Configuration

The Report Configuration section will display all of the timestamps in which audit events have been recorded.



The fields and values that are reported are:

- *Timestamp*

  This field will have values that can be selected from a dropdown box in the format of date, then time.

- *Granularity*

- This field allow you to choose:

  Minute

  Hour

  Day

- *Metric Name*

  This field permits narrowing down the returned results to specific configuration topics.

After selecting the values for these parameters, click the *Submit* button to process your selection.

29.1.6.2 Deployment History

Deployment History will provide information for the selected instance including installs, uninstalls, and changes to the tools release within the selected time period.

Deployment History Since 12/31/69 5:16 PM

Shown below are the deployment history for the selected instance including installs, uninstalls, and changing the tools release within the selected time period.

Previous 1 - 10 Next

Timestamp	User Name	Activity	Description
7/18/07 2:18 PM	*Unknown*	performDefaultConfig	The instance was configured to factory default values.
7/18/07 2:22 PM	jde_admin	start	The managed instance was started.
7/31/07 2:55 PM	jde_admin	stop	The managed instance was stopped.
7/31/07 2:55 PM	jde_admin	start	The managed instance was started.
7/31/07 3:09 PM	jde_admin	stop	The managed instance was stopped.
7/31/07 3:11 PM	jde_admin	start	The managed instance was started.
7/31/07 5:02 PM	jde_admin	stop	The managed instance was stopped.
7/31/07 5:02 PM	jde_admin	start	The managed instance was started.
8/1/07 11:08 AM	jde_admin	stop	The managed instance was stopped.
8/1/07 11:08 AM	jde_admin	start	The managed instance was started.

29.1.6.3 Changed Metrics

Changed Metrics will display all the configuration metric changes within the selected time period.

Changed Metrics Since 12/31/69 5:16 PM

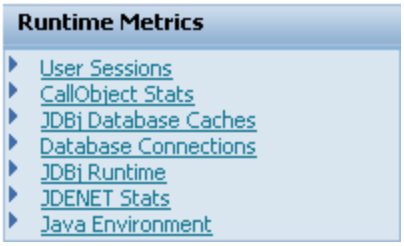
Previous 1 - 10 Next

Timestamp	User	Metric Name	Configuration Item	Old Value	New Value
7/18/07 2:18 PM	*Unknown*	JDENET Configuration	Net Temporary Directory	/u02/management-agent/targets/812_Enterprise/temp	/u02/management-agent/targets/DENLCMLX2_EnterpriseServer/temp
7/18/07 2:18 PM	*Unknown*	Workflow	Interoperability Flag	*Empty*	ON
7/18/07 2:18 PM	*Unknown*	Server Manager Configuration	Instance Name	812_Enterprise	DENLCMLX2_EnterpriseServer
7/31/07 2:36 PM	jde_admin	JDENET Configuration	Interop Timeout	60	0
7/31/07 2:36 PM	jde_admin	JDENET Configuration	entserver_jdenet.servicenameconnect	6014	6015
7/31/07 2:36 PM	jde_admin	JDENET Configuration	Service Name Listen	6014	6015
7/31/07 2:36 PM	jde_admin	JDENET Configuration	entserver_jdenet.servicenameconnect	6015	6018
7/31/07 2:36 PM	jde_admin	JDENET Configuration	Service Name Listen	6015	6018
7/31/07 2:56 PM	jde_admin	DB System Settings	Server Port	*Empty*	1521
7/31/07 3:10 PM	jde_admin	JDENET Configuration	Maximum Kernel Processes	31	50

29.2 EnterpriseOne Web-based Servers Runtime Metrics

Runtime Metrics for EnterpriseOne web products provides metric information for:

- User Sessions (HTML Server Only)
- CallObject Stats
- JDBj Database Caches
- Database Connections
- JDBj Runtime
- JDENET Stats
- Java Environment

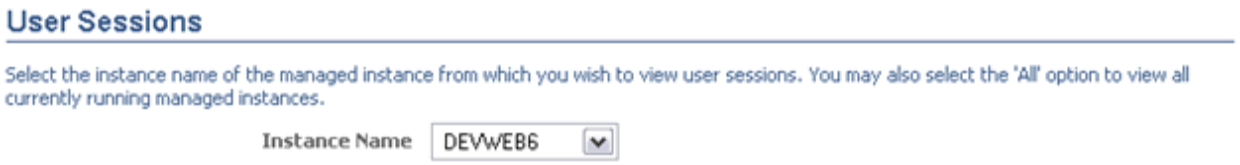


29.2.1 User Sessions (HTML Server Only)

Active user sessions may be viewed for a single HTML server instance or across all instances you are authorized to view.

This section describes:

- Terminate
- Send Message



In the Instance Name field, select the instance name of the managed instance from which you wish to view user sessions, or select ALL to view all instances.

- *Instance Name*

  The name of the instance. The selections available are:

  ALL

  individual instance name

  home

Active User Sessions information includes:

- *JVM Node Id*

  An identifier that uniquely identifies a singe JVM.

- *User Name*

  The user name that created the HTML server session.

- *Client Address*

  The name of the remote machine used to create the user session. This may be returned as the machine name or IP address. If proxy servers are used the machine name may be that of the proxy server and not the actual remote client.

- *Environment*

  The name of the user's sign in environment.

- *Display Mode*

  This value indicates the type of user session: 'HTML' for HTML server session, 'Data Browser', or 'Portal'.

- *Login Time*

  The time the user session was created.

- *Idle Time*

  The amount of time, in seconds, that the user has been idle.

- *Remote Environments*

  Each remote environment represents a call object kernel session that has been created for the user. The format is host:port PID:pid, where host indicates the name of the enterprise server, port indicates the JDENET port of the enterprise server, and pid indicates the process id of the corresponding call object kernel process.

- *Session Identifier*

  A unique identifier for each user session.

- *Open Applications*

  Each application stack currently active for the user session will be listed.

29.2.1.1 Terminate

The *Terminate* button is available to terminate user sessions. You may terminate a user session along with any applications that are running. Use caution because the user will not be informed of this action and any work in progress may be lost. Select a check box for the user session that

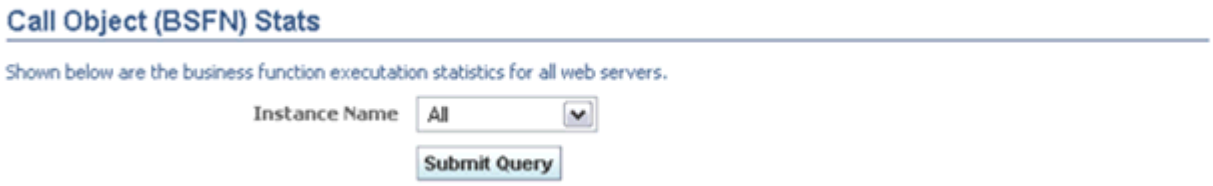
needs termination, and then click the *Terminate* button. A management console user must posses the userSession permission granted for the managed instance on which the user is active in order to terminate the session.

29.2.1.2 Send Message

The *Send Message* button is available to send messages to the applications active within a user session. You may select users and send a message. Messages will be received only by users who have an application running, and only when they perform an activity within the application such as pressing *Find* on the toolbar.

29.2.2 CallObject Stats

The CallObject statistics detail the business functions that have been invoked by a web product. Each business function that is called is recorded and displayed along with timing, invocation counts, and error counts.



Business function invocations and related statistics may be viewed for a single instance or multiple instances In the Instance Name field, select the instance name of the managed instance from which you wish to view user sessions, or select ALL to view all instances you are authorized to view. After making the selection, click the Submit Query button to refresh the results.

- *Instance Name*

  The name of the instance. The selections available are:

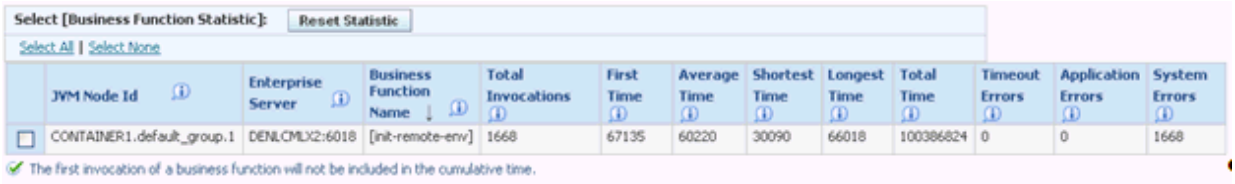
  ALL

  individual instance name

  home

29.2.2.1 CallObject Table

Statistics may be dynamically cleared for individual or all business function invoked.



The Call Object (BSFN) Stats window displays cumulative data about each type of business function that has run during a server session. This table summarizes the information displayed for each business function:

- *JVM Node Id*

  An identifier that uniquely identifies an individual JVM. This column will appear only if an instance was detected with multiple JVMs.

- *Enterprise Server*

  The Enterprise Server name and port of the Enterprise Server to which the statistic applies.

- *Business Function Name*

  The name of the business function.

- *Total Invocations*

  The total number of invocations of the business function.

- *First Time*

  The amount of time, in milliseconds, that a first invocation of the business function took. The first invocation is not counted towards the average due to its initial overhead.

- *Average Time*

  The average time, in milliseconds, that a first invocation of the business function took. The first invocation is not counted towards the average due to its initial overhead.

- *Shortest Time*

  The shortest amount of time, in milliseconds, that an invocation of this business function took.

- *Longest Time*

  The longest amount of time, in milliseconds, that an invocation of this business function took.

- *Total Time*

  The longest amount of time, in milliseconds, that an invocation of this business function took.

- *Timeout Errors*

  The number of invocations of this business function that resulted in a JDENET timeout rather than a successful completion.

- *Application Errors*

  The number of invocations of this business function that resulted in an application returned error rather than a successful completion.

- *System Errors*

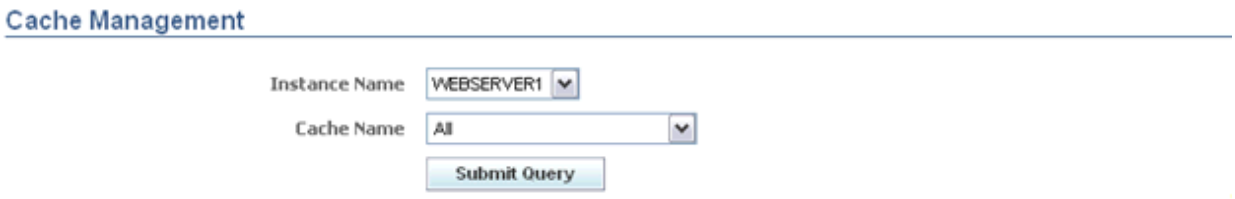
  The number of invocations of this business function that resulted in a system error rather than a successful completion.

The CallObject Information view also displays the number of business function processes in progress. This number can be important for troubleshooting purposes. A large number of in-progress processes may indicate that the Enterprise Server is running slowly and alert you that you need to investigate the possible causes.

29.2.2.1.1 Reset Statistic The *Reset Statistic* button will reset the statistics for the selected business functions.

29.2.3 JDBj Database Caches

JDBj Database Caches cache management enables one to select the Instance that they want to look at, and within the Instance the Cache name that they want to track. Based on this selection the appropriate JDBj Service Cache metrics are displayed. Caches maintained by the HTML server may be viewed and cleared across a single or multiple instances.



In the *Instance Name* field, select the instance name of the managed instance from which you wish to view user sessions, or select ALL to view all instances. After making the selection, click the *Submit Query* button.

The fields in the Cache Management section are:

- *Instance Name*

  All can be selected which will display every instance selected, or an individual instance can be selected. The selections available are:

  All

  individual instance name

  home

- *Cache Name*

  All can be selected which will display every cache within the instance selected, or an individual cache can be selected.

  Values available are:

  Data Dictionary Glossary Text

  Data Dictionary Alpha Cache

  Row Column Cache

  JDBJ Security Cache

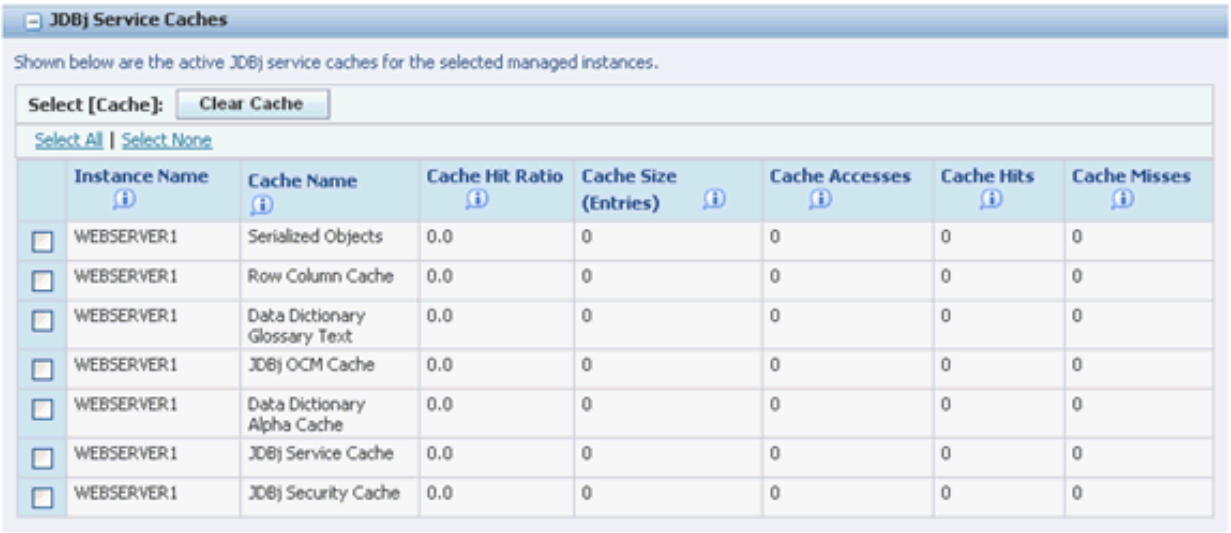
  JDBJ Service Cache

  Serialized Objects

  Menu Cache

Select a value from the Instance Name and Cache Name field. When both fields have been selected, then click on the Submit Query button.

29.2.3.1 JDBj Service Caches



JDBj Services Caches are displayed for the selected managed instances.

- *Instance Name*

  This will display based on the Instance Name selected in the previous Instance Name drop down selection. The unique name assigned to the managed instance at the time it was created or registered.

- *Cache Name*

  This will display based on the Instance Name selected in the previous Instance Name drop down selection. The name of the JDBj service cache.

- *Cache Hit Ratio*

  The ratio of cache requests that find an object in cache, as a faction of 1.

- *Cache Size (Entries)*

  The number of items that are stored with the cache.

- *Cache Accesses*

  The total number of requests the cache has serviced.

- *Cache Hits*

  The total number of requests the cache has serviced and returning a matched result.

- *Cache Misses*

  The total number of requests the cache has serviced and did not find within its cache.

29.2.3.2 Clear Cache

The *Clear Cache* button will clear cache for the selected Instance/JVM.

29.2.4 Database Connections

Database connections and prepared statement caches can be viewed across a single instance or multiple instances simultaneously. The Database Connections hyperlink will link to the JDBj Connection Caches screen.

The Instance Name field allows for all instances to be selected which will display every instance, or an individual instance can be selected. Once the Instance Name has been selected, click the Submit Query button.

