Installing Candle Products
on Windows

Version CT350

GC32-9218-00

October 2004

Candle Corporation
100 North Sepulveda Blvd.
El Segundo, California 90245
Contents

Preface ................................................................................................................. 11
  About This Book ......................................................................................... 12
  Adobe Portable Document Format ................................................................. 14
  Documentation Conventions ....................................................................... 16
  Candle Customer Service and Satisfaction ......................................................... 18

What’s New in This Release ............................................................................. 19

Chapter 1. Preparing for Installation ................................................................. 25
  What Are OMEGAMON XE and OMEGAMON DE? ........................................ 26
  CandleNet Portal Components in This Package .............................................. 32
  Installation Planning ...................................................................................... 33
  Configuring Your System for CandleNet Portal .............................................. 36
  Configuring OMEGAMON XE Across a Firewall ............................................ 37
  Prerequisites ................................................................................................. 40
  To Do Before Beginning ............................................................................... 56

Chapter 2. Preparing for Upgrading and Migrating from a Previous Installation ................................................................................................. 65
  Upgrade and Migration Planning ..................................................................... 66
  To Do Before Beginning ............................................................................... 68

Chapter 3. Installation Steps ............................................................................ 73
  Starting setup.exe ......................................................................................... 75
  Selecting Components and Starting to Copy Files .......................................... 76
  Initial Configuration Steps ........................................................................... 78
  Creating the CandleNet Portal Server Database ........................................... 79
  Configuring the CandleNet Portal Server ...................................................... 81
  Configuring the CMS .................................................................................... 94
  Configuring Agent-to-CMS Communication ................................................ 103
  Completing Installation .............................................................................. 107
  Configuring the Agents .............................................................................. 108
Contents

Universal Agent .................................................. 185
Warehouse Proxy .................................................. 190
WebSphere Application Server ................................. 197
WebSphere InterChange Server ................................. 199
Windows Management Web Service ......................... 204

Glossary .......................................................... 207

Index .............................................................. 221
Table 1. Symbols in Command Syntax ........................................... 17
Table 2. Products and Versions for Current Release ......................... 19
Table 3. CMS Hardware Requirements ......................................... 40
Table 4. CMS Software Requirements (minimum) ........................... 41
Table 5. CMW Hardware Requirements ........................................ 42
Table 6. CMW Software Requirements ......................................... 42
Table 7. CandleNet Portal Server and Desktop Client Hardware Requirements 45
Table 8. Individual Agent Requirements ...................................... 48
Table 9. Second CNP Server Configuration Dialog ............................ 83
Table 10. Communication Settings for this CMS ............................... 95
Table 11. Communication Settings for Remote CMS ......................... 99
Table 12. Second Configuration Defaults for Connecting to a CMS Dialog ... 105
Table 13. Add SNA Fields .......................................................... 113
Table 14. TCP/IP Fields in Hub Specification Dialog ....................... 127
Table 15. SNA Fields in Hub Specification Dialog .......................... 128
Table 16. Parameters for Oracle Monitoring Agent Access to Views .......... 156
Table 17. Parameters for KSAR3PWD.EXE .................................... 170
Table 18. Tuxedo Monitoring Agent Configuration Values .................. 182
Table 19. Tuxedo Monitoring Agent Queue Information ..................... 183
Table 20. Tuxedo Monitoring Agent Advanced Configuration Settings ........ 184
Table 21. Universal Agent Startup Arguments ................................ 187
Table 22. API Client Package ..................................................... 188
Table 23. Agent ID Field Description .......................................... 197
Figures

Figure 1. OMEGAMON XE Platform Components .................. 27
Figure 2. Configuration Including a Remote CMS ................ 31
Figure 3. Intranet with Integral Web Server .................... 87
Figure 4. Intranet with External Web Server .................... 88
Figure 5. Intranet with Integral Web Server; Internet with External Web Server 89
Figure 6. Intranet and Internet with Integral and External Web Servers .. 91
Figure 7. Two Host Addresses, Intranet and Internet, and with Integral and External Web Servers .......................... 92
Introduction

This installation guide contains instructions for installing and configuring OMEGAMON® XE (formerly named CandleNet Command Center® (CCC™)) on the following platforms:

- Windows XP Professional Edition
- Windows 2000
- Windows 2003 Server

Preface contents

- About This Book .................................................. 12
- Adobe Portable Document Format ............................. 14
- Documentation Conventions .................................. 16
- Candle Customer Service and Satisfaction .................. 18
About This Book

Who should read this book

This guide was written for individuals who install and configure Candle® products on Windows. Installers should have a working knowledge of the Windows operating system and a basic knowledge of networking.

Users of this guide must know the planned configuration for their OMEGAMON XE environment. They should consult with their Candle system administrator to ensure that they know where the Candle Management Server® (CMS™), CandleNet Portal® Servers, Candle Management Workstation® (CMW™), CandleNet Portal, and the agents are to be installed.

Scope of this guide

Notice many of the applications require prior purchase and installation of third-party software. It is beyond the scope of this guide to instruct you in how to install or configure non-Candle software.

Documentation set information

This guide covers the Windows operating system platforms; however, most Candle installations comprise several platforms. Refer to the following guides:

On the mainframe (CICAT™ (version 300) users):
- Installation and Configuration of Candle Products on OS/390 and z/OS

On the mainframe (versions of CICAT prior to version 300):
- Installing Candle Products on MVS
- Installing Candle Products and Candle Management Server on MVS

On distributed platforms:
- Installing Candle Products on UNIX
- Installing Candle Products on OS/400
- Installing Candle Products on HP NonStop Kernel

Note: The operating system formerly known as Tandem NonStop Kernel has been renamed to HP NonStop Kernel.
About This Book

As in previous releases, product-specific Configuration and Customization Guides may also be provided.

Where to look for more information
For more information related to this product and other related products, please see the

- Technical documentation CD-ROM that came with your product.
- Online Help provided with this and the other related products.

Ordering additional documentation
To order additional product manuals, contact your Candle Support Services representative.
Candle supplies documentation in the Adobe Portable Document Format (PDF). The Adobe Acrobat Reader will print PDF documents with the fonts, formatting, and graphics in the original document. To print a Candle document, do the following:

1. Specify the print options for your system. From the Acrobat Reader Menu bar, select File > Page Setup… and make your selections. A setting of 300 dpi is highly recommended as is duplex printing if your printer supports this option.

2. To start printing, select File > Print... on the Acrobat Reader Menu bar.

3. On the Print pop-up, select one of the Print Range options for
   - All
   - Current page
   - Pages from: [ ] to: [ ]

4. (Optional). Select the Shrink to Fit option if you need to fit oversize pages to the paper size currently loaded on your printer.

Printing problems?
The print quality of your output is ultimately determined by your printer. Sometimes printing problems can occur. If you experience printing problems, potential areas to check are:

- settings for your printer and printer driver. (The dpi settings for both your driver and printer should be the same. A setting of 300 dpi is recommended.)
- the printer driver you are using. (You may need a different printer driver or the Universal Printer driver from Adobe. This free printer driver is available at www.adobe.com.)
- the halftone/graphics color adjustment for printing color on black and white printers (check the printer properties under Start > Settings > Printer). For more information, see the online help for the Acrobat Reader.
- the amount of available memory in your printer. (Insufficient memory can cause a document or graphics to fail to print.)

For additional information on printing problems, refer to the documentation for your printer or contact your printer manufacturer.
Contacting Adobe

If additional information is needed about Adobe Acrobat Reader or printing problems, see the Readme.pdf file that ships with Adobe Acrobat Reader or contact Adobe at www.adobe.com.

Adding annotations to PDF files

If you have purchased the Adobe Acrobat application, you can add annotations to Candle documentation in .PDF format. See the Adobe product for instructions on using the Acrobat annotations tool and its features.
Documentation Conventions

Introduction
Candle documentation adheres to accepted typographical conventions for command syntax. Conventions specific to Candle documentation are discussed in the following sections.

Panels and figures
The panels and figures in this document are representations. Actual product panels may differ.

Required blanks
The slashed-b (ı) character in examples represents a required blank. The following example illustrates the location of two required blanks.

beBA*ServiceMonitorı0990221161551000

Revision bars
Revision bars (|) may appear in the left margin to identify new or updated material.

Variables and literals in command syntax examples
In examples of command syntax for the OS/390, VM, OS/400, and NonStop Kernel platforms, uppercase letters indicate actual values (literals) that the user should type; lowercase letters indicate variables that represent data supplied by the user:

LOGON APPLID (cccccccc)

However, for the Windows and UNIX platforms, variables are shown in italics:

-candle.kzy.instrument.control.file=instrumentation_control_file_name
-candle.kzy.agent.parms=agent_control_file_name

Note: In ordinary text, variable names appear in italics, regardless of platform.
Symbols

The following symbols may appear in command syntax:

Table 1. Symbols in Command Syntax

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Usage</th>
</tr>
</thead>
</table>
| | The “or” symbol is used to denote a choice. Either the argument on the left or the argument on the right may be used. Example:  
  **YES | NO**  
  In this example, YES or NO may be specified. |
| [ ] Denotes optional arguments. Those arguments not enclosed in square brackets are required. Example:  
  **APPLDEST DEST [ALTDEST]**  
  In this example, DEST is a required argument and ALTDEST is optional. |
| { } Some documents use braces to denote required arguments, or to group arguments for clarity. Example:  
  **COMPARE (workload) -**  
  **REPORT={SUMMARY | HISTOGRAM}**  
  The workload variable is required. The REPORT keyword must be specified with a value of SUMMARY or HISTOGRAM. |
| _ Default values are underscored. Example:  
  **COPY infile outfile - [COMPRESS={YES | NO}]**  
  In this example, the COMPRESS keyword is optional. If specified, the only valid values are YES or NO. If omitted, the default is YES. |
Candle Customer Service and Satisfaction

Background
To assist you in making effective use of our products, Candle offers a variety of easy-to-use online support resources. The Candle Web site provides direct links to a variety of support tools that include these services:

**eSupport** allows you to create and update service requests opened with Customer Service and Satisfaction (CSS).

**eDelivery** allows you to download products, documentation, and maintenance 24 hours a day, 7 days a week.

**eNotification** notifies you of product updates and new releases.

In addition, you can find information about training, maintenance plans, consulting and services, and other useful support resources. Refer to the Candle Web site at [www.candle.com](http://www.candle.com) for detailed customer service information.

Candle Customer Service and Satisfaction contacts
You will find the most current information about how to contact Candle CSS by telephone or email on the Candle Web site. Go to the [www.candle.com](http://www.candle.com) support section, and choose the link to Support Contacts to locate your regional support center.
What’s New in This Release

Major enhancements and changes affecting installation of the OMEGAMON XE product family are summarized below.

Product versions

The information in this installation guide applies to the products and versions shown below, some of which involve enhancements from the previous release.