- *Instance Name*

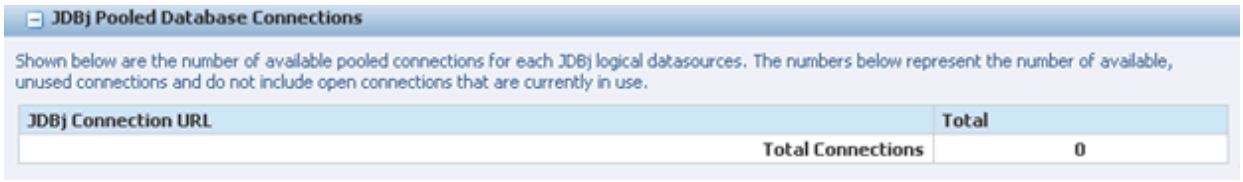
  All can be selected which will display every instance selected, or an individual instance can be selected. The selections available are:

  All

  individual instance name

  home

29.2.4.1 JDBj Pooled Database Connections



JDBj Pooled Database Connections shows the number of available pooled connections for each JDBj logical data source. The numbers below represent the number of available, unused connections and do not include open connections that are currently in use.

29.2.4.2 Prepared Statement Cache Detail

The Prepared Statement Cache Detail shows each of the SQL prepared statements being cached on each managed web server. The numbers indicate the number of pooled database connections that are caching that prepared statement. These values are further broken down by the logical database connection URL.

Note: Prepared statement caches are not maintained for the Oracle products; Oracle products use the Oracle native prepared statement caching instead.

29.2.5 JDBj Runtime

The JDBj Runtime screen allows for viewing or modifying the runtime configuration of JDBj, which can be done across a single instance or multiple instances simultaneously.

In the *Instance Name* field, select the instance name of the managed instance from which you wish to view user sessions, or select ALL to view all instances. After making the selection, click the *Submit Query* button.

- *Instance Name*

  All can be selected which will display every instance selected, or an individual instance can be selected. The selections available are:

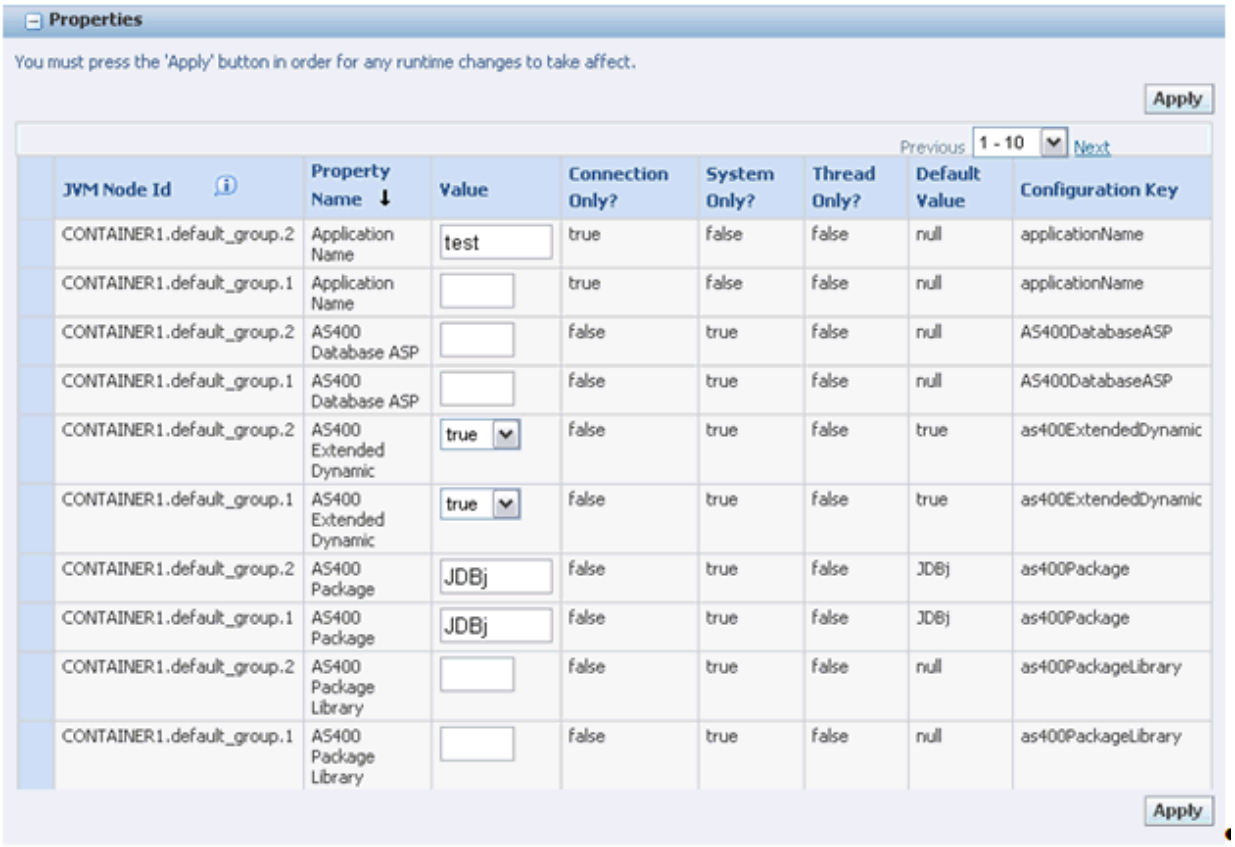
  All

  individual instance name

  home

29.2.5.1 Properties

The *Properties* section allows the Value of the property to by dynamically changed.



The Properties section allows the value of the property to by dynamically changed.

- *Value*

  The current value in use for the property. This value may be defined in a drop down menu or may be a text field that allows free-form entry of the value.

29.2.5.2 Apply

When a value has been entered, click the Apply button to dynamically apply the change.

29.2.6 JDENET Stats

The JDENET Stats hyperlink connects to the JDENET Connections screen, which has these sections:

- JDENET Connections
- JDENET Connection Pools
- JDENET Socket Connections

29.2.6.1 JDENET Connections

EnterpriseOne web products maintain a pool of JDENET connections that are shared among all the active users of the web product. A connection pool is created for each foreign host, such as an Enterprise Server, that the web product contacts using JDENET. Each connection pool has a number of established JDENET connections to the foreign host. A request to a particular host will use one of these sockets, or if no sockets are available, wait until a socket in the pool becomes available.

Viewing the JDENET statistics for connections established by the HTML server can be viewed across a single instance or multiple instances simultaneously.

The *Instance Name* field allows for all instances to be selected which will display every instance, or an individual instance can be selected. Once the Instance Name has been selected, the screen will refresh with the updated information. In the *Instance Name* field, select the instance name of the managed instance from which you wish to view user sessions, or select ALL to view all instances.

- *Instance Name*

  All can be selected which will display every instance selected, or an individual instance can be selected. The selections available are:

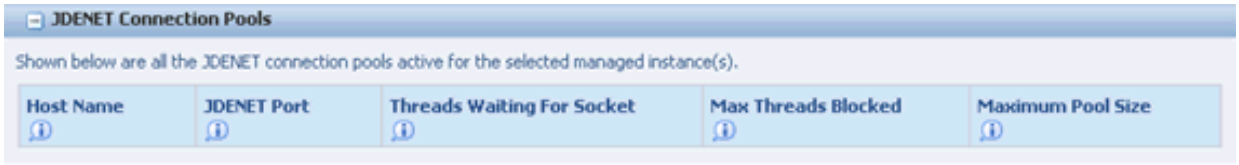
  All

  individual instance name

  home

29.2.6.2 JDENET Connection Pools

The JDENET Connection Pool Information view displays connection and messaging data for each Enterprise Server connected to the web server. Information about the volume of data and messages transmitted and received is contained in this set of parameters:



- *Host Name*

  The name of the Enterprise Server the connection pool represents.

- *JDENET Port*

  The JDENET port used to initially contact the Enterprise Server.

- *Threads Waiting for Socket*

  The number of threads that are currently waiting to use a socket connection contained within this thread pool. If this number is non-zero then one or more threads are being held up. In this case it may be beneficial to increase the maximum pool size.

- *Max Threads Blocked*

  The maximum number of threads that have been simultaneously been waiting for a socket from the connection pool.

- *Maximum Pool Size*

  The maximum number of sockets that may be created for this connection pool. Once this threshold is retrieved any additional threads attempting to connect to the Enterprise Server/port will wait until a in use socket is returned to the pool.

29.2.6.3 JDENET Socket Connections

JDENET Socket Connections displays all of the available socket connections in the connection pools for the selected managed instance(s). Sockets currently in use (check-out) are not displayed.

The grid fields for JDENET Socket Connections are:

- *Enterprise Server*

  The name of the Enterprise Server the connection pool represents.

- *Local TCP/IP Port*

  The TCP/IP port actually used by the connection.

- *Enterprise Server Connect Port*

The initial port (connect port) used to contact the Enterprise Server.

- *Actual Foreign Port*

  The actual port on the Enterprise Server used.

- *Socket Good?*

  If true the socket is valid and usable.

- *Timeout (ms)*

  Timeout in milliseconds.

- *Messages Written*

  The number of JDENET messages that have been written on the socket connection.

- *Bytes Written*

  The number of bytes that have been written on the socket connection.

- *Socket in Use?*

  If true the socket is in use by a thread

- *Checkout Time*

  The time the socket was checked out by the thread using it.

29.2.7 Java Environment

The java environment runtime metrics provide insight into the JVM(s) running the EnterpriseOne Web products. This information may be helpful in understanding or troubleshooting the java environment in which these products operate. The Java Environment hyperlink, when selected, will link to the Java Environment Runtime Detail screen.

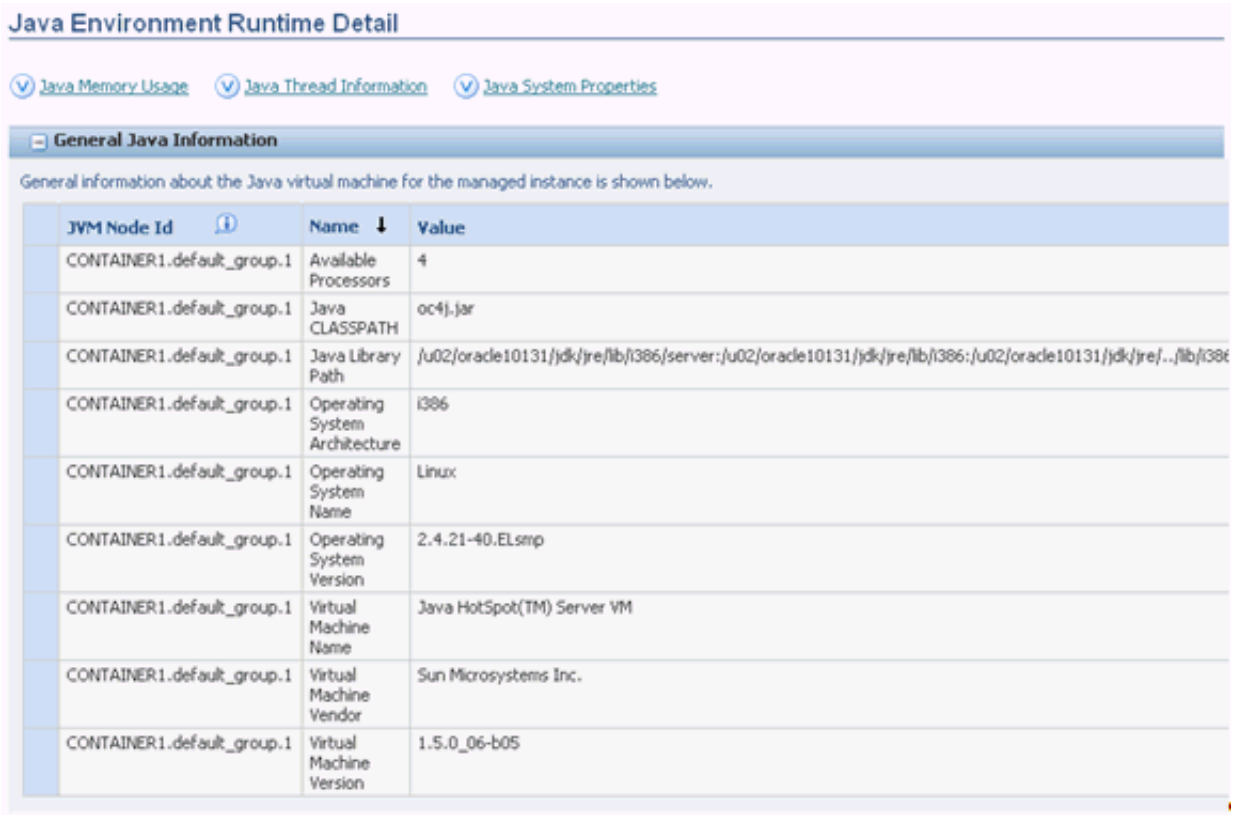
29.2.7.1 Java Environment Runtime Detail

Viewing Java JVM runtime information such as memory used, threads created, and system properties can be viewed across a single instance or multiple instances simultaneously. Garbage collection on the JVM may also be invoked.

The Java Environment Runtime Detail information includes:

- General Java Information
- Java Memory Usage
- Run Garbage Collection
- Java Thread Information
- Java System Properties

29.2.7.1.1 General Java Information



General information about the Java virtual machine for the managed instance is displayed in the General Java Information section:

- *JVM Node Id*

  An identifier that uniquely identifies a single JVM.

- *Name*

  A description of the java system property.

- *Value*

  The value of the system property.

29.2.7.2 Java Memory Usage

Information about the current memory usage is available. The information is current at the time the page is initially loaded.

29.2.7.3 Run Garbage Collection

Each container will have a Run Garbage Collection button that initiates the garbage collection process for each container providing more current usage information.

29.2.7.4 Java Thread Information

Each of the threads contained within the JVM are displayed.

- *Thread Name*

  The name of the java thread.

- *Thread Group*

  The group in which the thread belongs.

- *Is Alive?*

  True if the current thread.

- *Is Daemon Thread*

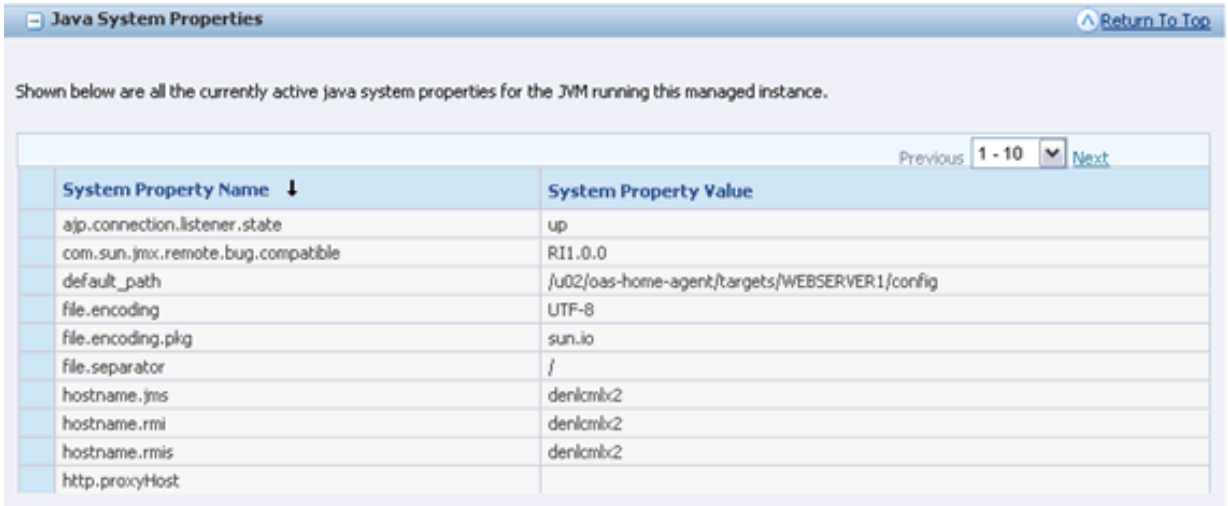
  True if the thread is a daemon, or background thread.

- *Thread Priority*

  The priority assigned to the thread.

29.2.7.5 Java System Properties

The Java System Properties displays all of the java system properties. This list is current at the time the page is loaded.



The Java System Properties displayed are:

- *System Property Name*

  The name of the system property.

- *System Property Value*

  The value of the system property.

29.3 Application Interface Services Server Runtime Metrics (Release 9.1 Update 5)

Runtime metrics for Application Interface Services Servers provide metric information for:

- AIS Information
- Login Metrics
- User Info Metrics
- Runtime Configuration
- Form Metrics
- Session Metrics
- Java Environment

29.3.1 AIS Information

The AIS Information section provides metrics for:

- AIS JVM Count
- AIS Uptime
- Online Users

See the context sensitive help for more information on each metric.

29.3.2 Login Metrics

Displays the login request and response metrics for the AIS Server.

29.3.3 User Info Metrics

Displays user information contained in the F0092 table.

29.3.4 Runtime Configuration

Displays the runtime configuration settings being used by the AIS Server.

29.3.5 Form Metrics

Displays the form related metrics specific to user activity with a particular application and form.

29.3.6 Session Metrics

Displays the user session SSO metrics.

29.3.7 Java Environment

See: 29.2.7.1 , "Java Environment Runtime Detail"

29.4 Transaction Server Administration

The Transaction Server Admin section has hyperlinks for:

- Failed Events
- Subscribers
- Event Metrics

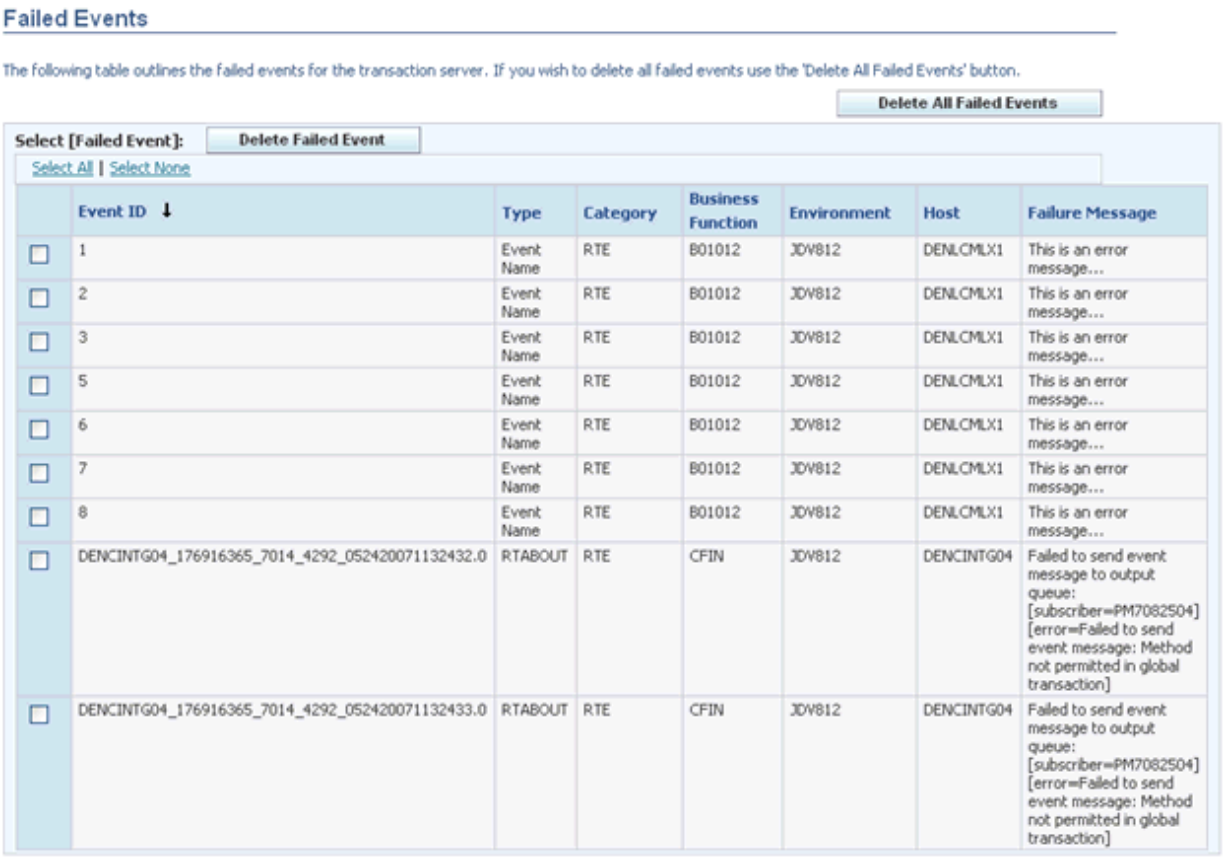
29.4.1 Failed Events

The Failed Events section contains:

- Select [Failed Events]
- Delete Failed Events
- Delete All Failed Event

29.4.1.1 Select [Failed Events]

Failed Events and their associated failure messages are listed for the transaction server.



Event ID	Type	Category	Business Function	Environment	Host	Failure Message
1	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
2	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
3	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
5	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
6	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
7	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
8	Event Name	RTE	B01012	JDV812	DENLCMLX1	This is an error message...
DENCINTG04_176916365_7014_4292_05242007113243 2.0	RTABOUT	RTE	CFIN	JDV812	DENCINTG04	Failed to send event message to output queue: [subscriber=PM7082504] [error=Failed to send event message: Method not permitted in global transaction]
DENCINTG04_176916365_7014_4292_05242007113243 3.0	RTABOUT	RTE	CFIN	JDV812	DENCINTG04	Failed to send event message to output queue: [subscriber=PM7082504] [error=Failed to send event message: Method not permitted in global transaction]

29.4.1.2 Delete Failed Events

The *Delete Failed Event* button will delete selected events.

29.4.1.3 Delete All Failed Event

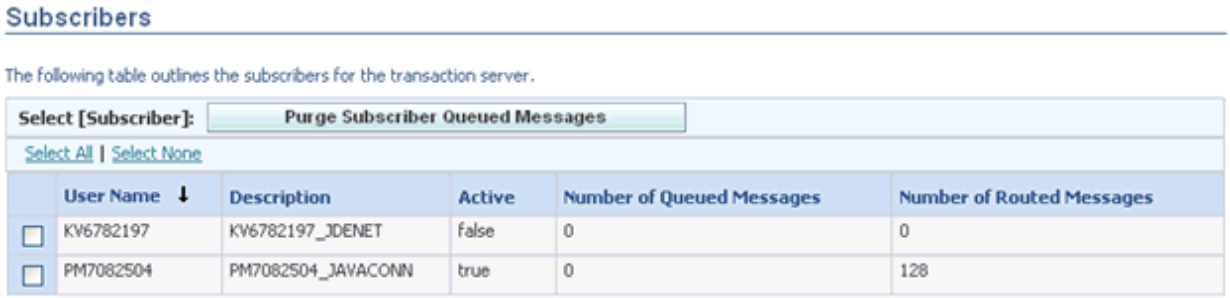
The *Delete All Failed Events* button will delete all failed events.

29.4.2 Subscribers

The Subscribers section contains:

- Select [Subscriber]
- Purge Subscriber Queued Messages

29.4.2.1 Select [Subscriber]



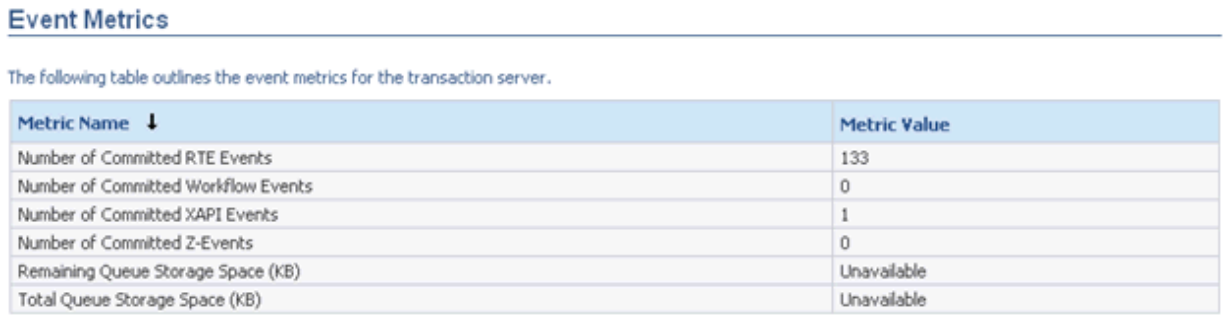
The subscribers section outlines the subscribers for the transaction server.

29.4.2.2 Purge Subscriber Queued Messages

The *Purge Subscriber Queued Messages* button, when selected, will purge all subscriber queued messages.

29.4.3 Event Metrics

The Event Metrics section outlines the event metrics for the transaction server. Information is provided for the *Metric Name* and the Metric Value grid fields.



30

Configure EnterpriseOne Server Instances

This chapter discusses:

- Section 30.1, "Configuration Overview (Release 9.1, Update 4)"
- Section 30.2, "General and Instance Properties"
- Section 30.3, "Instance Properties"
- Section 30.4, "Available Log Files"
- Section 30.5, "Configuration Groups"
- Section 30.6, "Configuration Items"
- Section 30.7, "Compare Instances"
- Section 30.8, "Troubleshooting the Configuration of EnterpriseOne Server Instances"

30.1 Configuration Overview (Release 9.1, Update 4)

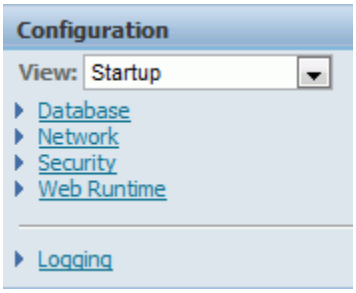
Every configuration setting (*.INI, .PROPERTIES, etc.) is manageable through the management console. The configuration files still exist in the same form as prior tools releases. The management console provides a front end for modifying the configuration values and adds the following benefits:

- Every configuration item is present and documented with online help.
- A list of values, when applicable, is used for settings that have distinct allowed values.
- Changes to configuration settings are recorded for historical analysis and auditing, including the user that made the change.
- The configurations of multiple managed instances may be compared to identify differences.
- New configuration settings are merged into existing configuration files when a tools release upgrade is performed.

Configuration is accessed from the management page for an instance. Configuration settings are grouped into high level categories. Selecting a category displays all the settings contained within.

Note: New categories are available in release 9.1.4.

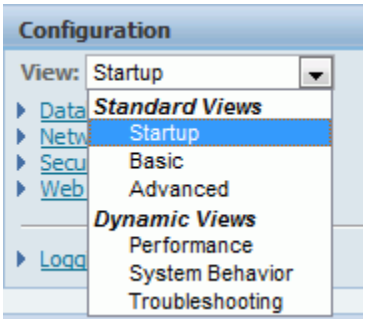
Figure 30–1 Configuration



Each high level category is divided into sub-categories containing the individual configuration parameters.

There is also a drop down menu that displays options for Standard and Dynamic views.

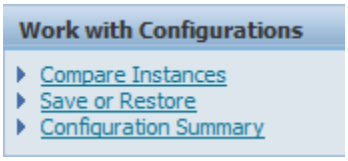
Figure 30–2 Configuration Dropdown



The Work with Configurations section provides the following:

- Compare Instances
- Save or Restore
- Configuration Summary

Figure 30–3 Work With Configurations



30.1.1 Save or Restore

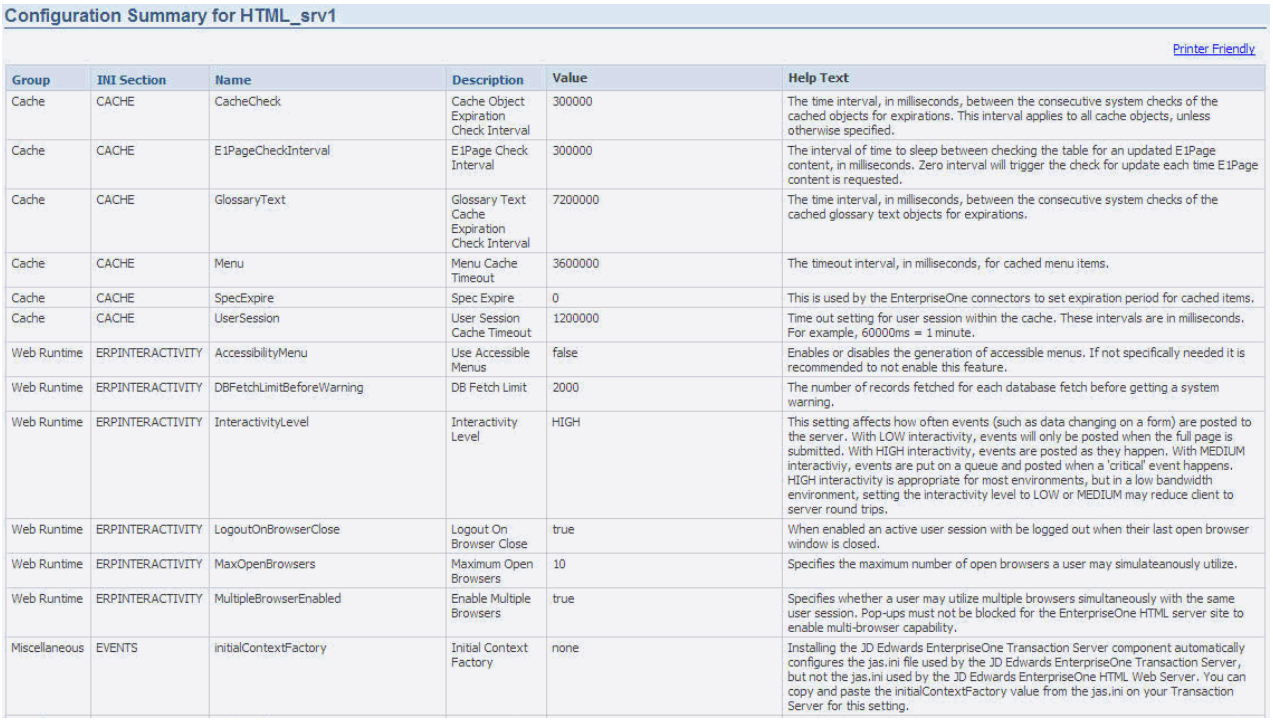
Save or Restore allows users to:

1. Save a copy of the current configuration for later reference.
2. Restore the configuration to a previously saved state.
3. Export a saved configuration to a zip file format (by clicking on the link to the configuration name)
4. Import a previously exported configuration from another instance or server.

30.1.2 Configuration Summary

The Configuration Summary provides a list of all current configuration values for an instance on one page.