Table 2. Products and Versions for Current Release

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Adapter™ for OMEGACENTER Gateway™ for MVS</td>
<td>150</td>
</tr>
<tr>
<td>Alert Adapter for Peregrine ServiceCenter</td>
<td>202</td>
</tr>
<tr>
<td>Alert Adapter for Remedy ARS</td>
<td>202</td>
</tr>
<tr>
<td>Alert Adapter for TME 10 NetView for AIX</td>
<td>200</td>
</tr>
<tr>
<td>Alert Adapter for AF/Remote®</td>
<td>121</td>
</tr>
<tr>
<td>CandleNet Portal</td>
<td>195</td>
</tr>
<tr>
<td>CMS</td>
<td>350</td>
</tr>
<tr>
<td>CMW</td>
<td>350</td>
</tr>
<tr>
<td>Command &amp; Control™</td>
<td>110</td>
</tr>
<tr>
<td>Log Alert Agent</td>
<td>200</td>
</tr>
<tr>
<td>OMEGAMON Alert Manager for HP OpenView IT/Operations</td>
<td>201</td>
</tr>
<tr>
<td>OMEGAMON Alert Manager for HP OpenView NNM</td>
<td>201</td>
</tr>
<tr>
<td>OMEGAMON Alert Manager for Tivoli/Enterprise Console</td>
<td>250</td>
</tr>
<tr>
<td>Product</td>
<td>Version</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>OMEGAMON DE</td>
<td>195</td>
</tr>
<tr>
<td>OMEGAMON Monitoring Agent® for eBA Solutions</td>
<td>251</td>
</tr>
<tr>
<td>OMEGAMON XE for BEA WebLogic Server</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for CASP</td>
<td>320</td>
</tr>
<tr>
<td>OMEGAMON XE for CICS</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for CICSplex</td>
<td>220</td>
</tr>
<tr>
<td>OMEGAMON XE for DB2 on zOS</td>
<td>300</td>
</tr>
<tr>
<td>OMEGAMON XE for DB2 Universal Database (DB2 UDB)</td>
<td>102</td>
</tr>
<tr>
<td>OMEGAMON XE for DB2 Universal Database (DB2 UDB)</td>
<td>400</td>
</tr>
<tr>
<td>OMEGAMON XE for DB2plex</td>
<td>220</td>
</tr>
<tr>
<td>OMEGAMON XE for IBM Cryptographic Coprocessors</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for IMS</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for IMSplex</td>
<td>220</td>
</tr>
<tr>
<td>OMEGAMON XE for Linux</td>
<td>120</td>
</tr>
<tr>
<td>OMEGAMON XE for Microsoft SQL Server</td>
<td>301</td>
</tr>
<tr>
<td>OMEGAMON XE for Mainframe Networks</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for NetWare</td>
<td>301</td>
</tr>
<tr>
<td>OMEGAMON XE for Oracle</td>
<td>301</td>
</tr>
<tr>
<td>OMEGAMON XE for OS/390</td>
<td>140</td>
</tr>
<tr>
<td>OMEGAMON XE for OS/390 UNIX System Services</td>
<td>220</td>
</tr>
<tr>
<td>OMEGAMON XE for OS/400</td>
<td>300</td>
</tr>
<tr>
<td>OMEGAMON XE for R/3™ a</td>
<td>301</td>
</tr>
<tr>
<td>OMEGAMON XE for Storage</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for Sybase</td>
<td>301</td>
</tr>
<tr>
<td>OMEGAMON XE for Sysplex</td>
<td>220</td>
</tr>
<tr>
<td>OMEGAMON XE for Tuxedo</td>
<td>301</td>
</tr>
<tr>
<td>OMEGAMON XE for UNIX</td>
<td>201</td>
</tr>
</tbody>
</table>
What’s New in This Release

Renamed products or platforms

- The product formerly known as Candle Command Center® for MQSeries has been renamed to OMEGAMON XE for WebSphere MQ Monitoring.
- The product formerly known as Candle Command Center for MQSeries Configuration has been renamed to OMEGAMON XE for WebSphere MQ Configuration.

Table 2. Products and Versions for Current Release (continued)

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMEGAMON XE for WebSphere Application Server</td>
<td>130</td>
</tr>
<tr>
<td>OMEGAMON XE for WebSphere Integration Brokers</td>
<td>120</td>
</tr>
<tr>
<td>OMEGAMON XE for WebSphere InterChange Server</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE for WebSphere MQ Configuration</td>
<td>360</td>
</tr>
<tr>
<td>OMEGAMON XE for WebSphere MQ Monitoring</td>
<td>360</td>
</tr>
<tr>
<td>OMEGAMON XE for Windows Active Directory Servers</td>
<td>400</td>
</tr>
<tr>
<td>OMEGAMON XE for Windows Servers</td>
<td>400</td>
</tr>
<tr>
<td>OMEGAMON XE for Windows Management Web Service</td>
<td>100</td>
</tr>
<tr>
<td>OMEGAMON XE Web Services</td>
<td>350</td>
</tr>
<tr>
<td>OMEGAVIEW II® for the Enterprise</td>
<td>300</td>
</tr>
<tr>
<td>Universal Agent</td>
<td>410</td>
</tr>
<tr>
<td>Warehouse Proxy</td>
<td>350</td>
</tr>
</tbody>
</table>

CandleNet Portal (version 195)
CandleNet Portal supersedes the CMW as the primary interface into your OMEGAMON XE products. CandleNet Portal (version 195) is included in the current release. For information on installing CandleNet Portal, refer to Installing Candle Products on Windows.

CMS (version 350)
Version 350 of the CMS is included in the current release.

a. R/3 is a trademark of SAP AG.
The product formerly known as OMEGAMON XE for WebSphere MQ Integrator has been renamed to OMEGAMON XE for WebSphere Integration Brokers.

The product formerly known as OMEGAMON XE for Windows has been renamed to OMEGAMON XE for Windows Servers.

Windows support
- Candle products are no longer supported on Windows 98 and Windows NT.
- Windows 2000 needs Service Pack 3 or higher.

Windows 2003 Server support
These products support Windows 2003 Server:
- CandleNet Portal
- CMS
- OMEGAMON XE for WebSphere MQ Configuration (version 360 and above)
- OMEGAMON XE for WebSphere MQ Monitoring (version 360 and above)
- OMEGAMON XE for WebSphere Application Server (version 130 and above)
- OMEGAMON XE for WebSphere Integration Brokers (version 120 and above)
- Universal Agent (version 410 and above)
- OMEGAMON XE for Windows Servers (version 400 and above)
- OMEGAMON XE for Windows Active Directory Servers (version 400 and above)

Windows XP support for CMW
Support for multiple Java Runtime Environment (JRE) versions

Earlier versions of CandleNet Portal required a specific release of JRE. CandleNet Portal (version 180) and (version 190), for example, both require JRE (version 1.3.1_04). Now, in version 195, CandleNet Portal can support multiple JRE versions: 1.3.1_04 to 1.4.2.

If your machine does not have any of these versions installed, the Candle installer will prompt you to install one.

*Note:* Supported versions of JRE are updated frequently to include the latest versions available. Go to Sun's Java 2 Platform, Standard Edition (J2SE) web page for downloading the latest supported version. (http://java.sun.com/j2se/1.3/download.html).

CandleNet Portal Server Database Support

This release of CandleNet Portal Server adds support for the DB2 Universal Database (DB2 UDB (version 8.1)) database product for creation of the CandleNet Portal Server database. The OMEGAMON installation package includes DB2 UDB, which Candle encourages you to use as the CandleNet Portal Server database. See “Installing DB2 UDB” on page 56.

This release continues to support the Microsoft SQL Server database product (versions 7.0 and 2000).

The Microsoft Data Engine (MSDE) database is no longer supported for use with CandleNet Portal Server. You must use Microsoft SQL Server or DB2 UDB.

If you are upgrading from CandleNet Portal (version 190) and were using MSDE, you must perform Installing DB2 UDB before you begin the Candle installer. During the Candle upgrade installation, the CandleNet Portal Server database will transfer from MSDE to DB2 UDB.

If you already have a DB2 UDB (version 7 or 8) installation, you need not install the DB2 UDB (version 8.1) included in your Candle package unless you want to upgrade to version 8.1.
SAP® R/3 support

The R/3 monitoring agent supports higher versions of SAP R/3 (versions 3.1H through 4.7).

Oracle (version 10g) support

OMEGAMON XE for Oracle supports Oracle (version 10g).

WebSphere Application Server monitoring agent packaging

OMEGAMON XE for WebSphere Application Server (version 120 and above) is now included on the product installation CD instead of being supplied on a separate CD.

InstallShield Wizard

The InstallShield Wizard comes with a modified (and enhanced) process for performing the installation of Candle products on Windows, and it provides a new look to the installation screens. Additional changes include:

- The CandleLight product has been removed from the installer
- The CandleNet Portal Browser Client will be installed automatically with CandleNet Portal.
- OMEGAMON Web Services (SOAP server) will be installed automatically with the CMS.
- You will not be required to enter a license key during installation of OMEGAMON XE or OMEGAMON DE. If you have purchased OMEGAMON DE, you will need to install the separate CD that is provided.

1. SAP is a registered trademark of SAP AG.
Preparing for Installation

Chapter contents

What Are OMEGAMON XE and OMEGAMON DE? .................................................. 26
CandleNet Portal Components in This Package ..................................................... 32
Installation Planning .............................................................................................. 33
Configuring Your System for CandleNet Portal ....................................................... 36
Configuring OMEGAMON XE Across a Firewall ..................................................... 37
Prerequisites .......................................................................................................... 40
To Do Before Beginning .......................................................................................... 56
What Are OMEGAMON XE and OMEGAMON DE?

What OMEGAMON XE does

OMEGAMON XE is a suite of Candle products that monitor and manage system and network applications on a variety of platforms. These products keep track of the availability and performance of all parts of your enterprise from one or more designated workstations, and provide reports you can use to track trends and troubleshoot problems.

How you can use OMEGAMON XE

You can use OMEGAMON XE to:

- Create situations (conditions to test when monitoring).
- Establish performance thresholds, and raise alerts when thresholds are exceeded or values are matched.
- Trace the causes leading up to an alert.
- Create and send commands to systems in your managed enterprise by means of the Take Action feature.
- Create comprehensive reports about system conditions.
- Define your own queries, using the attributes from an installed agent or from an ODBC-compliant data source, to monitor conditions of particular interest.

Components of the OMEGAMON XE platform

The client, server, and agent implementation includes

- A client, CandleNet Portal, with a Java-based user interface for viewing and monitoring your enterprise. CandleNet Portal offers two modes of operation: desktop and browser.
- A CandleNet Portal Server, placed between the client and the CMS, that enables retrieval, manipulation, and analysis of data from the agents. The CandleNet Portal Server is the central repository for all user data.
What Are OMEGAMON XE and OMEGAMON DE?

- A CMS, which acts as a collection and control point for alerts received from the agents, and collects their performance and availability data. It also serves as a repository for historical data. The CMS runs on OS/390, z/OS, UNIX, Windows XP Professional Edition, Windows 2000, or Windows 2003 Server.

- Agents installed on the systems or subsystems you want to monitor. These agents collect and distribute data to a CMS.

- (if necessary) A CMW, required primarily for the maintenance task of removing obsolete managed systems from the user interface. Although the CandleNet Portal client replaces the CMW as the user interface for your Candle monitored environment, the CMW still offers some features not otherwise available, such as the Universal Message Console and the Policy Microscope.

Figure 1. OMEGAMON XE Platform Components
What Are OMEGAMON XE and OMEGAMON DE?

What OMEGAMON DE does

OMEGAMON DE offers a dashboard view of your enterprise. It gives you a single point of control for managing the resources your business-critical applications rely on, including a range of operating systems, servers, databases, mainframes, and Web components. For example, a typical IT network might have a Web server running on Windows, an application server running on UNIX, a database on OS/390, and a transaction processor on CICS on the mainframe. OMEGAMON DE brings all these views together in a single window, so you can see when any component is not working as expected.