Figure 30–4 Configuration Summary



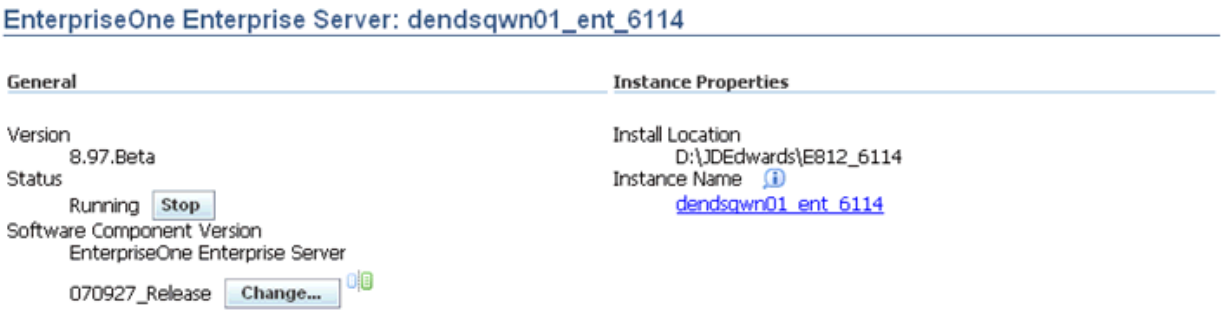
Configuration Summary for HTML_srv1

Printer Friendly

Group	INI Section	Name	Description	Value	Help Text
Cache	CACHE	CacheCheck	Cache Object Expiration Check Interval	300000	The time interval, in milliseconds, between the consecutive system checks of the cached objects for expirations. This interval applies to all cache objects, unless otherwise specified.
Cache	CACHE	E1PageCheckInterval	E1Page Check Interval	300000	The interval of time to sleep between checking the table for an updated E1Page content, in milliseconds. Zero interval will trigger the check for update each time E1Page content is requested.
Cache	CACHE	GlossaryText	Glossary Text Cache Expiration Check Interval	7200000	The time interval, in milliseconds, between the consecutive system checks of the cached glossary text objects for expirations.
Cache	CACHE	Menu	Menu Cache Timeout	3600000	The timeout interval, in milliseconds, for cached menu items.
Cache	CACHE	SpecExpire	Spec Expire	0	This is used by the EnterpriseOne connectors to set expiration period for cached items.
Cache	CACHE	UserSession	User Session Cache Timeout	1200000	Time out setting for user session within the cache. These intervals are in milliseconds. For example, 60000ms = 1 minute.
Web Runtime	ERPINTERACTIVITY	AccessibilityMenu	Use Accessible Menus	false	Enables or disables the generation of accessible menus. If not specifically needed it is recommended to not enable this feature.
Web Runtime	ERPINTERACTIVITY	DBFetchLimitBeforeWarning	DB Fetch Limit	2000	The number of records fetched for each database fetch before getting a system warning.
Web Runtime	ERPINTERACTIVITY	InteractivityLevel	Interactivity Level	HIGH	This setting affects how often events (such as data changing on a form) are posted to the server. With LOW interactivity, events will only be posted when the full page is submitted. With HIGH interactivity, events are posted as they happen. With MEDIUM interactiviy, events are put on a queue and posted when a 'critical' event happens. HIGH interactivity is appropriate for most environments, but in a low bandwidth environment, setting the interactivity level to LOW or MEDIUM may reduce client to server round trips.
Web Runtime	ERPINTERACTIVITY	LogoutOnBrowserClose	Logout On Browser Close	true	When enabled an active user session with be logged out when their last open browser window is closed.
Web Runtime	ERPINTERACTIVITY	MaxOpenBrowsers	Maximum Open Browsers	10	Specifies the maximum number of open browsers a user may simulateanously utilize.
Web Runtime	ERPINTERACTIVITY	MultipleBrowserEnabled	Enable Multiple Browsers	true	Specifies whether a user may utilize multiple browsers simultaneously with the same user session. Pop-ups must not be blocked for the EnterpriseOne HTML server site to enable multi-browser capability.
Miscellaneous	EVENTS	initialContextFactory	Initial Context Factory	none	Installing the JD Edwards EnterpriseOne Transaction Server component automatically configures the jas.ini file used by the JD Edwards EnterpriseOne Transaction Server, but not the jas.ini used by the JD Edwards EnterpriseOne HTML Web Server. You can copy and paste the initialContextFactory value from the jas.ini on your Transaction Server for this setting.

30.2 General and Instance Properties

When you click an instance name from the list of servers the Management Console displays another page called *server name: instance name*.



In the *General* section of the page you can:

- Start or stop a Managed Instance.

  Refer to the section entitled: Start or Stop a Managed EnterpriseOne Software Component in this guide.

- Change a Software Component Version.

  Refer to the section entitled: Change a Managed EnterpriseOne Software Component in this guide.

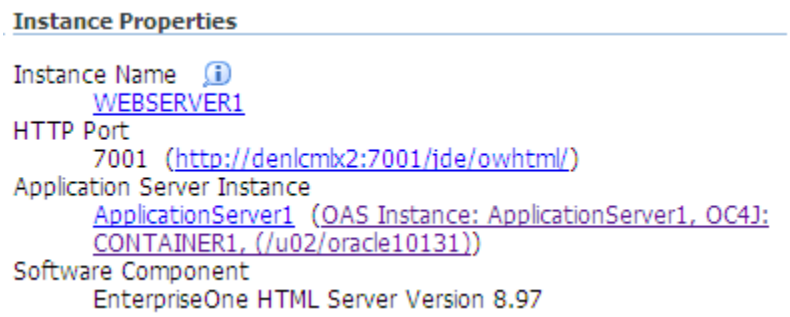
- View Software Release History.

  Refer to the section entitled: View the Software Release History for a Managed Instance in this guide.

30.3 Instance Properties

The Instance Properties section of the page lists specific properties for a managed instance. For example, the properties for a Managed Instance for a JD Edwards EnterpriseOne HTML Web Server would include:

- Instance Name
- HTTP Port
- Application Server Instance
- Software Component



30.4 Available Log Files

Refer to the section entitled: Available Log Files in this guide.

30.5 Configuration Groups

The Configuration section displays a list of Configuration Groups that varies according to the server type. This section lists the Configuration Groups for these JD Edwards EnterpriseOne servers:

- EnterpriseOne Enterprise Server
- EnterpriseOne HTML Server
- EnterpriseOne Business Services Server
- EnterpriseOne Application Interface Services Server (Release 9.1 Update 5)
- EnterpriseOne Transaction Server
- EnterpriseOne Data Access Server
- EnterpriseOne Data Access Driver

30.5.1 EnterpriseOne Enterprise Server

This section lists these Configuration Groups for an Enterprise Server:

- Batch Processing
- Database

- Installation
- Interoperability
- Kernel Definitions
- Logging and Diagnostics
- Miscellaneous
- Network and IPC
- Package Builds
- Security

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.5.2 EnterpriseOne HTML Server

This section lists these Configuration Groups for a HTML Web Server:

- Cache
- Database
- Miscellaneous
- Network
- Security
- Web Runtime

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.5.3 EnterpriseOne Business Services Server

This section lists these Configuration Groups for a Business Services Server:

- Cache
- Database
- HTTP Settings
- Inbound Settings
- Miscellaneous
- Network
- Runtime Settings
- Security

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.5.4 EnterpriseOne Application Interface Services Server (Release 9.1 Update 5)

This section lists these Configuration Groups for an Application Interface Services Server:

- Display

- JAS Information
- Security Information
- Logging

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.5.5 EnterpriseOne Transaction Server

This section lists these Configuration Groups for a Transaction Server:

- Database
- Network
- Real Time Events
- Security

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.5.6 EnterpriseOne Data Access Server

This section lists these Configuration Groups for a Data Access Server:

- JDBJ Database Configuration
- Network Settings

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.5.7 EnterpriseOne Data Access Driver

This section lists these Configuration Groups for a Data Access Server:

- Database
- Installation
- Network
- Security

For details of each Configuration setting within a configuration group, refer to the Server Manager internal help for each setting.

30.6 Configuration Items

This section describes:

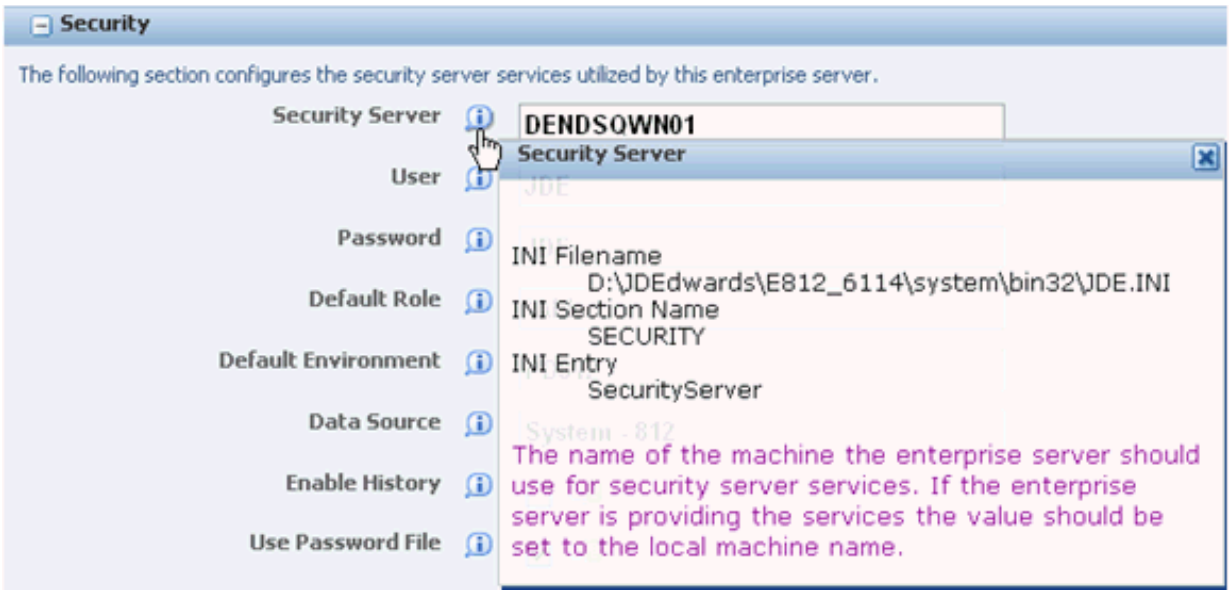
- Help
- History

30.6.1 Help

Each configuration item is identified using a short, readable name. Clicking the Help icon will link to the following information

- The INI section the parameter pertains to.

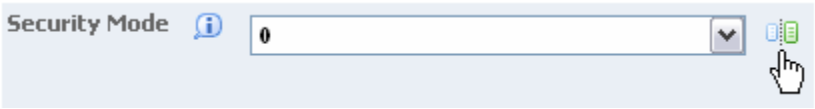
- The INI entry the parameter pertains to.
- The location of the INI file being updated.
- A list of allowed values, if applicable.
- An extended description detailing the purpose of the configuration parameter.
- The default value, if applicable.



30.6.2 History

History is maintained for each configuration item. The old and new values are recorded along with the user that made the change. Changes made directly to the configuration files are not audited.

To view History, click on the History icon.



The History - <configuration item> popup screen that appears contains these fields:

- *Date*

  The date the change occurred.

- *User*

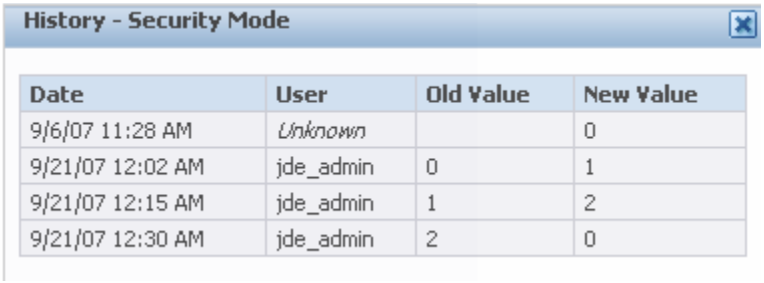
  The user that made the change.

- *Old Value*

  The value before the change.

- *New Value*

  The value after the change.



History may also be viewed for all configuration parameters for an instance.

See Also

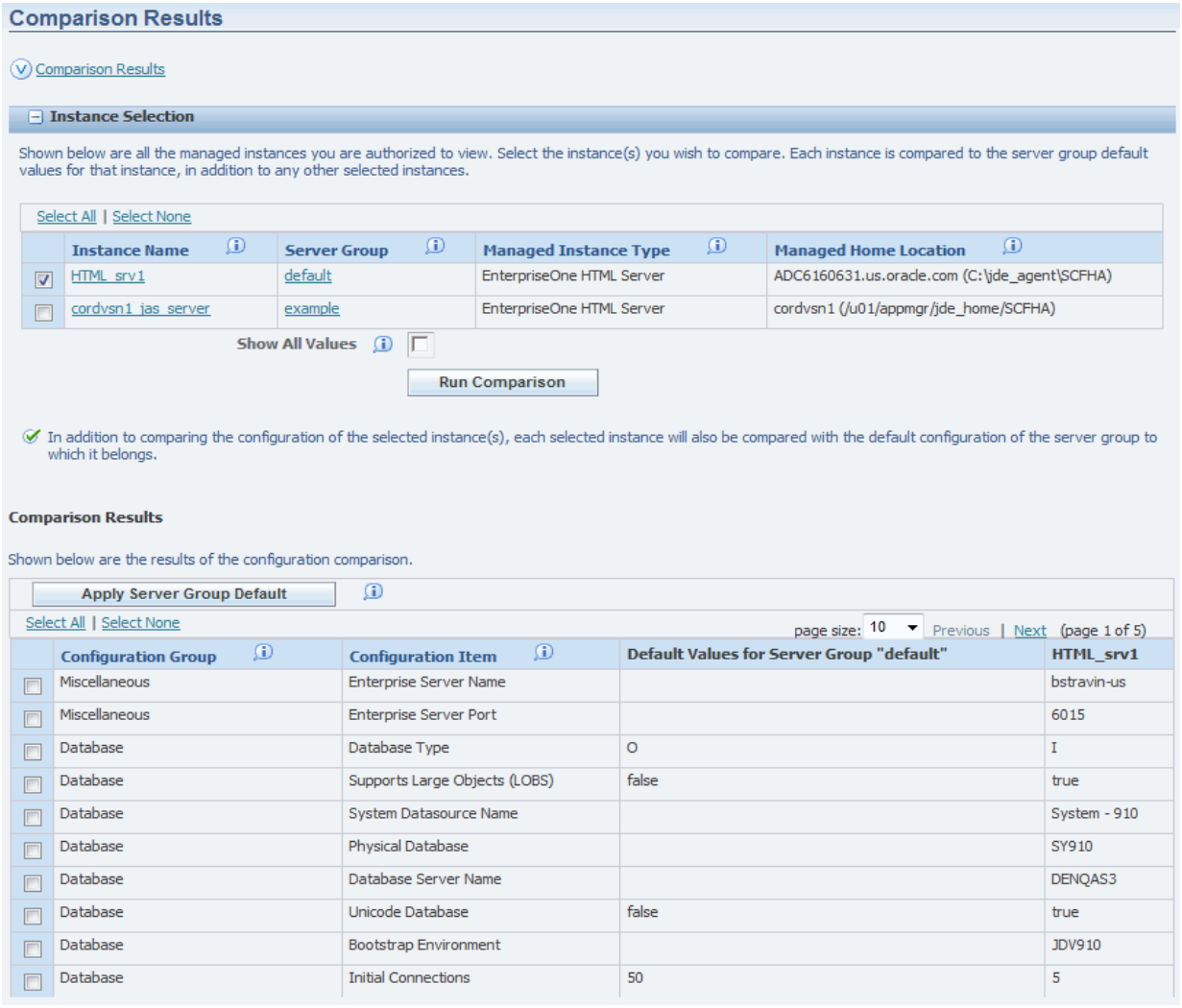
- Audit History

30.7 Compare Instances

Two or more managed instances may be selected to identify configuration differences. Each selected instance will also be compared with the default configuration of the server group to which it belongs.