What CandleNet Portal does

Running on Windows XP Professional Edition, Windows 2000, or Windows 2003 Server, CandleNet Portal is the interface into your OMEGAMON XE products. In the same way you use your browser home page as a starting point for navigating the Internet, you use CandleNet Portal to get a high-level overview of your network environment. One section of the window displays the Navigator, a tree-like view of your monitored network, with alert icons that appear when problems arise. The rest of the window is filled with views pertinent to the chosen item in the Navigator tree. From the top level or from your home workspace, you can navigate to specific locations to check activity and investigate problems.

Also see “CandleNet Portal Components in This Package” on page 32.

Two modes of operation

- Desktop mode, whereby the CandleNet Portal client is installed on your workstation and runs as a desktop application.
- Browser mode, whereby you can start CandleNet Portal from your browser, at which time the thin client software is downloaded to your system and thereafter only for software updates.

When using CandleNet Portal in browser mode, you can start it from any workstation by entering the web server URL.

What the agents do

The agents are the data collectors. The agents monitor systems, subsystems, or applications, collect data, and pass the data to CandleNet Portal or the
CMW through the CMS. The agents pass commands from the user to the
system, subsystem, or application. An agent interacts with a single system or
application and, in most cases, resides on the same machine where the system
or application is running.

Types of agents include:

- Monitoring agents
  These agents collect performance and analysis data for many systems
  (such as UNIX), subsystems (such as WebSphere MQ), and applications
  (such as R/3).

- Alert Managers
  These agents monitor non-Candle monitoring products for a remote
  system, subsystem, or application, and relay alert information to the CMS.
  Sources of alerts include console and message logs, network-management
  products, and system-management products. An Alert Adapter also may
  have an Alert Emitter™ feature that can export Candle alerts to a
  non-Candle monitoring product.

- Alert Emitters
  These agents monitor events (that is, exceptions) from any product
  running under control of the CMS and, if applicable, relay them to the
  monitored system, subsystem, or application for corrective action.

- Gateways
  These agents communicate events to a management application running
  on a supported platform using a network service. Examples include the
  SNMP Gateways, which communicate events to an SNMP management
  application running on AIX or Windows.

  Agents run on OS/390, z/OS, UNIX, Windows XP Professional Edition,
  Windows 2000, Windows 2003 Server, HP NonStop Kernel, and OS/400;
  however, not all agents are supported on all platforms.

**CMS**

The CMS can run as a stand-alone server, or as a remote server in a hierarchy
of servers that report to a master server called the hub CMS. A CMS can be
installed on UNIX, OS/390, z/OS, Windows XP Professional Edition, Windows
What Are OMEGAMON XE and OMEGAMON DE?

Hub CMS
The hub CMS serves as the focal point for managing your environment. The hub CMS may receive data from:

- Agents running on the same or remote systems.
- Other CMSs running as remote servers in a hierarchical configuration.

Depending on the complexity of your environment, the number of agents you install, and the amount of data you choose to collect, a single CMS may be all that you need. Or, you may want to configure a hierarchical set of CMSs where remote CMSs report to a hub CMS to distribute the activity.

Remote CMSs
If large amounts of network data are to be collected, excessive traffic can be minimized with the installation of remote CMSs which collect data from the agent and forward it to the hub CMS. Each remote CMS must reside on its own machine and have a unique CMS name (node), but the architectures of various remote CMSs may differ from each other as well as from the hub.

Naming your CMS
You must decide how the CMSs are to be named. In general, the names selected should be short, but meaningful within your environment. For the best performance, Candle recommends that you use the following guidelines:

- Each name must be unique. One name cannot match another CMS name for its entire length. (For example, “candle” and “candleremote” are unique and permitted; “server1” and “server1” are not unique and not permitted).
- Each name must begin with an alpha character. No blanks or special characters (“$#@”) can be used. An underline (“_”) is permitted and conforms to ISO 9660 standards.
- Each name must be between 2 and 32 characters in length.
- CMS naming is case-sensitive on all platforms.
Figure 2. Configuration Including a Remote CMS
CandleNet Portal Components in This Package

CandleNet Portal
CandleNet Portal includes its own server and two types of client interface components. Here is a brief description of the components you can install at your site.

CandleNet Portal Server
The CandleNet Portal Server communicates directly with your hub CMS. Install at least one CandleNet Portal Server in your network to deploy CandleNet Portal.

CandleNet Portal Browser Client interface (automatically installed with CandleNet Portal)
In your Internet browser, to start CandleNet Portal browser mode, you can enter the URL for a specific CandleNet Portal browser client installed on your Web server.

CandleNet Portal Desktop Client interface
The installation choice labeled “CandleNet Portal Client (Desktop Edition)” installs a Java-based graphical user interface on a Windows workstation. Once the Desktop Client is installed and configured, you can use it to start CandleNet Portal in desktop mode.

Candle products compatible with this release
For a list of the Candle products that are compatible with CandleNet Portal (version 195), see the What’s New in This Release chapter of this manual.
Installation Planning

Upgrading and migrating from a previous installation

See “Preparing for Upgrading and Migrating from a Previous Installation” on page 65. That chapter includes information you need to know and tasks you need to do to prepare for upgrading and migrating your previously installed OMEGAMON XE or CCC to the new OMEGAMON XE (version CT350).

What to install

This section contains guidelines for determining which OMEGAMON XE components your site should install.

Guidelines:

- What does your site need to monitor?
  Your site may need to monitor systems (such as the Windows operating system) or applications (such as WebSphere MQ or R/3).

- Where are the systems or applications running?
  Your site should install the appropriate agent on every machine where the system or application is running. There are some exceptions to this rule, such as OMEGAMON XE for Netware and OMEGAMON XE for R/3, whereby the agent can query a remote system.

- Where do you want to accumulate data generated by the agents? This is where you will install a CMS.

- How much data will you collect?
  Depending on the complexity of your environment, the number of agents you install and the amount of data you choose to collect, you may need multiple CMSs. Multiple CMSs can run in a hierarchy of servers where remote CMSs collect data from their agents and report the data to a hub CMS. Your site may also have multiple hierarchies of servers, each with its own hub.

  **Note:** Only a hub CMS can have a CMW or CandleNet Portal Server attached to it.
Installation Planning

- Where do you want to run the user interface to look at data and interact with the system? How many users need to use the interface? This is where you will install the CandleNet Portal or CMW user interface.

- What communications protocols are available? You may use TCP/IP or SNA for communication between OMEGAMON XE components.

- Does your site have a requirement for 24 x 7 operation? If so, you’ll need to consider the Hot Standby feature.

General order of installation or upgrade

New and existing customers should install or upgrade in the following order:

1. Hub CMS
2. Remote CMS
3. CandleNet Portal Server
4. CandleNet Portal Desktop Client and (if necessary) CMW
5. Agents

**Note:** Once the CMSs have been installed, the CMW and the agents can be installed in any order.

For new customers, this order provides maximum efficiency. For existing customers, this order prevents communication problems between components.

Platform support of various Candle products

The guidelines below gives an overview of which platforms support the various Candle products and components and where to look for installation and upgrade instructions. Unless otherwise specified, the instructions are the same whether you are installing or upgrading.

Also see “Prerequisites” on page 40 for the hardware and software requirements for the installation of various Candle products on Windows.


Your site may install a CMW on Windows XP Professional Edition or Windows 2000. Refer to this guide for instructions.


Finding out which fixpack is installed

You can get a report of the CMS or agent version in Manage Candle Services.

1. Select “Start>Programs>Candle OMEGAMON XE>Manage Candle Services”.

2. Right-click the CMS or agent row, then select “About Services” from the popup menu.

Hostname

TCP/IP network services such as NIS, DNS, and the /etc/hosts file should be configured to return the fully qualified hostname (for example: HostName.candle.com).
Configuring Your System for CandleNet Portal

Deploying CandleNet Portal

As with other client and server applications, components of CandleNet Portal can be installed on the same machine; however, it is more likely that you will install each component on a separate machine in your network.

To deploy CandleNet Portal at your site:

- Install at least one CandleNet Portal Server per hub CMS.
  
  You can have more than one CandleNet Portal Server connected to the same hub CMS, such as to provide a test environment and a production environment.

  Historical Configuration Note: If your Candle product uses the Candle Warehouse Proxy for warehousing historical data, install the CandleNet Portal Server on the same machine as the Warehouse Proxy, if possible, for ease of administration. The CandleNet Portal Server requires its own “Candle Data Warehouse data” source if it is not installed on the same machine as the Warehouse Proxy.

Order of installation

For CandleNet Portal, Candle recommends that you begin by installing and configuring the CandleNet Portal Server and one Desktop Client application. Always install the CandleNet Portal Server first. (Before installing the CandleNet Portal Server, make sure a hub CMS has been installed.)

After you verify that you can communicate properly with your supported Candle products, install additional clients on as many machines as you would like.
Configuring OMEGAMON XE Across a Firewall

Overview

This section provides an overview of Candle’s implementation of firewall support. It explains basic concepts and gives sample scenarios of various configurations. This section does not include specific steps for configuring OMEGAMON XE across a firewall; those steps can be found either in the installation chapters of this guide or in the other platform-specific installation guides, depending upon which operating systems you are configuring on.

Basic implementation

At this release, OMEGAMON XE supports most common firewall configurations, including those that use address translation (application proxy firewall is a notable exception). To enable this support, Candle uses the IPPPIPE socket address family, a TCP-based protocol that opens a single port on the firewall for communication by OMEGAMON XE components. If your target OMEGAMON XE environment includes a firewall between any CandleNet Command Center® (CCC™) components, you must specify IPPPIPE as your communication protocol during configuration. No other special configuration is needed unless your firewall also uses address translation.

Implementation with address translation

Address translation is an enhanced security feature of some firewall configurations. With this feature, components that must be reached across the firewall have two unique, but corresponding addresses: the external address (valid for components outside the firewall) and the internal address (valid for components inside the firewall).

With regard to OMEGAMON XE, the component that typically must be reached for connection is the CMS; however, the Warehouse Proxy, which runs on Windows as a server-type application, must also be accessible to clients and would also require an external and internal address. A component on either side of the firewall only knows about the address that is valid for its side (its “partition”).

To accommodate sites with address translation, Candle uses a partition-naming strategy. This strategy requires two steps:
The creation of a text file called a partition file as part of the configuration of a hub or remote CMS (or Warehouse Proxy). The partition file contains an entry that defines that component’s address in the other partition.

The specification of a partition name (any alphanumeric string up to 32 characters), as part of the configuration of any agent, a hub or remote CMS, a CMW, or Warehouse Proxy. A partition name must be specified for each component regardless of which side of the firewall it resides in.

Sample scenarios

Assuming that your site has one firewall, there would be two partitions: one outside the firewall, one inside the firewall. In the sample scenarios that follow we will specify the names OUTSIDE and INSIDE, respectively, for these partitions. (If your site’s configuration includes more than one firewall, Candle recommends that you contact Candle customer service for assistance in configuring OMEGAMON XE.)

Note: Whatever the platform, the command-line examples in the following scenarios adhere to the UNIX and Windows text formatting conventions for literals and variables.

Scenario 1: hub CMS INSIDE, agents and CMW OUTSIDE

As part of the configuration of the hub CMS, we specify the name of the partition that it resides in INSIDE. We also create a partition file parthub.txt, containing the following entry:

    OUTSIDE ip.pipe:hub’s_external_address

OUTSIDE is the partition name outside the firewall and hub’s_external_address is the address of the hub CMS that is valid for the agents and the CMW.

As part of the configuration of each agent and the CMW, we specify the name of the partition that each resides in OUTSIDE.

When an agent or the CMW starts, parthub.txt is searched for an entry that matches the partition name OUTSIDE and sees the CMS address that is valid for the agents and the CMW (the external address).

Scenario 2: hub and remote CMSs INSIDE, agents OUTSIDE

Note: In Scenarios 2 and 3 we will assume that all agents report to the remote CMS.
As part of the configuration of the hub CMS, we specify the name of the partition that it resides in INSIDE. No partition file is needed because the only component that reports to it (the remote CMS) is also inside the firewall.

As part of the configuration of the remote CMS, we specify the name of the partition that it resides in INSIDE. A partition file partremote.txt must also be created at the remote CMS. It contains the following entries:

\[ \text{OUTSIDE ip.pipe:remote's\_external\_address} \]

When configuring the agents (all of which are outside the firewall, reporting to the remote CMS), we specify the name of the partition that they reside in OUTSIDE. When the agents start, partremote.txt is searched for an entry that matches the partition name OUTSIDE and sees the remote CMS address that is valid for them (the external address).

**Scenario 3: hub CMS INSIDE, remote CMS and agents OUTSIDE**

As part of the configuration of the hub CMS, we specify the name of the partition that it resides in INSIDE. We also create a partition file parthub.txt, containing the following entry:

\[ \text{OUTSIDE ip.pipe:hub's\_external\_address} \]

OUTSIDE is the partition name outside the firewall and hub’s_external_address is the address of the hub CMS that is valid for the remote CMS.

As part of the configuration of both the agents and the remote CMS, we specify the name of the partition they reside in OUTSIDE.

A partition file partremote.txt also must be created at the remote CMS. It contains the following entry:

\[ \text{INSIDE ip.pipe:remote's\_internal\_address} \]

If the hub CMS needs to communicate with the remote CMS (for example, to issue a report request from an agent that is connected to the remote CMS), partremote.txt is searched for an entry that matches the partition name INSIDE and sees the remote CMS address that is valid for it (the internal address).
Prerequisites

Introduction

This chapter lists hardware and software prerequisites for the OMEGAMON XE components (CMS, CMW, CandleNet Portal, and agents) running on Windows.

CMS

This section lists hardware and software requirements for the CMS.

Hardware

This section lists two sets of hardware requirements:

- **Minimum**
  The minimum hardware levels are required for the CMS to operate.

- **Recommended**
  The hardware levels recommended for adequate CMS performance in an average monitoring environment.

Hardware: Evaluating CMS Performance

Your site should use the recommended hardware levels as starting points to evaluate the CMS performance in your particular environment. Many factors affect the performance of Candle components, including the following:

- Are the CMS and other components residing on the same machine?
- How many products are installed?
- What is the expected monitoring load? A large number of situation events flowing through the CMS may require additional resources for adequate performance.

The following table lists the minimum and recommended requirements:

<table>
<thead>
<tr>
<th></th>
<th>Minimum Requirements</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GHz CPU</td>
<td>1 GHz CPU</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisites

Operating system

The CMS is not supported on DEC Alpha machines.

Table 4. CMS Software Requirements (minimum)

<table>
<thead>
<tr>
<th>For TCP/IP Communications:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Windows 2000 Professional or Server with W2K Service Pac 3 or above. The Primary DNS suffix of this computer requires a specified domain name; for example, candle.com. The option “Change primary DNS suffix when domain membership changes should be checked. This setting is performed under the System Prop./Network ID settings.</td>
</tr>
<tr>
<td>- Microsoft Winsock v1.1 or higher</td>
</tr>
<tr>
<td>- Microsoft TCP/IP protocol stack</td>
</tr>
<tr>
<td>For SNA communications:</td>
</tr>
<tr>
<td>- Windows 2000 Professional or Server with W2K Service Pac 3 or above</td>
</tr>
<tr>
<td>- Microsoft SNA Server v3.0 or higher</td>
</tr>
<tr>
<td>- Service Pac 1 is required for SNA Server v4.0.</td>
</tr>
<tr>
<td>- IBM Communications Server v5.0 or 5.2 (fixes JR10466 and JR10368 are required for SNA Server v5.0.)</td>
</tr>
</tbody>
</table>

Additional Prerequisites for OMEGAMON XE Web Services (SOAP Server)
Candle recommends Internet Explorer (version 6.0x) for sites intending to use a SOAP Server. If you are running Internet Explorer (version 5.0x), you must install Service Pack MSXML (version 3.0) before executing SOAP requests.

CMW
You may install a CMW only on Intel-based (x86) CPUs and compatible CPUs that run Windows XP Professional Edition or Windows 2000. (The CMW is not supported on DEC Alpha machines). The following tables list the minimum and recommended hardware and software requirements.
Prerequisites

The CMW may include installation of the CandleLight® Workstation.

Table 5. CMW Hardware Requirements

<table>
<thead>
<tr>
<th>Minimum Requirements</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 MHz Pentium II (for configurations that produce up to 1000 rows per report)</td>
<td>400 MHz Pentium II or higher (for configurations that produce over 1000 rows per report)</td>
</tr>
<tr>
<td>96 Mb RAM</td>
<td>128 Mb RAM or more</td>
</tr>
<tr>
<td>Video support for 800 x 600 resolution</td>
<td>Video support for 1024 x 768 (to view maximum amount of monitoring data)</td>
</tr>
</tbody>
</table>

Table 6. CMW Software Requirements

For TCP/IP communications:
- Windows 2000 Professional, Server or Workstation with Service Pac 3 or above
- Microsoft Winsock v1.1 or higher
- Microsoft TCP/IP protocol stack

For SNA communications:
- Windows 2000 Professional, Server or Workstation with Service Pac 3 or above
- A 32-bit version of one of the following SNA Server or Client products:
  - IBM PCOMM v4.11 or higher (fix IC19970 on Windows 2000 Server or Workstation)
  - IBM Communications Server v5.0 or 5.2 (fixes JR10466 and JR10368 are required for SNA Server v5.0)
  - Microsoft SNA Server v3 or higher (Service Pac 1 is required for SNA Server v4.0)
  - Attachmate EXTRA! v6.2, 6.3, or 6.4 (fix for case number 1221139 is required for v6.2 and 6.3; fix for case number 1274151 is required for v6.4)
  - Walldata RUMBA v5.1 or higher (Walldata PTF OPK52002 is required for RUMBA versions less than v5.2A.)
Prerequisites

Table 6. CMW Software Requirements (continued)

<table>
<thead>
<tr>
<th>Note:</th>
<th>The OMEGAVIEW® Zoom feature is currently supported with the following products.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For TCP/IP communications:</td>
</tr>
<tr>
<td></td>
<td>– Attachmate EXTRA! v6.2, 6.3, or 6.4 (fix for case number 1221139 is required for v6.2 and 6.3; fix for case number 1274151 is required for v6.4.)</td>
</tr>
<tr>
<td></td>
<td>For SNA communications:</td>
</tr>
<tr>
<td></td>
<td>– Attachmate EXTRA! v6.2, 6.3, or 6.4 (EXTRA! 6.3 Service Pac is required for v6.3.)</td>
</tr>
</tbody>
</table>

The product must be installed with HLLAPI support (a quick way to check is to search the Program Files directory for the Attachmate EHLAPI32.DLL file). The emulation session that will be used for Zooming must be assigned a short name, for example, “A”. The emulation session must be open and ready before Zooming can occur.

To set up OMEGAVIEW Zoom from the CMW, see the CMW Online Help, or for a description of it, see the “Functional Comparison” section of the “CNP and the CMW” chapter of Administering Candle Products: CandleNet Portal.

For more information about OMEGAVIEW Zoom, see the OMEGAVIEW user documentation.

CandleNet Portal

Operating systems

All CandleNet Portal components are supported on the following Windows operating systems.

- Windows XP Professional Edition with Service Pac 1 or higher
- Windows 2000 with Service Pac 3 or higher
- Windows 2003 Server

Note: Windows operating systems listed are for Intel-based (x86) CPUs and compatible CPUs only.
Prerequisites

Candle component levels
CandleNet Portal requires the following Candle component levels:

- CMS (version CT350 or higher)
- CMW (version CT350 or higher)

Note: OMEGAMON XE for WebSphere Integration Brokers does not require a CMW for use with CandleNet Portal.

Communications
CandleNet Portal requires TCP/IP.

Candle products do not require a Domain Name Server (DNS). If your Windows systems are running without DNS, make sure the `/etc/hosts` file of the local machine is up to date.

TCP/IP network services such as NIS, DNS, and the `/etc/hosts` file should be configured to return the fully qualified hostname (for example: hostname.candle.com).

Additional communications software requirements are listed by component in the sections that follow.
Prerequisites

CandleNet Portal Server and Desktop Client

Hardware

Table 7. CandleNet Portal Server and Desktop Client Hardware Requirements

<table>
<thead>
<tr>
<th>Minimum Requirements</th>
<th>Recommended Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GHz or higher processor</td>
<td>1 GHz or higher processor</td>
</tr>
<tr>
<td>512 Mb RAM</td>
<td>1 GB RAM</td>
</tr>
<tr>
<td>300 Mb or more of available hard drive space</td>
<td></td>
</tr>
<tr>
<td>150 Mb or more of virtual memory in addition to operating system or other application requirements</td>
<td></td>
</tr>
<tr>
<td>Video card supporting 64K color and 1024 by 768 resolution (Super VGA)</td>
<td>Video card supporting 65,000 colors and 1,024 by 768 resolution or higher</td>
</tr>
</tbody>
</table>

SUN Microsystems JRE

CandleNet Portal Server requires one of these versions of the JRE: 1.3.1_04 to 1.4.2.

**Note:** Supported versions of JRE are updated frequently to include the latest versions available. Go to Sun’s Java 2 Platform, Standard Edition (J2SE) web page for downloading the latest supported version. (http://java.sun.com/j2se/1.3/download.html).

Communications

For TCP/IP communications (required regardless of communication method used between the CandleNet Portal Server and the CMS):

- Microsoft Winsock (version 1.1 or higher)
- Microsoft TCP/IP protocol stack

For SNA communications ((optional) If used, can only be used for communication between the CandleNet Portal Server and the CMS:

- Microsoft SNA Server (version 3.0 or higher), Service Pac 1 is required for SNA Server (version 4.0).
- IBM Communications Server (versions 5.0 or 5.2), fixes JR10466 and JR10368 are required for SNA Server (version 5.0).
Prerequisites

CandleNet Portal Server database
The CandleNet Portal Server requires prior installation of one of the following database products locally:

- DB2 UDB (version 8.1)

**Note:** The OMEGAMON installation package includes DB2 UDB, which Candle encourages the customer to use as the CandleNet Portal Server database. See “Installing DB2 UDB” on page 56.

- Microsoft SQL Server (version 7.0 or 2000)

CandleNet Portal Browser Client requirements
The CandleNet Portal Browser Client is automatically installed with CandleNet Portal on the same system as your CandleNet Portal Server. The Browser Client software is downloaded from here the first time a user enters the URL to start CandleNet Portal browser mode.

SUN Microsystems JRE
The CandleNet Portal Browser Client requires one of the versions of JRE that are listed as a requirement for the CandleNet Portal Server: 1.3.1_04 to 1.4.2.

**Note:** Supported versions of JRE are updated frequently to include the latest versions available. Go to Sun's Java 2 Platform, Standard Edition (J2SE) web page for downloading the latest supported version. ([http://java.sun.com/j2se/1.3/download.html](http://java.sun.com/j2se/1.3/download.html)).