This section describes:

- Create Comparison
- Comparison Results



30.7.1 Create Comparison

To create an instance comparison:

1. Click *Compare Instances* in the *Work With Configurations* section.
2. Select the check box for the instances to compare.
3. Select the check box for *Show All Values.*

   If selected all configuration items for each selected instance and corresponding server group(s) will be displayed. If not selected only configuration items that are not identical between the selected instances and their server groups will be displayed.
4. Click the *Run Comparison* button.

30.7.2 Comparison Results

This section describes:

- Results
- Modifications

30.7.2.1 Results

The comparison results appear in a new pane under the *Instance Selection* section.

The comparison is detailed by these columns:

- Configuration Metric

  Configuration items are associated into logical groupings, which are referred to as a Configuration Metric.

- Configuration Item

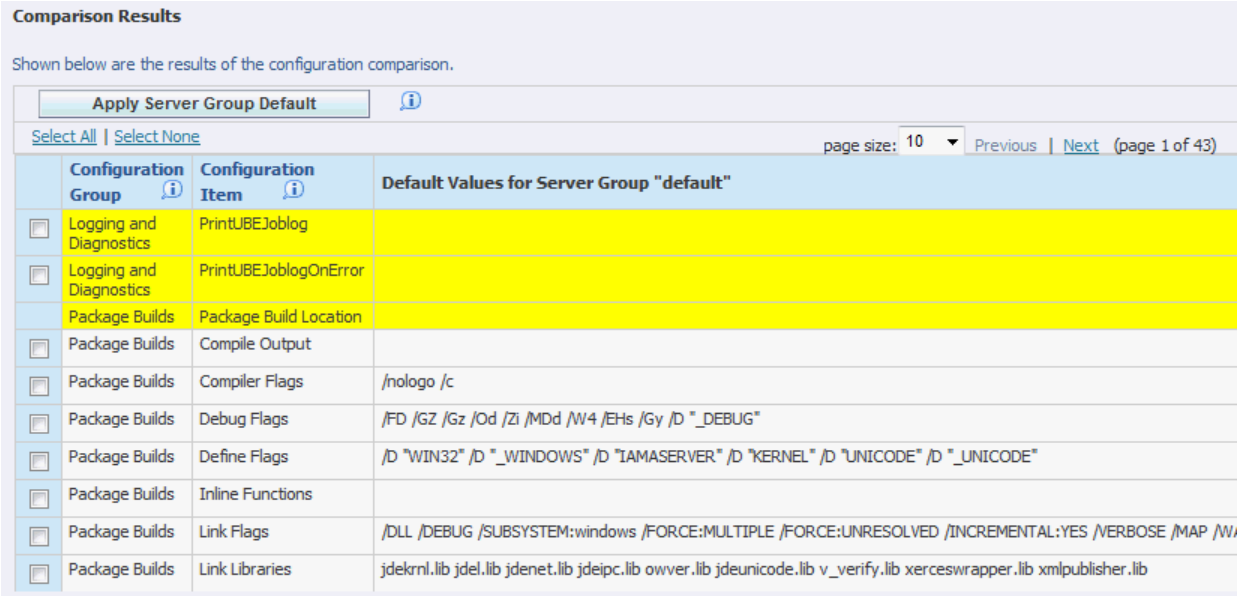
  The individual configuration item that is being compared between the selected instance(s) and their corresponding server group.

- Permissions for Server Group: <Server Group Name>

  Specifies configuration values.

- <Instance Name>

  Specifies configuration values and paths.



30.7.2.2 Modifications

You can apply the Server Group default values to an instance by selecting the configuration items and then selecting the *Apply Server Group Default* button.

30.8 Troubleshooting the Configuration of EnterpriseOne Server Instances

This section describes:

- Permission Denied

30.8.1 Permission Denied

If you receive an error that permission is denied to write to a configuration file, you need to ensure that the file is not purposely locked in a manner that prevents the user under which Server Manager is running from modifying it. You should check the file permissions to ensure the file is writable.

31

Administer Server Groups

This chapter provides an overview of server groups and discusses how to:

- Section 31.1, "Overview of Server Groups"
- Section 31.2, "Manage Server Groups"

31.1 Overview of Server Groups

In Server Manager, you manage servers by grouping similarly purposed servers into logical groupings called server groups. You determine how you want to group servers depending on your particular JD Edwards EnterpriseOne implementation. For example, you may want to put all production servers in one server group and manage development servers in another. Or, you may decide to place servers in separate server groups based on geographical location. How you organize and manage servers in server groups is up to you.

The Management Console provides a default server group that you can use to initially manage servers. You can move any server from the default server group to a newly created server group. A server cannot belong to more than one server group, including the default server group.

You can include the following types of servers in a server group:

- JD Edwards EnterpriseOne Enterprise Server
- JD Edwards EnterpriseOne HTML Server
- JD Edwards EnterpriseOne Collaborative Portal Server
- Transaction Server
- PIM Synch Server
- Business Services Server

In the Management Console, you can configure default configuration settings for each type of server in a server group. When you add a server to a server group, Server Manager automatically applies the default configuration settings for that type of server to the newly added server.

Note: You can manage and monitor certain features of application servers (Oracle Application Server or IBM WebSphere Application Server) through the Management Console, but these types of servers cannot be members of a server group. See Overview of Basic Instance Administration for more information.

31.1.1 Server Group Security

Server Manager contains a set of server group permissions that enable you to control the activities Management Console users can perform on the servers within a particular server group. This layer of security enables you to control the tasks that Management Console users can perform on a server as well as the configuration data that they can access. You can grant permissions that allow a set of users to perform certain types of tasks in one server group, but not another. For example, you can permit developers total access to a server group that manages servers for a test environment, but not give the same developers access to production servers managed in another server group.

Security for server groups, or server group permissions, is assigned to user groups. See Assign Server Manager Permissionsfor more information.

31.2 Manage Server Groups

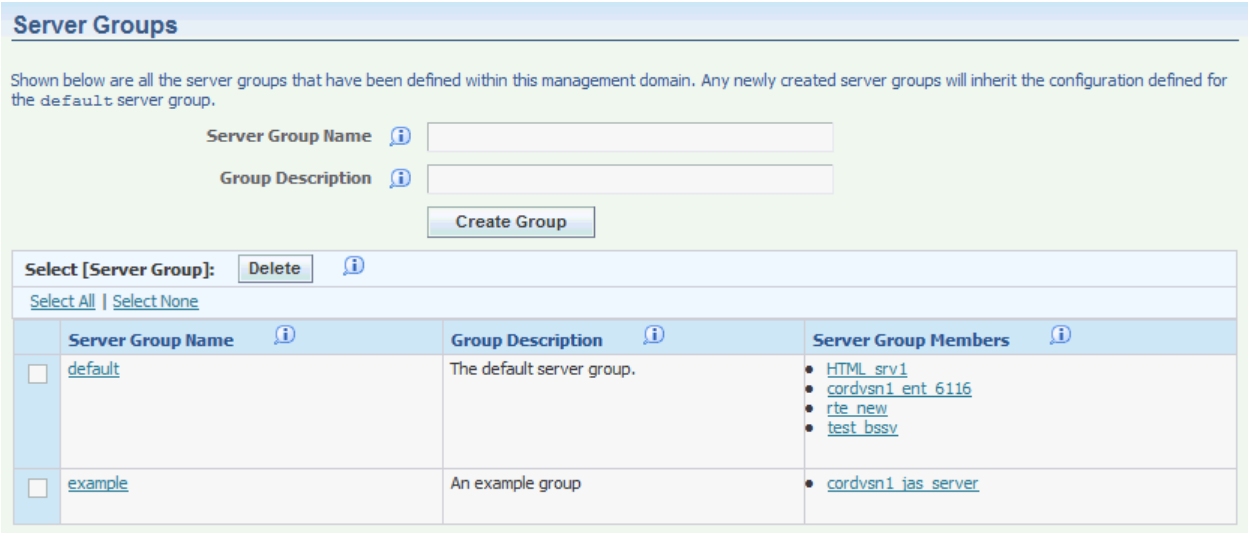
You can create your own unique server groups to manage different sets of servers. How you choose to manage servers in server groups, and whether you choose to use server groups at all or just manage all servers in the default server group, is up to you.

Note: When you create a server group, the Management Console copies default configuration settings from the default server group to the new server group. In the new server group, you can modify the default configuration settings as appropriate.

31.2.1 Create Server Group

To create a server group:

1. In the Quick Links section of the Management Console, click the Server Groups link.



2. On Server Groups, enter a unique name in the Server Group Name field.
3. Complete the Group Description field.
4. Click the Create Group button.

   The Management Console displays the new server group in the grid.

Note: You must have the consoleConfig permission to create a new server group.

31.2.2 Modify Server Group

This section describes:

- Add Server Group Members
- Delete Server Group

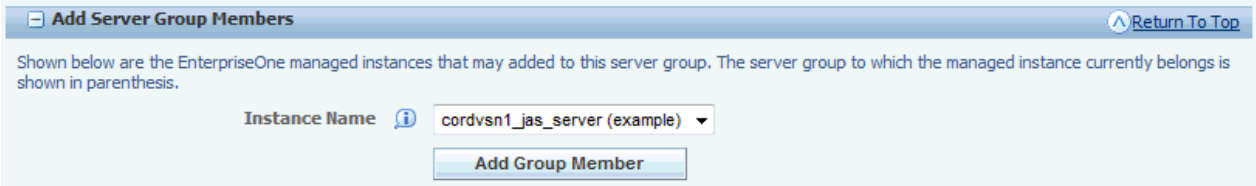
31.2.2.1 Add Server Group Members

You can move servers from the one server group to another server group, provided a second server group has been created. Moving a server changes its group membership only; it does not modify the configuration of the server.

A server, or managed instance, cannot belong to more than one server group.

To add server group members:

1. In the Quick Links section of the Management Console, click the *Server Groups* link.
2. On Server Groups, click the group name link for the group that you want to add a server to the server group.



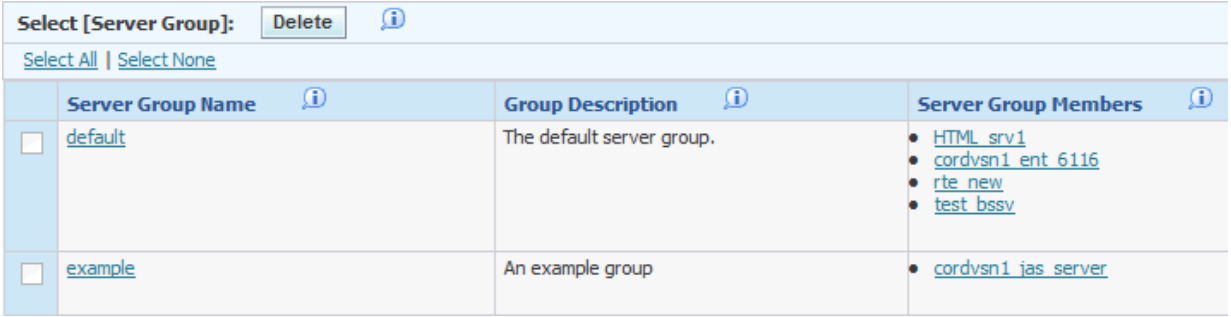
3. In the Add Server Group Members section, click the *Instance Name* drop-down menu to select a managed instance (server) that you want to migrate to the server group. The list contains all the servers that do not belong to the current server group. The group to which the servers belong is shown in parenthesis.
4. Click the *Add Group Member* button to add the server as a member of the server group.

   The system displays all members of the server group under the Server Group Members heading.

31.2.2.2 Delete Server Group

To delete a server group:

1. 1. On Server Groups, click the check box next to the server group that you want to delete.



2. Click the *Delete* button.

Note: You may not remove a server group that has server members.

32

Clear Table Cache (Tools Release 9.1 Update 2)

This chapter discusses these topics:

- Section 32.1, "Understanding Clear Table Cache"
- Section 32.2, "Using the Clear Table Cache Feature"

32.1 Understanding Clear Table Cache

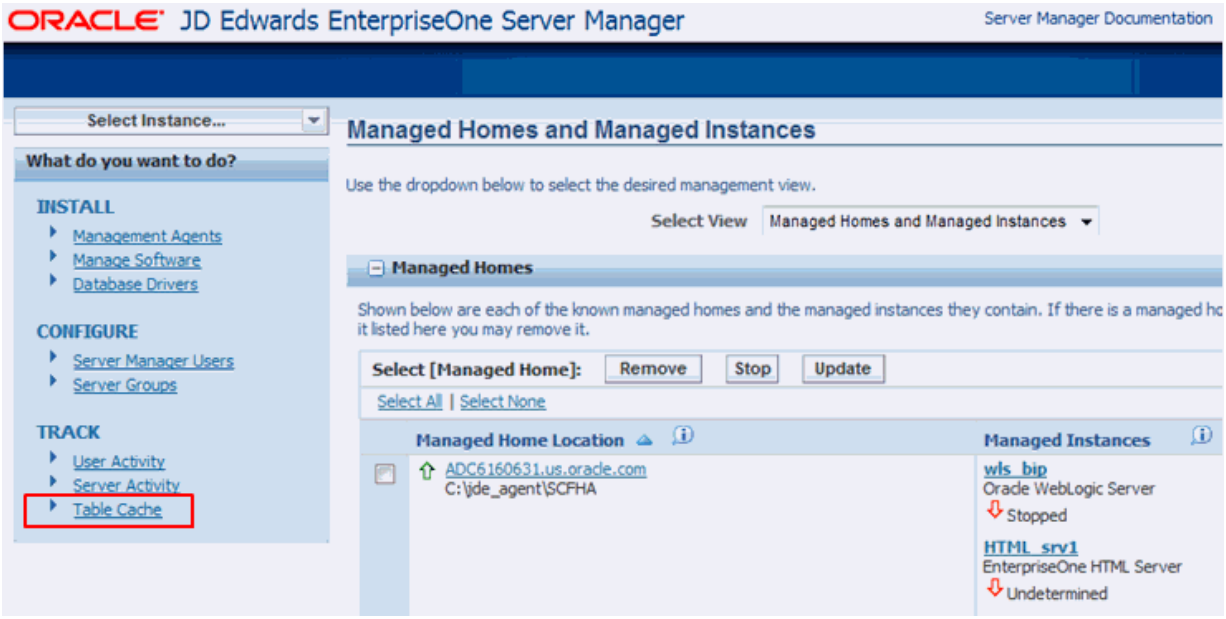
Beginning with Tools Release 9.1 Update 2, a JDB feature called Clear Table Cache can be used to improve performance by caching specific tables in the Call Object Kernel. For tables cached by JDB, any update or delete of a record in a cached table requires a clear of the cache on that kernel for the data to be available to all users. The adoption of the JDB Clear Cache API in specific EnterpriseOne Applications provides up-to-date data availability. CNC administrators with administrator access can use Server Manager to perform a dynamic cache refresh while users are logged on.

Clear Table Cache refresh allows a specific JDB table cache that is registered in the F98613 table to be cleared across kernel processes and across all Enterprise Servers as long as they are managed by the same Server Manager. As a result, all Enterprise Servers and all JD Edwards EnterpriseOne HTML Web Servers managed by the same Server Manager no longer need to be bounced (restarted) in order to clear cache. Since there is no table caching for the HTML Web Servers, it is not necessary to clear the cache on those machines.