Supported Web Browser
CandleNet Portal browser mode requires Microsoft Internet Explorer 5.5 running on one of the operating systems listed in “Operating systems” on page 43.

Default web browser settings are assumed.

Agents

Overview
You may install agents on Intel-based (x86) CPUs and compatible CPUs running Windows XP Professional Edition, Windows 2000, or Windows 2003 Server; however, not all agents run on all these platforms.
This section lists the system software, disk space, and anything else that may be required by the various agents. Notice that many of the applications require prior purchase and installation of third-party software. As mentioned earlier, it is beyond the scope of this guide to instruct you in how to install or configure non-Candle software.

**Operating systems**
- Windows 2000 Professional server or workstation, with Service Pac 3 or above
- Windows XP Professional Edition, with Service Pac 1 or above
- Windows 2003 Server

**TCP/IP communications:**
- Microsoft Winsock (version 1.1 or higher)
- Microsoft TCP/IP protocol stack

**SNA communications:**
- A 32-bit version of one of the following SNA Server or Client products:
  - IBM PCOMM (version 4.11 or higher)
    Fix IC19970 is required on Windows 2000 Server or Workstation.
  - IBM Communications Server (version 5.0 or higher)
    Fixes JR10466 and JR10368 are required for SNA Server (version 5.0).
  - Microsoft SNA Server (version 3 or higher)
    Service Pac 1 is required for SNA Server (version 4.0).
  - Attachmate EXTRA! (version 6.2, 6.3, or 6.4)
    Fix for case number 1221139 is required for versions 6.2 and 6.3.
    Fix for case number 1274151 is required for version 6.4.
  - Walldata RUMBA (version 5.1 or higher)
    Walldata PTF OPK52002 is required for RUMBA versions less than 5.2A.
Prerequisites

Hardware and other requirements

In addition to the minimum software requirements for agents listed in the previous section, and the individual agent requirements listed in the following table, agent installation requires a minimum of:

- 32 Mb RAM.
- 150 Mb virtual memory, plus 5 Mb for each agent installed.

Table 8. Individual Agent Requirements

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Framework (required for all agents)</td>
<td>Windows XP Professional Edition or Windows 2000</td>
<td>11 Mb disk space</td>
<td>At least 6 Mb disk space in the location referenced by your TEMP system variable.</td>
</tr>
<tr>
<td>BEA WebLogic Server</td>
<td>Windows XP Professional Edition with SP1 Windows 2000</td>
<td>12 Mb disk space</td>
<td>WebLogic Server v7 or v8</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional Edition or Windows 2000</td>
<td></td>
<td>JRE 1.3.1 (for WebLogic v7) or JRE 1.4 (for WebLogic v8)</td>
</tr>
<tr>
<td>DB2 UDB monitoring agent (version 102)</td>
<td>Windows XP Professional Edition or Windows 2000</td>
<td></td>
<td>DB2 UDB v6, 7 or 8</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional Edition or Windows 2000</td>
<td></td>
<td><strong>Note: If the DB2 UDB monitoring agent is being installed on the same machine as a CandleNet Portal Server, you must have DB2 UDB v7 or 8 installed. V6 will not be supported.</strong></td>
</tr>
<tr>
<td>DB2 UDB monitoring agent (version 400)</td>
<td>Windows 2000 (32-bit only) or Windows 2003 Server (32-bit only)</td>
<td></td>
<td>DB2 UDB v8.1</td>
</tr>
</tbody>
</table>
### Prerequisites

Table 8. Individual Agent Requirements (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
</table>
| eBA® Solutions monitoring agent | Windows XP Professional Edition or Windows 2000       | 200K disk space | - Install on the ETEWatch® Manager Server machine. (See “Installing ETEWatch, if necessary” on page 62.)  
- JRE v1.1.6 (the version packaged with ETEWatch)  
- JDBC or ODBC connectivity to the ETEWatch database |
| Microsoft SQL Server monitoring agent | Windows XP Professional Edition or Windows 2000       | 2Mb disk space | - Microsoft SQL Server v7.0 or 2000  
- Grant select permissions for Microsoft SQL Server  
- Microsoft SQL Server must be configured to run under either the Windows integrated or the mixed security mode |
| Novell NetWare monitoring agent | Windows XP Professional Edition or Windows 2000       | 4Mb disk space | - Novell NetWare v4.11 or 4.2 (with support pack 7a recommended) or v5.0  
- NetWare monitoring agents v2.6  
Important: NetWare v5.0 requires the latest maintenance from Novell to be applied before starting the monitoring agent for Novell NetWare. |
### Prerequisites

**OMEGAMON XE for WebSphere Integration Brokers**

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
</table>
Additional disk space for historical recording depending on the historical configuration | IBM’s broker product, which includes any of the following:  
- WebSphere MQ Integrator v2.1  
- WebSphere MQ Integrator Broker v2.1  
- WebSphere MQ Event Broker v2.1  
- IBM WebSphere Business Integration Event Broker v5  
- IBM WebSphere Business Integration Message Broker v5  
- IBM WebSphere Business Integration Message Broker with Rules and Formatter Extension v5  
| The monitoring agent must be installed on the same machine on which the WebSphere message broker is installed. |
Table 8. Individual Agent Requirements (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
</table>
| OMEGAMON XE for WebSphere MQ  | Windows XP Professional Edition | 1Mb disk space | - IBM WebSphere MQ v5.2, 5.2.1, or 5.3  
- Install on the machine where you will run the application.  
- WebSphere MQ Default Objects must exist before starting the agent.  
- Set user ID authorization required for running OMEGAMON XE for WebSphere MQ Configuration. (See “Authorizing users for OMEGAMON XE for WebSphere MQ” on page 63.) |
- Install on the machine where you will run the application.  
- WebSphere MQ Default Objects must exist before starting the agent.  
- Set user ID authorization required for running OMEGAMON XE for WebSphere MQ Monitoring. (See “Authorizing users for OMEGAMON XE for WebSphere MQ” on page 63.) |
Prerequisites

Table 8. Individual Agent Requirements (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
</table>
| Oracle monitoring      | Windows XP Professional Edition or Windows 2000        | 4Mb disk space    | ▪ Oracle 8.1.7, 9.2 or 10g  
▪ For agent on Oracle v10g:  
  ▪ CPU speed: 933MHz  
  ▪ RAM: 2GB  
▪ Install Oracle V$Dynamic performance tables  
▪ Grant select permissions for Oracle |
| agent                  |                                                        |                   |                                                                                     |
| Peregrine ServiceCenter| Windows XP Professional Edition or Windows 2000        | 300K disk space   | ▪ Peregrine ServiceCenter v2.0  
▪ This product requires the licensing of ServiceCenter SCAuto® SDK for the appropriate operating system. |
| Alert Adapter          |                                                        |                   |                                                                                     |
| R/3 monitoring agent   | Windows XP Professional Edition or Windows 2000        | 3Mb disk space    | ▪ Install on the target R/3 Server or on a remote Windows host with TCP/IP access to the target R/3 Server  
▪ SAP® R/3 v3.1H through 4.7 |
| Remedy ARS alert       | Windows XP Professional Edition or Windows 2000        | 2 Mb disk space   | Remedy ARS v3  
▪ Sybase v10 or 11  
▪ Grant select permissions for Sybase |
| manager                |                                                        |                   |                                                                                     |
| Sybase monitoring      | Windows XP Professional Edition or Windows 2000        | 2Mb disk space    |                                                                                     |
| agent                  |                                                        |                   |                                                                                     |
| Tuxedo monitoring      | Windows XP Professional Edition or Windows 2000        | 300K              | Install locally on the Tuxedo Application Server machine or remotely on the Tuxedo Client Workstation machine.  
▪ BEA Tuxedo v6.3, 6.4, or 6.5 |
| agent                  |                                                        |                   |                                                                                     |
Table 8. Individual Agent Requirements (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warehouse Proxy</td>
<td>Windows XP Professional Edition or Windows 2000</td>
<td>300K disk space</td>
<td>Important: Also ensure that there is sufficient room for the System Log.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Databases software</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Microsoft SQL Server v7.0 or 2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ODBC connectivity to the database.</td>
</tr>
<tr>
<td>Web Pulse monitoring agent</td>
<td>Windows XP Professional Edition or Windows 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebSphere Application Server monitoring agent</td>
<td>Windows 2003 Server or Windows 2000</td>
<td></td>
<td>One of these versions of IBM WebSphere Application Server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- v5.0.x or v5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Advanced Edition v4.0.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise Edition v4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Network Deployment v5.0.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Refer to IBM’s “WebSphere Application Server - System Requirements” at <a href="http://www-306.ibm.com/software/webservers/appserv/doc/latest/prereq.html">http://www-306.ibm.com/software/webservers/appserv/doc/latest/prereq.html</a> to determine the hardware requirements for your particular operating system and version of WebSphere Application Server.</td>
</tr>
</tbody>
</table>
Prerequisites

Table 8. Individual Agent Requirements (continued)

<table>
<thead>
<tr>
<th>Agent</th>
<th>Operating Systems</th>
<th>Hardware</th>
<th>Other Requirements</th>
</tr>
</thead>
</table>
| WebSphere InterChange Server | Windows 2000, Windows XP Professional Edition | 2 Mb of disk space | - IBM® WebSphere® InterChange Server, v4.2.2  
- One of the IBM SNMP agents that come with WebSphere Interchange Server must be installed and configured to monitor each server you want to monitor. The OMEGAMON XE for WebSphere InterChange Server monitoring agent must be configured as the SNMP manager for the agent. The SNMP Polling Interval (set in the SNMP Agent Configuration Wizard) should not exceed 5 minutes.  
- Only one OMEGAMON XE for WebSphere InterChange Server monitoring agent (KICAgent) should be installed, preferably on the same host as the CandleNet Portal Server.  
- One WebSphere InterChange Server Data Source should be installed on the host of each monitored WebSphere InterChange Server. On Windows, the user ID SYSTEM must have full control of all the files in the WebSphere InterChange Server directory in order for log data to be available. Check the Security tab of the directory’s properties page to ensure that SYSTEM has the proper authority. |
### Prerequisites

**Windows Management Web Service monitoring agent**
- **Operating Systems**: Windows XP Professional Edition recommended (.NET platforms only)
- **Hardware**: Can run on Windows 2000 only if the .NET framework has been installed.
- **Other Requirements**: Windows Management Instrumentation (WMI) Universal Agent WBEM Data Provider

**Windows Active Directory Servers monitoring agent**
- **Operating Systems**: Windows 2003 Server
- **Hardware**: 2Mb disk space
- **Other Requirements**: Active Directory 2003 in a native mode environment

**Windows Servers monitoring agent**
- **Hardware**: 2Mb disk space

---

**Table Note 1– Supported Historical Database Client Software**: Candle has tested and supports the Warehouse Proxy on Windows XP Professional Edition or Windows 2000 with the following database client software.
- Microsoft SQL Server v7.0
To Do Before Beginning

Windows logon ID
Your Windows logon ID must be a member of the “Administrators” system group.

Stopping Lotus Notes server
If the Lotus Notes server is running on this machine, stop the Lotus Notes server before starting the OMEGAMON XE installation. This applies only to the server (not to individual Lotus Notes applications).

HOST file
Candle products do not require a DNS. If your Windows systems are running without DNS, make sure the HOST file of the local machine is up to date.

Downloading JRE, if necessary
CandleNet Portal requires one of the supported versions of the JRE: 1.3.1_04 to 1.4.2. If you do not plan to install CandleNet Portal Server or CandleNet Portal Desktop Client, skip this step. This step is required only if you intend to install these components and you do not have the required JRE installed locally.

2. Follow the download instructions on the site.

Note: CandleNet Portal supports multiple versions of the JRE on the same machine and on different browser clients. See the "Java Runtime Environment" section of the CandleNet Portal Administrator’s Guide for details and for troubleshooting notes.

Installing DB2 UDB
The OMEGAMON XE installation package comes with DB2 Universal Database Workgroup Server Edition. Install DB2 UDB on the machine where
you will be installing a CandleNet Portal Server. If you do not intend to install
a CandleNet Portal Server, skip this step.

**Note:** If you already have a DB2 UDB (version 7 or 8) installation, you need
not install the DB2 UDB (version 8.1) included in your Candle
package unless you want to upgrade to version 8.1.

**Upgrading from a version that used MSDE or Microsoft SQL Server**

If you will be upgrading the CandleNet Portal Server from an earlier version
that used MSDE for the CandleNet Portal Server database, the migration to
DB2 UDB is done by the Candle installer.

If Microsoft SQL Server (version 7.0) was used for the CandleNet Portal
Server database, the Candle installer will give you the choice of moving it to
DB2 UDB or keeping the database on Microsoft SQL Server. We recommend
you migrate the database to DB2 UDB.

**Installation**

1. On the machine where the CandleNet Portal Server will be installed, log on to
Windows with a local ID that has Administrator authority. If you are unsure,
see “Windows User Accounts” on page 60 before proceeding.

The DB2 UDB installation will add a local “db2admin” user account to
Windows, which it cannot do if your local ID does not have Administrator
authority. Without the db2admin ID, DB2 UDB will be unable to create the
CandleNet Portal Server database and the CandleNet Portal Server will not
start.

2. Insert the *DB2 Universal Database Workgroup Server Edition* CD to start the
install wizard.

3. Select “Install Products” and proceed through the license agreement and
other screens.

4. Select the installation type: Accept the defaults.
To Do Before Beginning

Do not select “Data warehousing”. This is unrelated to the Candle data warehouse, which is configured separately.

5. Select the “installation” folder: Change the installation drive if necessary.

6. Set user information for the DB2 Administration Server:
   1. Accept the user name of “db2admin”.
   2. Enter a password. We recommend “candle”.
   3. Do not enter a domain name in the drop-down list.

The "db2admin" user name and “candle” password are not an absolute requirement. If you use a different name (up to eight letters and numbers) and password, keep them written down somewhere. DB2 UDB requires the user name and password for all administrative tasks, and the Candle installer requires them to create the CandleNet Portal Server database, as does Candle Support if you need troubleshooting assistance.

If the Windows Local Security Settings on this machine enables complex or long passwords, use whatever password fits the requirements. This Windows setting also affects CandleNet Portal Server installation. See “Windows local security settings: long or complex passwords” on page 61.
7. On the remaining screens, select the defaults.
8. Click **Install** to start copying the files.
9. After the installation is complete, restart Windows before installing Candle products. (Restart Windows even if the DB2 UDB installer does not ask you.)

**Note:** If the Windows Local Security Policy on this machine is set to require complex passwords, you must create a new Windows user named CNPS before the Candle installer can configure the CandleNet Portal Server. Follow the instructions under “Windows local security settings: long or complex passwords” on page 61 before proceeding.

**Troubleshooting**

If the CandleNet Portal Server does not start after it has been installed, it may be because the Candle installer fails when it attempts to create the CandleNet Portal Server database for the CandleNet Portal Server. Two likely causes are:

- the db2admin user ID was created on the network domain and not the local host.
- the db2admin user ID no longer has administrator privileges
Both conditions are described in the “Installing DB2 Servers (Windows)” chapter of the *IBM DB2 Universal Database – Quick Beginnings for DB2 Servers* manual.

**Windows User Accounts**

The Windows user ID you use when you install DB2 UDB must be part of the “Administrators” group on this machine. Additionally, another instance of this user name must not exist on the network domain unless it has administrator authority.

If you are not sure, check your ID in the Control Panel User Accounts. The machine’s host name should show in the Domain column (“CNPUSER” in the example right) and “Administrators” in the Group column.

**Is the db2admin user account on the local domain?**

If you have already installed DB2 UDB, you can check that the domain associated with the db2admin user ID is the host name, and change it if necessary.

2. Select “Services”.
3. In the Services window, right-click the service named “DB2 - DB2” and select “Properties” from the pop-up menu.
4. Check the Log On tab for ".\db2admin" as the user account.

5. If the account shows the network domain (such as \NOTES\db2admin), edit it to remove the network domain and type a period ("." ) for the local domain:

   
   .\db2admin
   

Windows local security settings: long or complex passwords

The following Windows user IDs are required by DB2 UDB:

- "db2admin", added when you install DB2 UDB and required by the Candle installer when the database is created for the CandleNet Portal Server.
- "CNPS", added during installation when the CandleNet Portal Server database is configured.

If the Windows Local Security Settings are enabled for long or complex passwords, you must use a password of the required syntax for these IDs.
To Do Before Beginning

Additionally, if your environment requires passwords to be changed periodically, do the following to change CandleNet Portal Server database user account password:

1. On the machine where the CandleNet Portal Server is installed, log on to Windows with a local administrator ID.

2. Select Start > Programs > Candle OMEGAMON XE > Manage Candle Services.

3. Right-click the CandleNet Portal Server and select Advanced > Utilities > Build CNPS Database from the pop-up menu.

4. Click “DB2” to open the CNPS Data Source Config Parameters dialog.

5. Enter the new password for the CandleNet Portal Server database user ID.

Uninstalling DB2 UDB

If a Candle Support representative instructs you to uninstall DB2 UDB, you need also to remove the DB2 data folders.

1. Insert the DB2 Universal Database Workgroup Server Edition CD to start the install wizard, and follow the steps to uninstall.

   This uninstalls DB2 UDB from c:\Program Files\IBM\SQLLIB, but not the data folder, which also has to be deleted.

2. Delete the DB2 UDB directory on the drive where you installed it.

   It is normally on the root directory of the drive, such as c:\DB2.

Installing ETEWatch, if necessary

If you do not intend to install the eBA Solutions monitoring agent, skip this step.

The monitoring agent for ETEWatch allows you to monitor ETEWatch data in your OMEGAMON XE environment. This agent makes ETEWatch detail and summary data, including exceptions detected by the ETEWatch Manager.
To Do Before Beginning

Client, available to OMEGAMON XE for situation monitoring and workflow management.

You must install ETEWatch before installing the eBA Solutions monitoring agent. For more information, see the OMEGAMON Monitoring Agent for eBA Solutions User’s Guide.

Be sure that:

- When configuring the ETEWatch Manager Client (which summarizes data and transmits it to the ETEWatch Manager Server), activate the setting that causes the client to send data to the Manager Server. Remember to enable alerts (exceptions).

- If an ODBC driver is used to access the ETEWatch database, create a Data Source Name (System DSN) and configure the ETEWatch Manager Server to log data to it (by turning on the “Use ODBC” option and entering the previously created DSN in the Database Connection field).

  For more information on configuring the Manager Server to store ETEWatch data in an external database, see the OMEGAMON Monitoring Agent for eBA Solutions User’s Guide.

- You verify your ETEWatch installation, ensuring that all components are running.

Authorizing users for OMEGAMON XE for WebSphere MQ

If you are not installing OMEGAMON XE for WebSphere MQ Monitoring and OMEGAMON XE for WebSphere MQ Configuration, skip this step.

This step sets user ID authorization required for running OMEGAMON XE for WebSphere MQ Monitoring and OMEGAMON XE for WebSphere MQ Configuration. Only Windows user IDs that are members of group “mqm” are authorized to start and stop OMEGAMON XE for WebSphere MQ Monitoring or OMEGAMON XE for WebSphere MQ Configuration.

Follow these steps:

1. Log on to Windows as a System Administrator.
2. From the Start button, select: “Programs > Administrative Tools > User Manager“.
3. Double-click the user IDs in the upper window that you wish to assign to group “mqm”.

63
The User Properties dialog opens.

4. Click the Groups button (bottom left corner).
   The Group Memberships dialog opens.

5. Check the “Member of list.” If group “mqm” is not listed, select it from the “Not Member of” list, and click Add.

6. Click OK twice to exit the dialogs.

7. Close the User Manager window.
Preparation for Upgrading and Migrating from a Previous Installation

Introduction

This chapter includes information you need to know and tasks you need to do to prepare for upgrading and migrating your previously installed OMEGAMON XE or CCC to the new OMEGAMON XE (version CT350).

Chapter contents

Upgrade and Migration Planning ........................................... 66
To Do Before Beginning ..................................................... 68
Upgrade and Migration Planning

This section discusses some issues you should consider before upgrading Candle products.

Staging your upgrade--version compatibility

Existing customers who wish to upgrade their Candle products in stages should review the following guidelines, which expand upon the general order noted in “General order of installation or upgrade” on page 34:

- After you upgrade your hub CMS to version CT350, it will continue to communicate properly with CMSs and CMWs running previous versions.
- After you upgrade your hub CMS to version CT350, it will continue to communicate properly with agents from a previous release. However, be aware that some older products may not have the same level of Y2K compliance as the latest version. For information regarding the level of compliance for each Candle product, visit the Candle Web site at www.candle.com and click the Customer Support link.
- After you upgrade your CMW to version CT350, you may experience loss of function with some agents from a previous release. Therefore, Candle recommends that you maintain a CMW (version CT300) connected to the back-level versions of the agents. As you upgrade each agent, reconnect it to the CMW (version CT350).

Product versions earlier than those listed above may not be compatible with this release. Contact your Candle customer support representative for assistance. Note that until your upgrade is complete, you may not experience the full capabilities of this release.

Migrated information when upgrading from a previous version

If you are installing over a previous release (into the same Candle directory) the following information is migrated into version 350:

- CMW customizations (user IDs, managed systems lists, workgroups)
- Port number and communication protocol settings
- Situations
Preserving a previous version

If you want to preserve an existing CCC (version 3xx) as well as install an OMEGAMON XE (version CT350), and you have enough disk space to install another version on your workstation, consider using the Candle System Backup and Restore Utility to back up that version's registry entries in case you want to back out of the OMEGAMON XE (version CT350) install. See “Candle System Backup and Restore Utility” on page 139 before proceeding.

*Note:* You cannot have both versions running in the same Windows environment at the same time. Start one version or the other.

Upgrading a remote CMS while retaining a prior level hub CMS

If you are incrementally upgrading a remote CMS to version CT350 but retaining an older version of the hub CMS, the following steps must be performed for successful operation. Version CT350 requires a new logical network static definition kept in the static definition file QA1CIOBJ.

1. Bring down the hub CMS.
2. From a CMS (version CT350) obtain a copy of QA1CIOBJ.DB and QA1CIOBJ.IDX.
3. Place these files into the hub tables environment before restarting the hub CMS.
4. Restart the hub CMS.

Affinity considerations

Each installed package for a CMS distinguishes itself from other packages/products by using affinity information to describe it. With some installed packages it is possible to lose resolution to the installed agents if the package is not strictly following versioning guidelines set forth by the hosting OMEGAMON XE environment. If agents of a given product are no longer visible to the end user at a CMW or CandleNet Portal client then it is likely a specific affinity change to the installed products may be necessary. Since this involves changing product-provided data to reflect the affinity change, it is recommended that you contact Candle customer support with the problem and the necessary changes can be implemented with the help of Candle customer support personnel on your behalf.
To Do Before Beginning

Stopping components

Stopping software components that are being upgraded
To upgrade a software component, that software component must be stopped before performing the installation.