32.2 Using the Clear Table Cache Feature

To use the Clear Table Cache feature in Server Manager:

1. Launch the Server Manager Management Console.

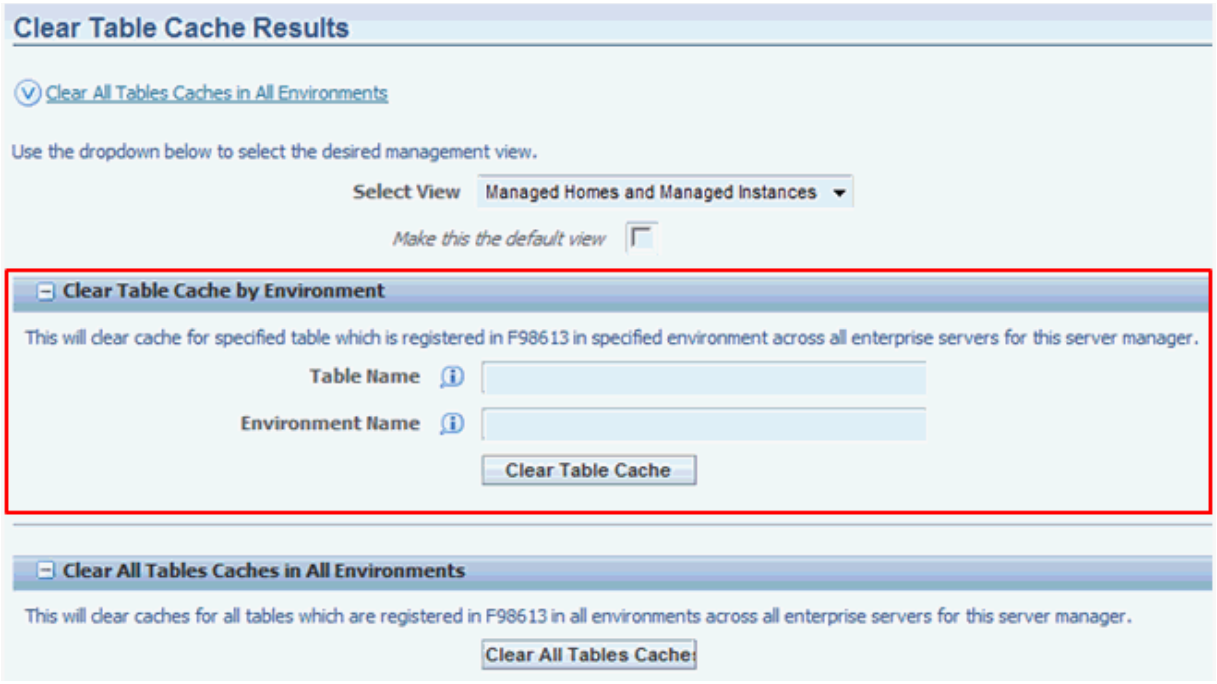


2. In the *What do you want to do?* section, click the **Table Cache** link.

3. On the Clear Table Cache Results page there are two sections:
   - Section 32.2.1, "Clear Table Cache by Environment"
   - Section 32.2.2, "Clear All Tables Caches in All Environments"

32.2.1 Clear Table Cache by Environment

To clear all caches for all tables which are registered in F98613 in all environments across all Enterprise Servers that are managed by the same Server Manager:



1. On the Clear Table Cache Results page, go to this section:

   Clear Table Cache by Environment

2. Complete these fields:

   - *Table Name*

     Enter a valid table name that is registered as a cached table in F98613 table using the P98613 application.

   - *Environment Name*

     Enter a valid JD Edwards EnterpriseOne environment from which the table cache will be cleared.

3. Click the **Clear Table** Cache button.

   The system displays a section that lists all cache that has been cleared for the requested table. For example, if you chose the F0010 table and the JDV910SA1 environment the following is displayed:

32.2.2 Clear All Tables Caches in All Environments

To clear all caches for all tables which are registered in F98613 in all environments across all Enterprise Servers that are managed by the same Server Manager:

1. On the Clear Table Cache Results page, go to this section:

   Clear All Table Caches by Environment

2. Click the **Clear All Table Caches** button.

   The system displays a section that lists all cache that has been cleared for all tables in the selected environment. An example is shown below.

A

Best Practices

This appendix discusses:

- Appendix A.1, "Multiple Management Consoles"
- Section A.2, "Management Agents"
- Section A.3, "Multiple Agents on a Single Machine"
- Section A.4, "Multiple WebSphere Application Servers"
- Section A.5, "Separate WAS Profiles"
- Section A.6, "Verify HTTP Ports"
- Section A.7, "HTTP Ports on UNIX Operating Systems"
- Section A.8, "Setting Up Windows Firewall in Windows Server 2008"

A.1 Multiple Management Consoles

If desired, you can install and operate multiple separate Management Console installations on a single machine. This model is supported in addition to the standard functionality whereby you can use a single Management Console to manage separate JD Edwards EnterpriseOne installations.

To install multiple Management Consoles on a single machine, you should install each Management Console in completely separate locations. The Management Console installer automatically detects a prior console installation and will properly configure any subsequent installations. This includes the configuration of the TCP/IP ports used by the embedded J2EE application server and the creation of the Microsoft Windows service name to ensure there are no conflicts. Additionally, you should ensure the HTTP port supplied during the Server Manager installation is unique and not currently in use. Refer to Verify HTTP Ports in this appendix.

When you are installing an additional Management Console on a machine it is important that the existing previous installations be stopped. There are two TCP/IP ports utilized by server manager that must be manually configured to prevent conflicts during the setup wizard:

- *Management Server JMX Port*

  This is the port on which the Management Console listens for incoming connections from remote Management Agents. The default value is 14501.

  You must define this value to an unused port on the machine. A good practice is to increase the value by 1000 to 15501 for the second console, 16501 for the third, and so on, provided those ports are not used by any other application running on the machine. You must properly set this value prior to installing any Managed Homes.

- *Management Agent Starting Port*

  This port is the start port the Management Console will assign to remote Management Agents. The default value is 14502.

  If you will be using the new Management Console to manage machines that are also managed from another Management Console, you must change this value. A good practice is to change this value anytime you change the *Management Agent Starting Port*. Unlike the *Management Server JMX Port*, you can change this port at any time, including after you have installed Managed Homes.

When you have properly configured these ports you can simultaneously start and run any other Management Console instances on the same machine.

A.2 Management Agents

This section describes these recommendations:

- One Agent Per Application Server Installation
- Management Agents on OAS
- Management Agents on JD Edwards EnterpriseOne Enterprise Servers
- Multiple Agents on a Single Machine

A.2.1 One Agent Per Application Server Installation

You should only use one Management Agent to manage an Application Server installation. The reason is because if you use multiple agents to manage the same application server it can lead to slow response times and unpredictable results such as this scenario:

- *Management Agent A*

  WAS61/Profile1/ServerA: EnterpriseOne HTML Server

- *Management Agent B*

  WAS61/Profile1/ServerA:

For the above two agents, *Management Agent B* cannot determine if *Management Agent A* has an *EnterpriseOne HTML Server* installed on *WAS61/Profile1/ServerA*. As a result, if you start or stop *ServerA* you would also unknowingly start or stop the JD Edwards EnterpriseOne HTML Web Server.

A.2.2 Management Agents on OAS

In order for Server Manager to manage OAS, you should install the Management Agent on your machine that has Oracle Application Server as the *oracle* user. Additionally, you should enable the Management Agent to run as the *oracle* user.

For UNIX systems, if you cannot install the agent as a non-root user (for example, on AIX), then install the agent as the *ROOT* user and then change the owner using the `chown` command.

Before proceeding, you should ensure that you stop the Management Agent and select it with the new owner.

A.2.3 Management Agents on JD Edwards EnterpriseOne Enterprise Servers

In order for Server Manager to manage JD Edwards EnterpriseOne Enterprise Servers, you should install the Management Agent as the EnterpriseOne user. For example, depending on your JD Edwards EnterpriseOne applications release, valid users might be:

- jdeb9
- e810
- e811
- e812
- e900

A.3 Multiple Agents on a Single Machine

You can install multiple agents on a single machine provided you adhere to the caveats explained in these preceding sections:

- One Agent Per Application Server Installation
- Management Agents on OAS
- Management Agents on JD Edwards EnterpriseOne Enterprise Servers

A.4 Multiple WebSphere Application Servers

It is recommended that you only install only one version of WebSphere Application Server (WAS) per machine. This is because running multiple versions of WAS on the same machine can lead to conflicts in the assignment of port numbers, node names, and cell names. This can cause unexpected results when trying to manage applications running in these application servers using both the native WAS management tools and through Server Manager.

A.5 Separate WAS Profiles

It is recommended that you create separate WAS profiles when managing:

- Multiple environments (such as production, test, and development)
- Multiple instances of a web-based server (such as HTML Web Server, Transaction Server, PIM Sync Server, and Business Services Server) in a Network Deployment (ND) WAS installation. Also in a ND WAS installation all the different WAS profiles can share one web server definition.
- Multiple foundations of JD Edwards EnterpriseOne (such as Tools Release 8.97, 8.97 Update 1, 8.98 etc.)
- Transaction Server

Note: During profile creation, it is recommended that you specify your starting port number to a value that will give you a sufficient amount of port numbers (for example, 1000) between the last profile you created so as to not conflict with other currently assigned ports and ports that will be assigned in the future.

Note: If you configure the WebSphere Application Server SOAP_CONNECTOR_ADDRESS port number outside of Server Manager (for example, from the WebSphere Administrative Console), you must restart the Management Agent that is managing that WebSphere Application Server instance. This is required because Server Manager uses that port to communicate with the WebSphere Application Server and only acquires the port value on start up of the Management Agent.

Note: *WAS Base/Standalone*. The general recommendation is to use a single WAS profile to deploy and manage multiple instances of EnterpriseOne web-based servers (such as HTML Web Server, PIM Sync Server, and Business Services Server). This is because of the limitation of WAS Base/Standalone functionality and how the web server plug-ins are used and modified across profiles. The exception to the general recommendation is the Transaction Server. The recommendation is to deploy and manage the Transaction Server in a separate WAS profile. This is because of conflicts between HTML Server and Transaction Server within the same profile. In WAS standalone, when creating separate profiles you must create a separate web server definition and have a separate HTTP Server. See IBM WebSphere Administration documentation for more details on this requirement.

A.6 Verify HTTP Ports

When installing any JD Edwards EnterpriseOne web-based servers that requires you to specify a HTTP port, you must ensure that the port you specify is available and is not being used by any other application currently installed and running on your application server. This applies not only to the instances within Server Manager, but any software installed on that machine. The port number entered for this instance must not be in use. You must be sure to know the ports being used on all machines in the managed domain. The installer does not programmatically determine whether a port is used by another application, so if you specify a port that conflicts with another application unpredictable results will occur.

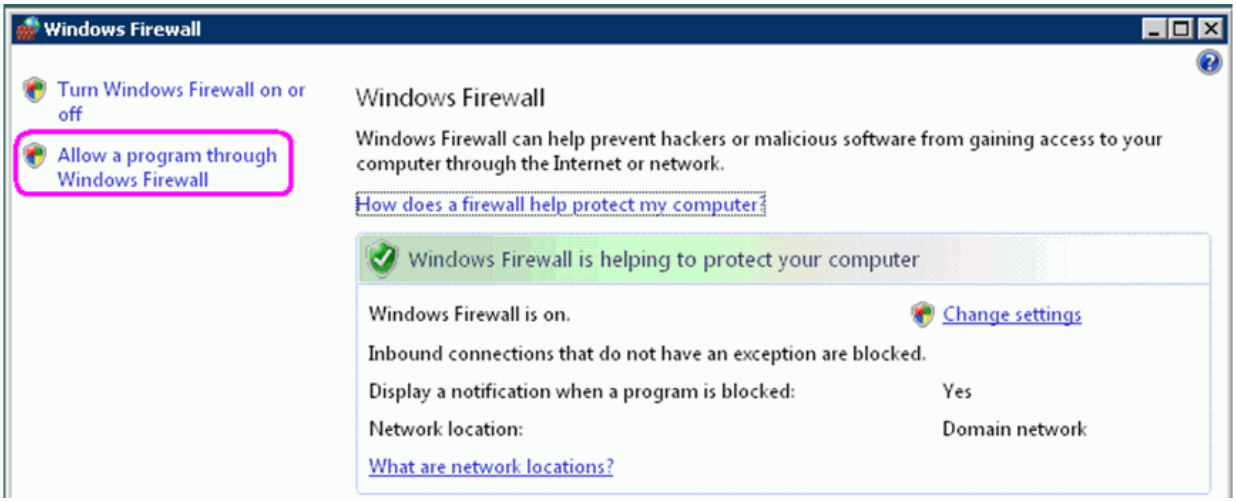
A.7 HTTP Ports on UNIX Operating Systems

When using HTTP ports to install a Web-Based Server, make sure not to select a port in the range restricted by the UNIX operating system for root access only. These are usually ports from 1 1024, but may include others in your particular environment. Using a port in a restricted range will cause undesirable results as the Management Agent will not have the rights to manage the products installed to these ports.

A.8 Setting Up Windows Firewall in Windows Server 2008

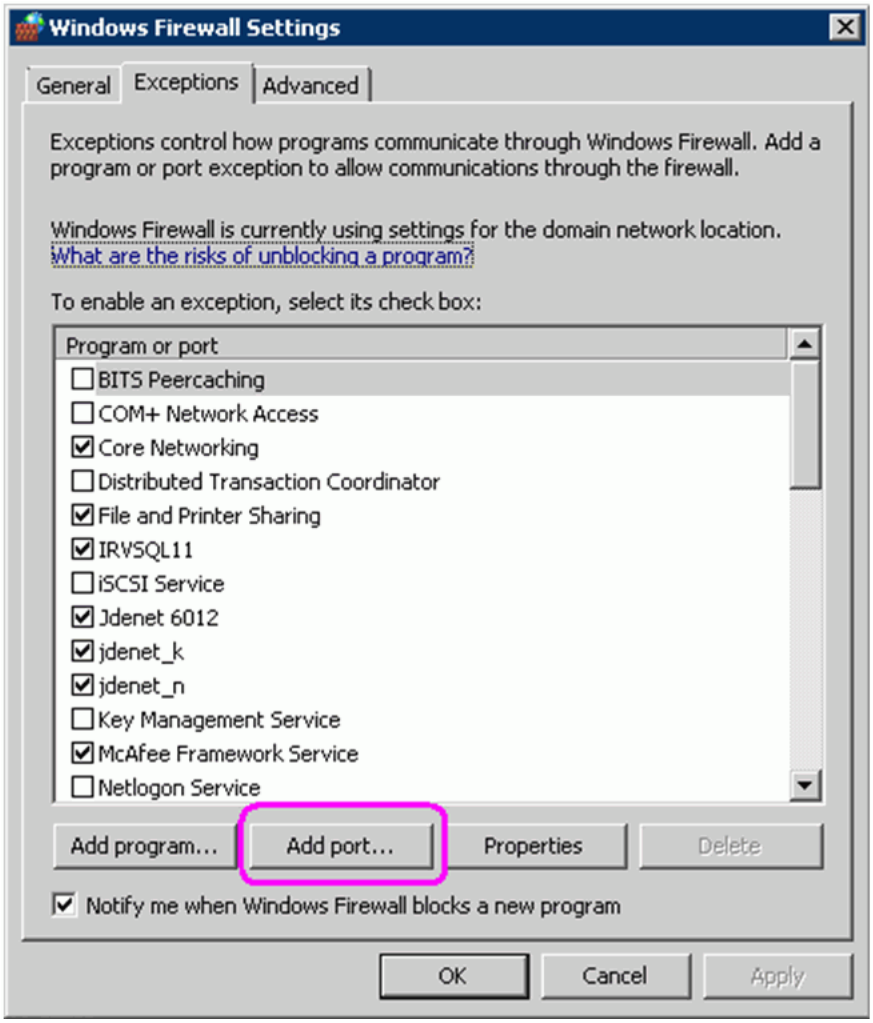
By default, Windows Server 2008 has the Windows Firewall turned on. This default firewall prohibits Server Manager from being fully functional. Additionally, the Server Manager Agent may not work correctly unless you follow these procedures.