Stopping the WebSphere Application Server and Candle processes
To upgrade from a previous installation of OMEGAMON XE for WebSphere Application Server, the WebSphere Application Server and all Candle processes must be shut down prior to the upgrade installation in order to release all open files. This will include:

- WebSphere Application Server
- CMS
- CandleNet Portal Server

This is in addition to the requirement of stopping the OMEGAMON XE for WebSphere Application Server agent prior to the upgrade installation.

OMEGAMON XE for WebSphere Integration Brokers: deactivating brokers
On a Windows system that has a previous release of the OMEGAMON XE for WebSphere Integration Brokers installed, if a broker is active during the installation of the OMEGAMON XE for WebSphere Integration Brokers agent, the new release of the CandleMonitor node plug-in module will not be installed properly in the broker environment.

It is recommended that Windows brokers are not active during the installation of the OMEGAMON XE for WebSphere Integration Brokers agent so that the installation can be completed successfully.

Note: If you must leave the broker active during the install and when the broker is shut down, you will have to manually copy the kqipnode.lil file from the Candle\CMA directory to the applicable IBM broker product bin directory and restart the broker. (See the “Activating the CandleMonitor Node” section of the “Configuring the CandleMonitor Node” chapter of the “OMEGAMON XE for
To Do Before Beginning

WebSphere Integration Brokers User’s Guide” for further details about where to copy the files.) On any platform, the broker will have to be restarted after the installation of the OMEGAMON XE for WebSphere Integration Brokers agent in order to pick up the new release of the CandleMonitor node plug-in module.

**Hot Standby feature: upgrading a hub CMS**

- If you have already installed other parts of this release and have already configured the Hot Standby feature, and you are upgrading a hub CMS, stop all the CMWs and agents that are connected to it, even the ones on remote machines, before starting the OMEGAMON XE installation. Otherwise, CMWs and agents that have been configured for Hot Standby will switch to the backup CMS.

**Handling of existing historical data**

This information applies to these products:

- OMEGAMON XE for WebSphere Integration Brokers
- OMEGAMON XE for WebSphere MQ Configuration
- OMEGAMON XE for WebSphere MQ Monitoring
- OMEGAMON XE for WebSphere Application Server

If you are upgrading from a previous version of one of these products (for example, from version 110 to version 120 of OMEGAMON XE for WebSphere Integration Brokers), you should use standard procedures to archive and clear out any existing historical data prior to doing an upgrade. (Consult the Historical Data Collection Guide for OMEGAMON XE and CandleNet Command Center for information about handling history files.) If this is not done, it is likely that any previously existing historical data will not be archived properly once the new agent is run. Also, historical reports will not show data.

If there is no concern for archiving the previous historical data, the history files can just be deleted. These files are in one or more of these locations:

1. the c:\Candle\Cma\logs subdirectory
2. the c:\Candle\Cma\logs\history\pc\instancename subdirectory
3. if history was configured to be collected at the CMS, the c:\candle\cms subdirectory
To Do Before Beginning

where

- **pc** is the product code:
  - “qi” for OMEGAMON XE for WebSphere Integration Brokers
  - “mc” for OMEGAMON XE for WebSphere MQ Configuration
  - “mq” for OMEGAMON XE for WebSphere MQ Monitoring
  - “we” for OMEGAMON XE for WebSphere Application Server

- **instancename** is the name entered for a previous creation of an instance

These files have names of the format

- “kqi*.hdr” and “kqi*.” for OMEGAMON XE for WebSphere Integration Brokers
- “kmc*.hdr” and “kmc*.” for OMEGAMON XE for WebSphere MQ Configuration
- “kmq*.hdr” and “kmq*.” for OMEGAMON XE for WebSphere MQ Monitoring
- “kwe*.hdr” and “kwe*.” for OMEGAMON XE for WebSphere Application Server

**Note:** These formats for filenames

- kqi*.
- kmc*.
- kmq*.
- kwe*.

*denote filenames that do not have associated extensions.*

CandleNet Portal Server database requirements

If you have installed previous versions of Candle products or are migrating from a previous version of Candle Technologies® (CT®), you still need to install Microsoft SQL Server or DB2 UDB (See “Installing DB2 UDB” on page 56 and “CandleNet Portal Server database” on page 46.) before you go on to install the CandleNet Portal Server. If you have a previous installation of the CandleNet Portal Server that uses MSDE, you must install DB2 UDB. The
To Do Before Beginning

installer migrates the CandleNet Portal Server database from MSDE to DB2 UDB. MSDE is no longer supported
To Do Before Beginning
Introduction


Note: The installation procedure is based on a first-time installation of OMEGAMON XE. If this is an upgrade of your components, see “Preparing for Upgrading and Migrating from a Previous Installation” on page 65 before continuing with these steps.

Chapter contents

Starting setup.exe ................................................. 75
Selecting Components and Starting to Copy Files .................. 76
Initial Configuration Steps ......................................... 78
Creating the CandleNet Portal Server Database ..................... 79
Configuring the CandleNet Portal Server .......................... 81
Configuring the CMS ............................................. 94
Configuring Agent-to-CMS Communication ........................ 103
Completing Installation ........................................... 107
Configuring the Agents .......................................... 108
Installing OMEGAMON DE ........................................ 110
Rebooting and Starting Candle Services .............................. 111
Starting the CMW .................................................. 112
Using KIB_CLEAN=Y, if Necessary ................................. 114
Starting CandleNet Portal Desktop Mode ........................... 116
Starting CandleNet Portal Browser Mode ........................... 117
Configuring the ODBC Data Source, if Necessary ................. 119
Starting setup.exe

In this step you will start the setup.exe installation program and specify the target directory for the OMEGAMON XE software.

Note: Previous users: If you are upgrading from a previous release of OMEGAMON XE, the software will be loaded to your existing Candle directory. Do not create a new directory.

Follow these steps:

1. Log onto Windows using an ID with Administrator authority and close any running applications.

2. Insert the OMEGAMON XE CDROM into your CDROM drive. Installation begins automatically. (If the installer does not start, go to CD directory WINDOWS and run setup.exe. If setup.exe initialization fails, you do not have enough disk space to decompress the setup files.)

   The Candle CD Browser opens.

3. If you want to access the documentation that pertains to the products you are installing, click Launch Documentation.

4. When you want to proceed with the installation, click Install Product.

   The Candle OMEGAMON XE - InstallShield Wizard dialog opens.

5. Read the text that welcomes you to the installation, and click Next to continue.

6. When the License Agreement opens, read the software license agreement, select “I accept the terms of the license agreement,” and click Next.

   The Choose Destination Location dialog is displayed.

7. Specify the target drive and directory where you want to download the OMEGAMON XE software. The default is:

   C:\Candle

   (If necessary, change the destination path.)

8. Click Next to continue.
Selecting Components and Starting to Copy Files

In this step you will choose the OMEGAMON XE components you want to install locally.

The Select Features dialog is displayed.

1. Select (check) the main OMEGAMON XE features that you want to install on this machine. You may install all components at once, any combination of components, or any single component.

2. If you tried to select “CandleNet Portal Server and Application Support” and you
   - have not already installed a required version of JRE (1.3.1_04 to 1.4.2),
   - or
   - have not already installed a required version of DB2 Universal Database
   a dialog box will appear that tells you of the requirements to do so.
   1. Click **OK** in the dialog box that tells you of the requirements.
   2. Perform the instructions for “Downloading JRE, if necessary” on page 56 or “Installing DB2 UDB” on page 56.
   3. Restart setup.exe.

3. If you tried to select “CandleNet Portal Desktop Client and Application Support” and you have not already installed a required version of JRE (1.3.1_04 to 1.4.2), a dialog box will appear that tells you of the requirement to do so.
   1. Click **OK** in the dialog box that tells you of the requirement.
   2. Perform the instructions for “Downloading JRE, if necessary” on page 56.
   3. Restart setup.exe.

4. Click the + sign next to each main feature to expand the tree.

5. Leave selected (checked) each product or type of support that you want to install. Deselect (uncheck) each product or type of support that you do not want to install.

   **Note:** OMEGAMON Web Services (SOAP server) will be installed automatically with the CMS.

6. Click **Next** to continue.
Selecting Components and Starting to Copy Files

Note: The instructions for the rest of the chapter correspond to a full installation of Candle products that is typical of first-time installations. If you are installing only particular components, for example only agents, some steps may be unnecessary and the referred-to screens may not appear.

7. If you left the Monitoring Agent for Tuxedo selected in Step 5. on page 76, the Setup Type dialog will appear. Select the version of Tuxedo you will be monitoring.
   Click Next.

8. The Select Program Folder will appear. To determine the folder in which the files will be installed, accept the folder name that appears in the Program Folder text box, type in a new name, or select one of the existing folders in the list below. Candle recommends that you use the default Program Folder name shown.

9. Click Next to continue.
   The Start Copying Files dialog will appear. This dialog shows the destination directory and program folder information you supplied in the previous steps, and lists the modules you chose to install.

10. Review the settings and click Back if you want to go back and change them. If you want to start copying files with the settings that are listed, click Next.
    The installer will begin configuring the installation and copying files needed to complete the installation.
Initial Configuration Steps

In this step, you will perform configuration of certain components before the completion of installation.

The Setup Type dialog will appear.

1. Leave selected (checked) the items that you want to configure before completion of the installation. Deselect the items for which you want to delay configuration until after completion of the installation.

2. Click **Next** to continue.

   The Define CNP Host Information dialog will appear.

3. Confirm the local host name.

4. Click **Next** to continue.
Creating the CandleNet Portal Server Database

If you are not installing the CandleNet Portal Server, skip this step.

In this step you will identify the CandleNet Portal Server database. The Setup installation tool attempts to detect the required database product and prompts you to confirm the database you want to use.

After the Candle software is copied to disk, the CNPS Data Source Config Parameter dialog opens.

1. Enter the password for db2admin, then enter a password for the CandleNet Portal Server database user ID to be created, and click OK.

You can use a different name for the CandleNet Portal Server database user ID, but it must adhere to the rules for DB2 UDB user accounts, described in the “Installing DB2 Servers (Windows)” chapter of the IBM DB2 Universal Database – Quick Beginnings for DB2 Servers manual.

2. When the following message appears, click OK to continue.

   **CNPS configuration completed successfully. Please see C:\Candle\INSTALL\CNPS_ODBC.log for details.**
Creating the CandleNet Portal Server Database

If, instead, you get an error, the Candle installer was unable to create the CandleNet Portal Server database. See “Installing DB2 UDB” on page 56 and the troubleshooting notes in the same section, or contact Candle support.
Configuring the CandleNet Portal Server

Complete this step only if you installed the CandleNet Portal Server on this machine.

The first CNP Server Configuration dialog opens:

1. Do one of the following:
   - If the CandleNet Portal Server will access the CMS through a firewall, check “Connection must pass through firewall”.
     - The IP.PIPE protocol is automatically selected for Protocol 1. You must use IP.PIPE if the CandleNet Portal Server resides outside a firewall. The remaining two Protocol fields are disabled; only IP.PIPE may be used.
     - If your site uses Network Address Translation (NAT) between the CandleNet Portal Server and the CMS, check “Address Translation Used”.
   - If the CandleNet Portal Server will not communicate with the CMS across a firewall, select up to three communications protocols (Protocol 1, Protocol 2, and Protocol 3) for the CandleNet Portal Server:
     - TCP/IP
Configuring the CandleNet Portal Server

- SNA
- IPPipe

The CandleNet Portal Server will use Protocol 1, if it is available. If not, it will use Protocol 2. If that is not available, it will use Protocol 3.