1. In Windows Server 2008, open *Windows Firewall*.

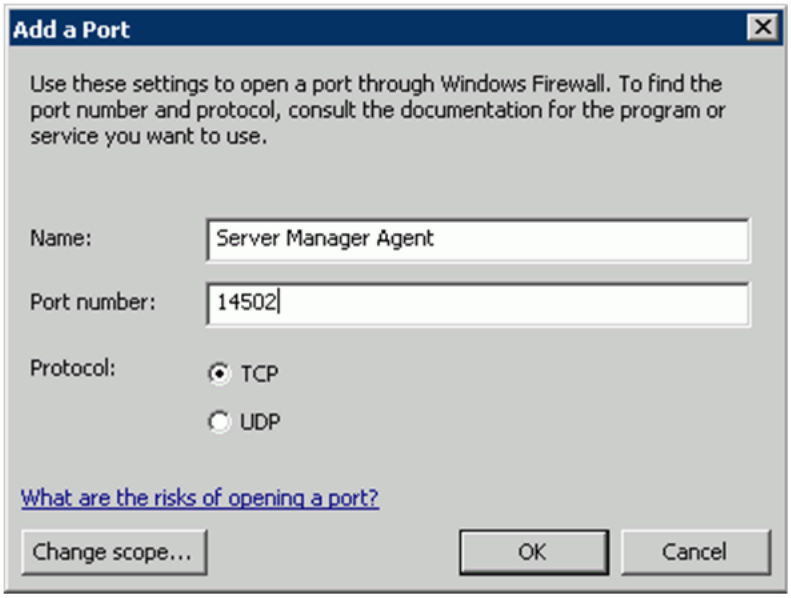


2. On *Windows Firewall*, in the left-hand pane, click this setting:

   Allow a program through Windows Firewall



3. On *Windows Firewall Settings*, on the *Exceptions* tab, click the *Add Port* button.



4. On *Add a Port*, complete these fields to add a port for the Server Manager Agent:

   - *Name*

     Enter this value:

     Server Manager Agent

   - *Port Number*

     Enter this value:

     14502

   - *Protocol*

     Choose the radio button for this value:

     TCP

5. Click the *OK* button.

6. Repeat Steps 3 and 4 to add another Server Manager port.

   On Add a Port, complete these fields to add a port for the Server Manager JMX connection:

   - *Name*

     Enter this value:

     Server Manager JMX Port

   - *Port Number*

     Enter this value:

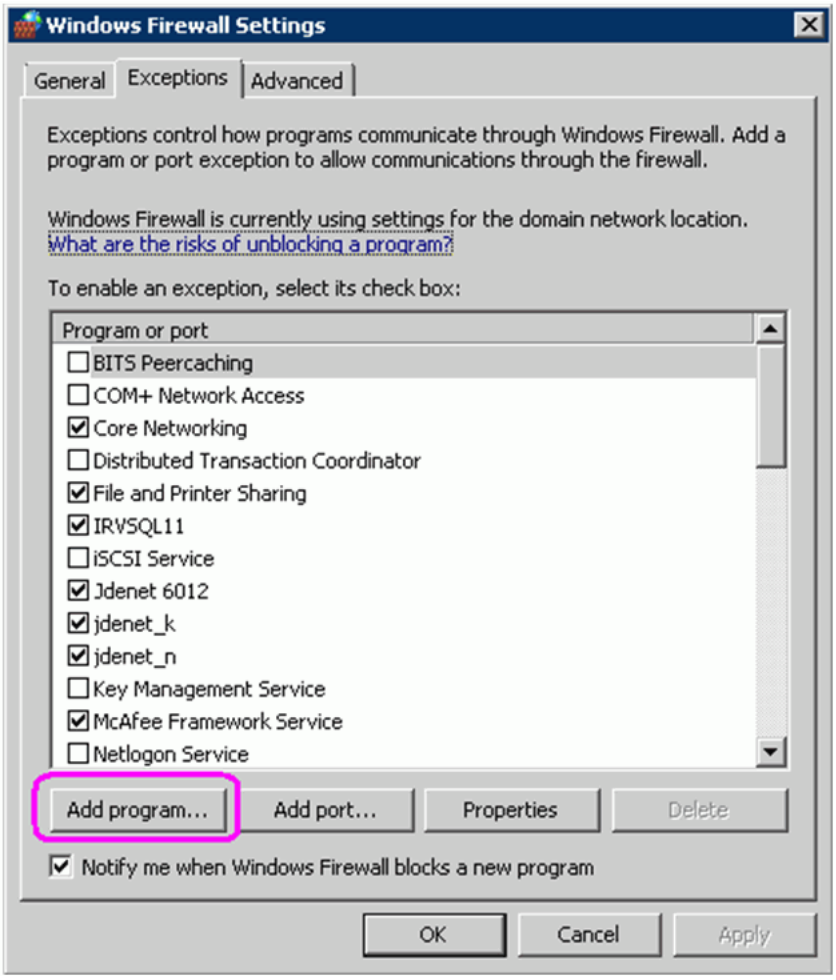
     14501

   - *Protocol*

     Choose the radio button for this value:

     TCP

7. At this point, if not already installed, you can install the Server Manager Agent for Microsoft Windows as described in the Server Manager Guide, in the section entitled: Install a Management Agent.



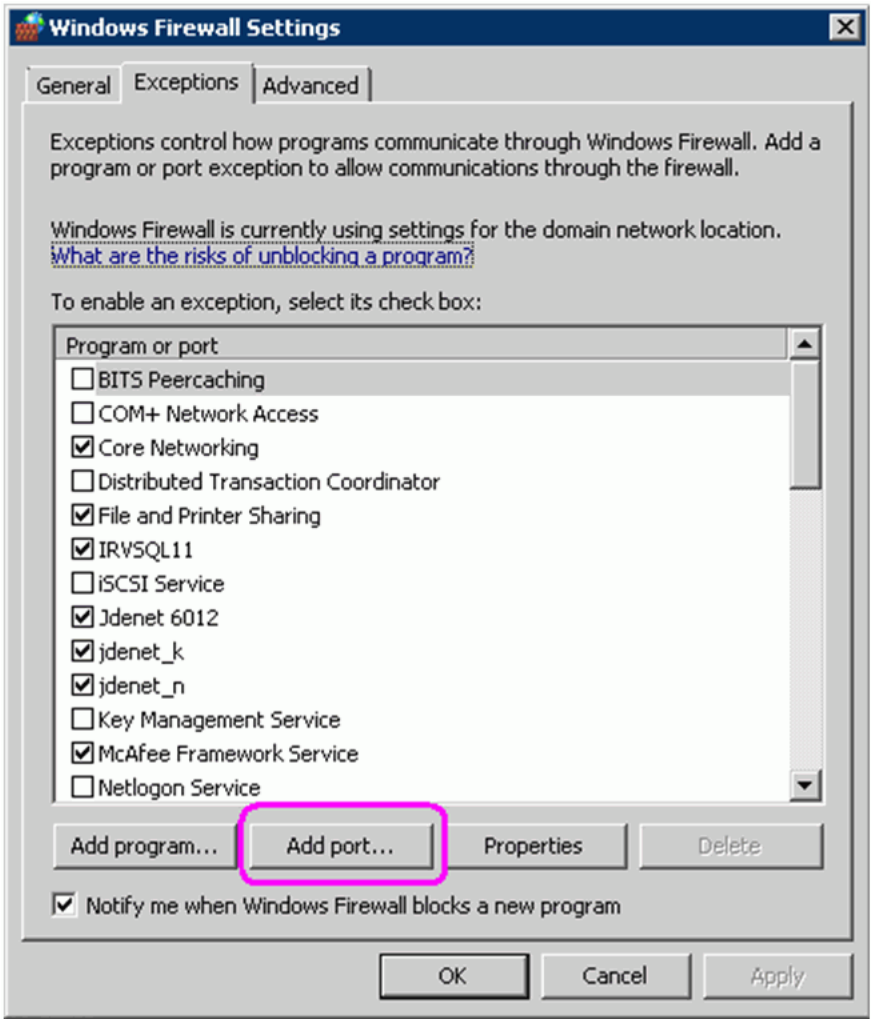
8. On *Windows Firewall Settings*, on the *Exceptions* tab, click the *Add Program* button.

9. On *Add a Program*, browse the list and locate this program:

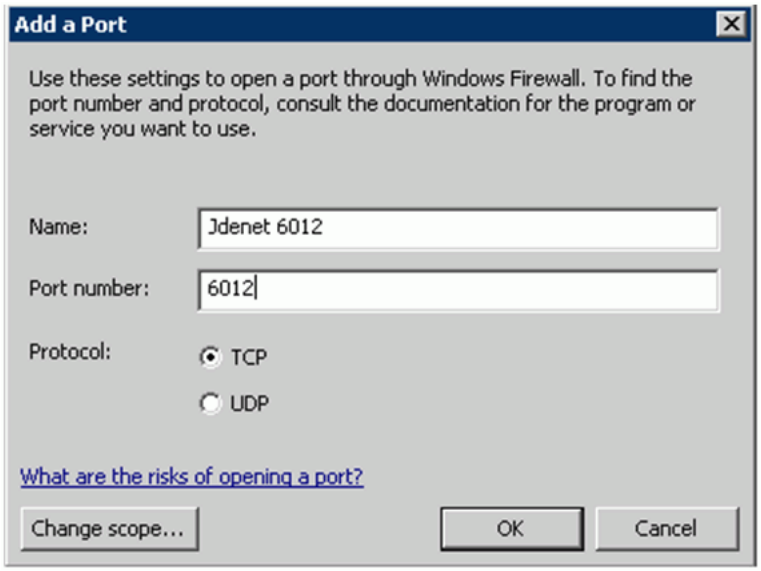
   scfagent

10. Click the *OK* button.

11. At this point, if not already installed, you can install a Managed Instance for the Enterprise Server as described in the Server Manager Guide, in the section entitled: Register or Create a JD Edwards Enterprise Server as a New Managed Instance.



12. On *Windows Firewall Settings*, on the *Exceptions* tab, click the *Add Port* button.



13. On *Add a Port*, complete these fields to add a port for the Server Manager Agent:

- *Name*

  Enter this value:

  JDENET <port>

  where <*port*> is a variable value for JDENET corresponding to the JD Edwards EnterpriseOne Applications Release. See description below for valid values.

- *Port Number*

  Enter this value:

  <port>

  where <*port*> is a variable value for JDENET corresponding to the JD Edwards EnterpriseOne Applications Release. For example, the default values per release are listed in this table:

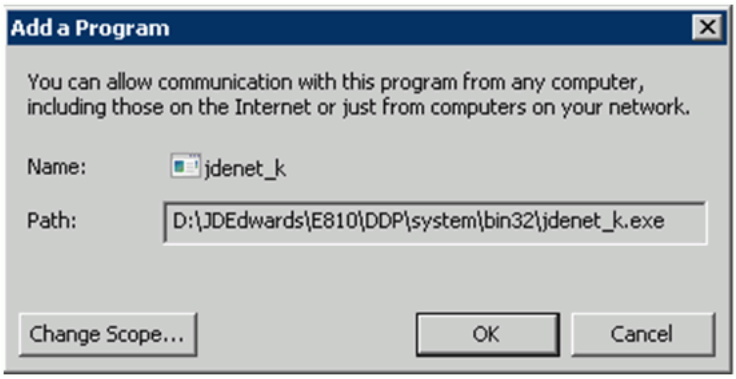
JD Edwards Application Release	Default JDENETPort Value
8.10	6012
8.11	6013
8.12	6014
9.0	6015

- *Protocol*

  Choose the radio button for this value:

  TCP

14. On *Windows Firewall Settings*, on the *Exceptions* tab, highlight the *jdenet_k* program and click the *Add Program* button.



15. On *Edit a Program*, verify the values in these fields are correct for *jdenet_k*:

- *Name*

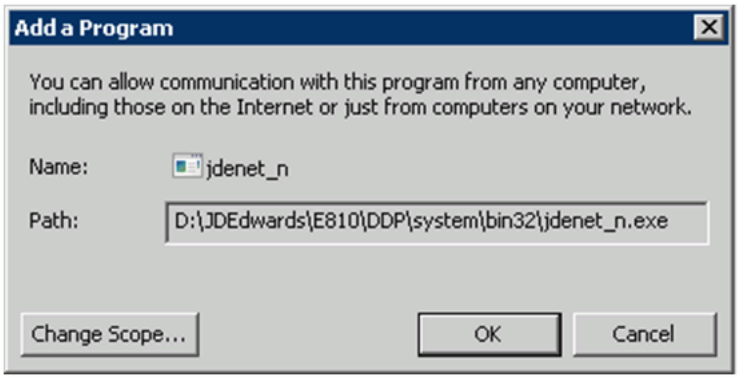
  jdenet_k

- *Path*

  Path to the jdenet_k.exe program. For example:

  `D:\JDEdwards\E810\DDP\system\bin32\jdenet_k.exe`

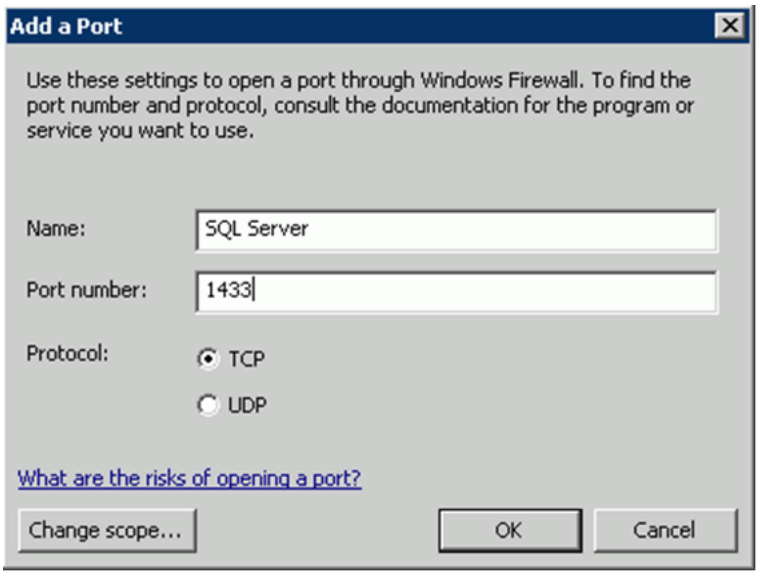
16. Click the *OK* button to accept the values.



17. Repeat Steps 14 through 16 above, substituting *jdenet_n.exe* for *jdenet_k.exe*.

18. Optionally, if the database for your JD Edwards EnterpriseOne applications reside on a different machine than the Enterprise Server, you must repeat the applicable steps above to add a port for that database. You may need to check with your DBA or database vendor documentation to determine the applicable port.

    The below example shows the typical database port for SQL Server 2008.



B

Using SSL with Standalone OC4J

Follow the steps below to use SSL with Standalone OC4J.

These steps have been taken from the ***Using SSL with Standalone OC4J*** section of http://docs.oracle.com/cd/E16439_01/doc.1013/e13977/configssl.htm.

B.1 Configuring HTTPS/SSL on the Server Manager Console on OC4J

Standalone OC4J supports SSL communication directly between a client and OC4J using HTTPS. This section describes how to accomplish this.

Use the following steps to use SSL with Standalone OC4J:

1. Create a Keystore.
2. Export a Certificate File.
3. Update the OC4J Configuration.
4. Import the New Certificate.

B.1.1 Create a Keystore

In the following example, we generate a keystore to reside in a file named mynewkeystore.jks, which has a password of changeit, using the RSA key pair generation algorithm:

```
C:\jde_home_console\SCFMC\jdk\bin\keytool -genkey -keyalg RSA -keystore
C:\jde_home_console\SCFMC\jdk\bin\mynewkeystore.jks -storepass changeit
```

In this tool:

- The keystore option sets the filename where the keys are stored.
- The storepass option sets the password for protecting the keystore. You can optionally omit this from the command line and be prompted for a password instead.

The keytool prompts you for additional information, as follows:

```
What is your first and last name?
  [Unknown]:  <Machine_Name_where_Server_Manager_Console_is_installed>
What is the name of your organizational unit?
  [Unknown]:  <UnitName>
What is the name of your organization?
  [Unknown]:  <OrgName>
What is the name of your City or Locality?
  [Unknown]:  <CityName>
What is the name of your State or Province?
  [Unknown]:  <StateName>
```

```
What is the two-letter country code for this unit?
  [Unknown]:  <CountryName>
Is <CN=<Machine_Name_where_Server_Manager_Console_is_installed>, OU=<UnitName>,
O=<OrgName>, L=<CityName>, ST=<StateName>, C=<CountryName>> correct?
```

Note: When the keytool prompts for **first and last name**, you must use the exact host name that the Server Manager Console uses for itself. This is the name that shows up for the console managed home location.

Enter key password for

```
(RETURN if same as keystore password):
```

Always press RETURN for the key password. In OC4J 10.1.3.x implementations, the keystore password must be the same as the key entry password.

The mynewkeystore.jks file is created in the C:\jde_home_console\SCFMC\jdk\bin directory.

Note: The keytool utility supports PKCS12 format wallets as well as JKS format keystores.

B.1.2 Export a Certificate File

To create/export/import/use a certificate:

1. Extract the custom certificate into a .cer file (Not required if customer already has the required certificate).
2. Run:

```
C:\jde_home_console\SCFMC\jdk\bin\keytool -export -storepass changeit -file
C:\jde_home_console\SCFMC\jdk\bin\mynewcertificate.cer -keystore
C:\jde_home_console\SCFMC\jdk\bin\mynewkeystore.jks
```

The certificate stored in file <C:\jde_home_console\SCFMC\jdk\bin\mycertificate.cer> message will be seen.

B.1.3 Update the OC4J Configuration

To update the OC4J configuration:

1. Create a copy of

```
C:\jde_home_console\SCFMC\targets\oc4j\j2ee\home\config\default-web-site.xml
```

   and name it as

```
C:\jde_home_console\SCFMC\targets\oc4j\j2ee\home\config\secure-web-site.xml
```

2. In the secure-web-site.xml look for the line:

```
<web-site xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://xmlns.oracle.com/oracleas/schema/web-site
-10_0.xsd"  port="8999" display-name="OC4J 10g (10.1.3) Default Web Site"
schema-major-version="10" schema-minor-version="0" >
```

3. Add the secure="true" attribute, so now the entry should look like below, this indicates to OC4J that this file contents are for HTTPS/SSL:

```
<web-site xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://xmlns.oracle.com/oracleas/schema/web-site
-10_0.xsd"  port="8999" secure="true" display-name="OC4J 10g (10.1.3) Default
Web Site" schema-major-version="10" schema-minor-version="0" >
```

4. You will also need an <ssl-config> element for your SSL configuration; that is discussed later in this procedure.

   ```
   <ssl-config factory="com.evermind.ssl.JSSESSLServerSocketFactory"
   keystore="C:\jde_home_console\SCFMC\jdk\bin\mykeystore.jks"
   keystore-password="changeit" truststore-password=""/>
   ```

5. Save the changes to secure-web-site.xml.

   Please note that if the same port is used in both the default-web-site.xml and secure-web-site.xml then HTTPS/SSL will work at this port and access over HTTP will be prevented. If you would like to use both HTTPS/SSL and HTTP access, then use different ports in both the files (in the above example port number 8999 is being used).

6. First backup the server.xml file.

7. Ensure that server.xml points to the secure-web-site.xml file in addition to default-web-site.xml.

   All three of the xml files from a working setup are attached for reference.

8. In the server.xml look for below line and delete it:

   ```
   <web-site default=″true″ path="./default-web-site.xml" />
   ```

9. Add the below two lines in its place:

   ```
   <web-site default="true" path="./secure-web-site.xml" />
   <web-site path="./default-web-site.xml" />
   ```

10. Save the changes to server.xml.

    It is necessary to first import the certificate created before into the cacerts file of the Server Manager Console JDK.

B.1.4 Import the New Certificate

These steps are for the Server Manager Console on Windows + OC4J combination.

1. Slight modifications are necessary to the command below for running it with:

   Server Manager Console on Windows + Weblogic, Windows + WebSphere

   Server Manager Console on Linux/Solaris + Weblogic

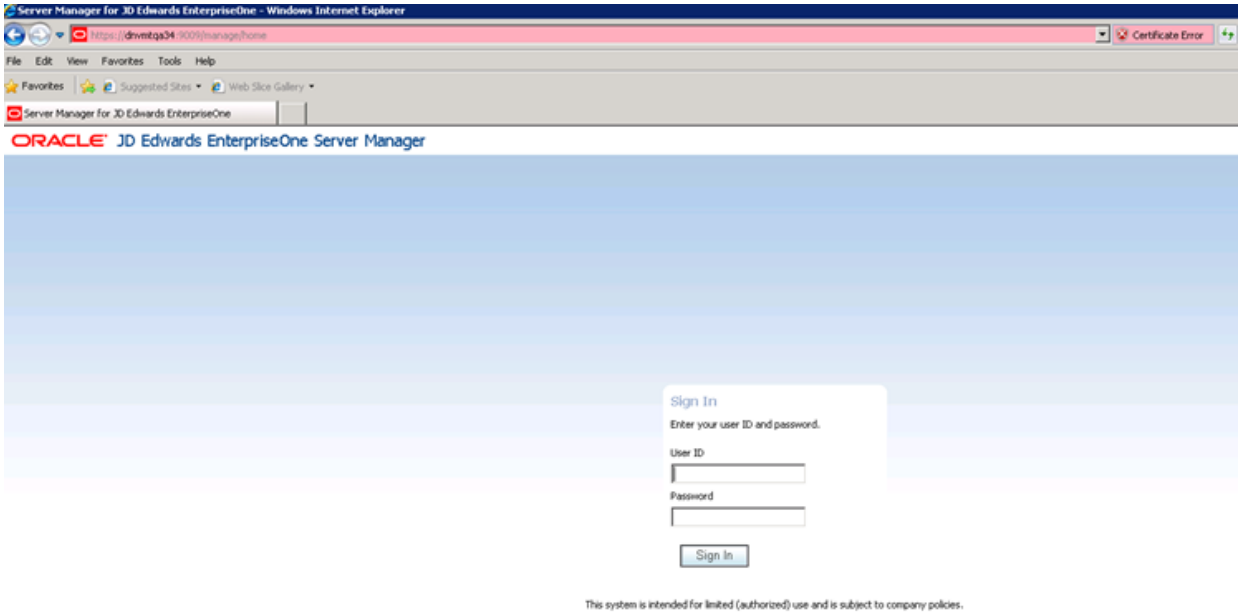
   ```
   C:\jde_home_console\SCFMC\jdk\jre\bin\keytool -import -trustcacerts -keystore
   C:\jde_home_console\SCFMC\jdk\jre\lib\security\cacerts -storepass changeit
   -noprompt -alias mynewcert -file C:\jde_home_console\SCFMC\jdk\
   bin\mynewcertificate.cer
   ```

2. Stop and start the Server Manager Console Windows Service to initialize the secure-web-site.xml file additions. Follow appropriate steps to restart the Server Manager Console on Weblogic and Websphere Application Servers.

3. Test the SSL port by accessing the site in a browser on the SSL port.

4. If successful, you will be asked to accept the certificate, because it is not signed by a certified authority. If a certificate issued by a trusted CA is used then no warning will be displayed. Refer to sample screenshot below:

Figure B–1 Login Screen



5. After implementing Server Manager over HTTPS/SSL and in case a self update is performed, once the self update completes, it is necessary to add this line

   ```
   <web-app application="ManagementConsole" name="ManagementConsole_WAR"
   load-on-startup="true" root="/manage" />
   ```

   into the default-web-site.xml and secure-web-site.xml, if this entry is removed during the update. Also check to make sure the entry below exists in the server.xml:

   ```
   <application name="ManagementConsole"
   path="../applications\ManagementConsole.ear" parent="default" start="true" />
   ```

6. Please restart the Server Manager Console after making this change and access the Server Manager Console URL over SSL and verify that it is working fine.

B.2 Configure Server Manager Agents to work successfully with HTTPS/SSL Server Manager Console

If HTTPS/SSL is enabled for Server Manager Console installed on Weblogic and Websphere the SM Console URL can be accessed in the browser and the certificate saved to a .cer file and then follow the steps below.

B.2.1 Importing the custom Certificate into the cacerts file of the SM Agent Machine(s) JRE

Copy the generated mynewcertificate.cer to the SM Agent machine from the SM Console machine (use Binary mode for FTP). The command below assumes the file is copied to C:\jde_home_agent\SCFHA\jdk\jre\bin\ location for Windows platform and /u01/jde_home_agent/SCFHA/jdk/jre/bin for UNIX Platforms.

B.2.1.1 For Windows Platform:

1. Create a backup of the Z:\jde_home_agent\SCFHA\jdk\jre\lib\security\cacerts file.

2. Run this command:

```
C:\jde_home_agent\SCFHA\jdk\jre\bin\keytool -import -trustcacerts -keystore
C:\jde_home_agent\SCFHA\jdk\jre\lib\security\cacerts -storepass changeit
-noprompt -alias mynewcert -file C:\jde_home_
agent\SCFHA\jdk\jre\bin\mynewcertificate.cer
```

   The certificate added to the keystore message will be seen.

B.2.1.2 For UNIX Platforms (including Linux):

1. Create a backup of /u01/jde_home_agent/SCFHA/jdk/jre/lib/security/cacerts file.
2. Run this command:

```
/u01/jde_home_agent/SCFHA/jdk/jre/bin/keytool -import -trustcacerts -keystore
/u01/jde_home_agent/SCFHA/jdk/jre/lib/security/cacerts -storepass changeit
-noprompt -alias mynewcert -file /u01/jde_home_
agent/SCFHA/jdk/jre/bin/mynewcertificate.cer
```

   The certificate added to the keystore message will be seen.

B.2.1.3 For AS/400 Platforms as QSECOFR (or equivalent user profile):

1. Create a backup of the ***/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit/jre/lib/security/cacerts*** file.
2. Run this command:

```
/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit/jre/bin/keytool -import
-trustcacerts -keystore
/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit/jre/lib/security/cacerts -storepass
changeit -noprompt -alias mynewcert -file /JDEdwards/JDE_
HOME/SCFHA/bin/mynewcertificate.cer
```

3. The certificate added to the keystore message will be seen.
4. It is necessary to restart the SM Agent after importing the certificate into the cacerts file.

B.2.2 Exceptions

Common possible exceptions in this setup:

1. This exception occurs if the certificate is not imported correctly in the SM Agent/Console logs.

Figure B–2 Imported Incorrectly

```
javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated
        at com.sun.net.ssl.internal.ssl.SSLSessionImpl.getPeerCertificates(SSLSessionImpl.java:352)
        at org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:126)
        at org.apache.http.conn.ssl.SSLSocketFactory.connectSocket(SSLSocketFactory.java:437)
        at
org.apache.http.impl.conn.DefaultClientConnectionOperator.openConnection(DefaultClientConnectionOperator.java:181)
        at org.apache.http.impl.conn.ManagedClientConnectionImpl.open(ManagedClientConnectionImpl.java:300)
        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.targets.log.ServerLogFile.send(ServerLogFile.java:195)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
        at java.lang.reflect.Method.invoke(Method.java:597)
        at org.apache.commons.modeler.BaseModelMBean.invoke(BaseModelMBean.java:458)
        at com.jdedwards.mgmt.JdeModelMBean.invoke(JdeModelMBean.java:400)
        at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.invoke(DefaultMBeanServerInterceptor.java:836)
        at com.sun.jmx.mbeanserver.JmxMBeanServer.invoke(JmxMBeanServer.java:761)
        at javax.management.remote.generic.ServerIntermediary.handleRequest(ServerIntermediary.java:280)
        at javax.management.remote.generic.ServerIntermediary$PrivilegedRequestJob.run(ServerIntermediary.java:951)
        at
javax.management.remote.generic.ServerIntermediary$RequestHandler.handleMBSReqMessage(ServerIntermediary.java:727)
        at javax.management.remote.generic.ServerIntermediary$RequestHandler.execute(ServerIntermediary.java:629)
        at
com.sun.jmx.remote.generic.ServerSynchroMessageConnectionImpl$RemoteJob.run(ServerSynchroMessageConnectionImpl.java:
266)
        at com.sun.jmx.remote.opt.util.ThreadService$ThreadServiceJob.run(ThreadService.java:208)
        at com.sun.jmx.remote.opt.util.JobExecutor.run(JobExecutor.java:59)
```

2. This exception is seen when the CN of the certificate is not the same as the SM Console hostname.

Figure B–3 CN and SM do not match

```
javax.net.ssl.SSLException: hostname in certificate didn't match: <DENPBDS11.oradev.oraclecorp.com> != <test user>
        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.targets.log.ServerLogFile.send(Unknown Source)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:88)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:55)
        at java.lang.reflect.Method.invoke(Method.java:613)
        at org.apache.commons.modeler.BaseModelMBean.invoke(Unknown Source)
        at com.jdedwards.mgmt.JdeModelMBean.invoke(Unknown Source)
        at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.invoke(DefaultMBeanServerInterceptor.java:831)
        at com.sun.jmx.mbeanserver.JmxMBeanServer.invoke(JmxMBeanServer.java:803)
        at javax.management.remote.generic.ServerIntermediary.handleRequest(ServerIntermediary.java:280)
        at javax.management.remote.generic.ServerIntermediary$PrivilegedRequestJob.run(ServerIntermediary.java:951)
        at java.security.AccessController.doPrivileged(AccessController.java:314)
        at
javax.management.remote.generic.ServerIntermediary$RequestHandler.handleMBSReqMessage(ServerIntermediary.java:727)
        at javax.management.remote.generic.ServerIntermediary$RequestHandler.execute(ServerIntermediary.java:629)
        at
com.sun.jmx.remote.generic.ServerSynchroMessageConnectionImpl$RemoteJob.run(ServerSynchroMessageConnectionImpl.java:
266)
        at com.sun.jmx.remote.opt.util.ThreadService$ThreadServiceJob.run(ThreadService.java:208)
        at com.sun.jmx.remote.opt.util.JobExecutor.run(JobExecutor.java:59)
```