2. Click **OK** to open the second CNP Server Configuration dialog:
Configuring the CandleNet Portal Server

Use the following table to complete the second CNP Server Configuration dialog:

**Table 9. Second CNP Server Configuration Dialog**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If you’re configuring TCP/IP communication, enter the following under IP Settings of the CMS:</strong></td>
<td></td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides.</td>
</tr>
<tr>
<td>Port number</td>
<td>The CMS listening port for the agent. Candle recommends you use port number 1918; however, if you must change it, enter the new port number (Candle recommends numbers 1025 to 65535).</td>
</tr>
<tr>
<td><strong>If you are configuring SNA communication, enter the following under SNA Settings of the CMS:</strong></td>
<td></td>
</tr>
<tr>
<td>Network Name</td>
<td>Your site’s SNA network identifier.</td>
</tr>
<tr>
<td>LU Name</td>
<td>The LU name for this agent. This LU name corresponds to the Local LU Alias in your SNA communications software.</td>
</tr>
<tr>
<td>LU6.2 LOGMODE</td>
<td>The name of the LU6.2 logmode. Candle recommends that you use the default name shown: CANCTDCS.</td>
</tr>
<tr>
<td>TP Name</td>
<td>The Transaction Program name for this agent.</td>
</tr>
<tr>
<td><strong>If you’re configuring IP.PIPE communication, enter the following under IP.PIPE Settings of the CMS</strong></td>
<td></td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides.</td>
</tr>
<tr>
<td>Port number</td>
<td>The listening port for the agent. Candle recommends that you use port number 1918; however, if you must change it, enter the new port number (Candle recommends numbers 1025 to 65535).</td>
</tr>
<tr>
<td>Partition Name</td>
<td>(Required only by sites using address translation.) The name of the partition that the CandleNet Portal Server uses, up to 32 letters and numbers. This name will be stored in the CandleNet Portal Server KFWENV file and corresponds to the partition name entry in the hub CMS partition file.</td>
</tr>
<tr>
<td>Entry Options:</td>
<td>Candle recommends that you retain the default setting.</td>
</tr>
</tbody>
</table>
Configuring the CandleNet Portal Server

3. Click **OK** to confirm the CandleNet Portal Server configuration you have supplied.

Connection to an external Web server

**Browser client**
During installation, the Candle integral Web server is installed as a component of the CandleNet Portal Server. You can also use an external Web server on your CandleNet Portal Server machine, as shown in the “Firewall scenarios” starting on page 86.

Currently, Candle supports an external Web server for Browser Client access only on the same machine as the CandleNet Portal Server.

**Desktop client**
Although the desktop client does not need a Web server to start CandleNet Portal, it does use it for common files stored on the CNP Server, such as the graphic view icons and style sheets. If your CNP Server setup disables the integral Web server and uses only an external web server, you need to specify the “ior” for every desktop client.

1. On the machine where the CandleNet Portal desktop client was installed select “Start > Programs > Candle OMEGAMON XE > Manage Candle Services”.
2. Right-click CandleNet Portal – Desktop, then select Reconfigure from the pop-up menu.
4. In the Value field, enter the Web server address where the cnps.ior can be found.
   For example, if the web server name is xyz.myserver.com and the document root for the web server was configured to be `\candle\cnb`, the value to enter would be
   \[ http://xyz.myserver.com/cnps.ior \]
5. Check “In Use” and click **OK**.

**NATted firewall or multiple NICs**

The URL for starting CandleNet Portal browser mode includes the CNP Server machine’s hostname or IP address. The address for starting CandleNet
Portal is set for the desktop client during installation or through Manage Candle Services. If any of the following is true in your configuration, you need to define a CNPS interface through Manage Candle Services:

- A firewall with Network Address Translation (NAT) is used between the client and CNP Server.
- The CNP Server was configured to be accessed via a secondary Network Interface Card (NIC).

### Defining a CandleNet Portal Server interface

1. On the machine where the CandleNet Portal Server is installed, select “Start > Programs > Candle OMEGAMON XE > Manage Candle Services”.
2. Right-click “CandleNet Portal Server” to open the pop-up menu.
3. Point to “Advanced” and select “Configure CNPS Interfaces”.

The CNPS Interface Definitions dialog opens. Initially, the list has one definition named “cnps”, using port 15001 for the CandleNet Portal Server, and the Candle integrated web server at http://mysystem:1920///cnp/client (where mysystem is the host name). Port 80, for an external Web server, is assumed if the URL does not specify 1920 for the integrated Web server.
Configuring the CandleNet Portal Server

4. Click **Add**.

![Define CNPS Interface](image)

5. Define the interface as follows:
   1. “Interface Name”: enter a one-word title for the interface.
   2. “Host”: If you are defining an interface for a specific NIC or different IP address on this machine, enter the TCP/IP host address. Otherwise, leave this field blank.
   3. “Proxy Host”: If address translation (NAT) will be used, enter the TCP/IP address used outside the firewall. This is the NATed address.
   4. “Port”: Enter a new port number for the CandleNet Portal Server. The default 15001 is for the server’s host address, so a second host IP address or a NATed address requires a different port number.
   5. “Proxy Port”: If the port outside the firewall will be translated to something different than what is specified for “Port”, set that value here.

6. Click **OK** to add the new CandleNet Portal Server interface definition to the list.

**Firewall scenarios**

These diagrams illustrate several firewall scenarios using various combinations of the Candle integral Web server, a third-party Web server, NAT, and a second NIC on the CandleNet Portal Server machine.
Figure 3. Intranet with Integral Web Server

Figure 3 shows a configuration that:
- Has an intranet firewall.
- Has no NAT.
- Uses the integral Web server.

The default CandleNet Portal interface, cnps is used. No additional interface definitions were needed. Browser mode users, whether going through the firewall or not, start CandleNet Portal with

http://10.10.10.10:1920///cnp/client

or substitute the host name for the IP address.

For configurations using only the Candle Web server and these port numbers, use the default cnps interface definition.

In this scenario, the CMS and agents may or may not be installed on the CandleNet Portal Server system.
Figure 4. Intranet with External Web Server

Figure 4 shows a configuration that:
- has an intranet firewall
- has no NAT
- uses an external Web server (such as Apache or IIS)

Browser mode users, whether going through the firewall or not, start CandleNet Portal with http://10.10.10.10 or http://10.10.10.10/mydirectory (where mydirectory is the alias), or substitute the host name for the IP address.

For intranet configurations using an external Web server, with no NAT, you do not need to add a new interface definition. Web server port 80 is used automatically when none is specified in the URL.

In this scenario, the CMS and agents may or may not be installed on the CandleNet Portal Server system.
Figure 5 shows a two-part configuration:

- intranet firewall without NAT and using the integral Web server
- Internet firewall with NAT and using an external Web server

Intranet users can enter the URL for either the integral Web server or the external Web server: http://10.10.10.1920///cnp/client or http://10.10.10.10.

Internet users enter the URL for the NATed address: http://198.210.32.34/?ior=internet.ior (or substitute the host name for the IP address).
Configuring the CandleNet Portal Server

The Internet configuration requires a new CandleNet Portal Server interface definition: proxy host address 198.210.32.34 and port number 15002. The intranet firewall uses the cnps definition.

![Define CNPS Interface](image)

In this scenario the CMS and agents may not be installed on the CandleNet Portal Server system.
Figure 6 shows a three-part configuration:

- intranet firewall with NAT through the firewall to the external Web server
  http://192.168.1.100/?ior=intranet.ior
- without NAT inside the DMZ to the integral Web server
  http://10.10.10.10:1920///cnp/client
- Internet firewall with NAT through the firewall to the external Web server

The intranet firewall configuration requires a new CandleNet Portal Server interface definition: proxy host 192.168.1.100 and port 15003.

The intranet DMZ configuration uses the default CandleNet Portal Server interface definition.
Configuring the CandleNet Portal Server

The Internet configuration uses the same CandleNet Portal Server “internet” interface definition as the previous scenario: proxy host 198.210.32.34 and port 15002.

In this scenario, the CMS and agents may not be installed on the CandleNet Portal Server system.

Figure 7. Two Host Addresses, Intranet and Internet, and with Integral and External Web Servers

Figure 7 shows a two-part configuration:

- Intranet firewall with NAT through the firewall to the external Web server uses http://192.168.1.100, and without NAT inside the DMZ to the integral Web server uses http://10.10.10.1920///cnp/client
- Internet firewall with NAT through the firewall to the external Web server http://198.210.32.34
The intranet firewall configuration uses the same CandleNet Portal Server interface definition (named “intranet”) as in the previous scenario: host 10.10.10.10; proxy host 192.168.1.100; and port 15003.

The intranet DMZ configuration uses the default CandleNet Portal Server interface definition. CandleNet Portal Server interface definition: host 192.168.33.33; proxy host 198.210.32.34; port 15002; and proxy port 444.

In this scenario, the CMS and agents may not be installed on the CandleNet Portal Server system.
Configuring the CMS

Complete this step only if you installed a CMS on this machine.

In this step you will configure the CMS. You will:

- Define the type of CMS (hub or remote).
- Assign a unique name to the CMS.
- Specify communication protocol information for the CMS.
- Seed the CMS (unless instructed to do so at a later time).

The Candle Management Server Configuration dialog is displayed.

1. Under CMS Type, select the type of CMS: “Hub” or “Remote”.
2. In the CMS Name field, enter the unique name you want to assign to this CMS. The name must be alphanumeric (2-32 characters) and must begin with an alpha character. No blanks or special characters are allowed.
   
   The default CMS name for a new installation is:

   **HUB_hostname**

   Where *hostname* is the TCP/IP hostname of the local machine.

   If a CMS has already been configured on this machine, then the current CMS name is displayed. If you need to support legacy agents on other machines, then you should re-use the name of your current CMS.

3. Under Protocol for this CMS, select up to three communications protocols (Protocol 1, Protocol 2, and Protocol 3) for the CMS. The CMS will use Protocol 1, if it is available. If not, it will use Protocol 2. If that is not available, it will use Protocol 3.

   The following protocols are valid:

   - TCP/IP
   - SNA
   - IP.PIPE

   If your OMEGAMON XE agents, CandleNet Portal Server or CMW must communicate with the CMS across a firewall, you must select “IP.PIPE”. When it is selected, the Address Translation field is enabled. If your firewall uses address translation, click this field.
4. Do not select “Configure Hot Standby CMS” the first time you configure. You can easily reconfigure the CMS at a later time if you decide to enable this advanced feature. See “Hot Standby Feature (optional)” on page 134 for more information.

5. “Configuration Auditing” is selected by default. Candle recommends that you retain this setting.

6. If you are installing OMEGAMON SOAP Server and want to enable support for it, make sure “OMEGAMON SOAP Server” is selected. See “Configuring OMEGAMON XE Web Services (SOAP Server)” on page 125 for more information.

7. Do not select “Security: Validate User” the first time you configure the CMS. Instructions for enabling this feature are provided later in this chapter, in “Enabling Security (optional)” on page 121.

8. Click OK to continue.

9. The Hub CMS Configuration dialog opens. (If you chose a remote type CMS, skip to page 99.) One or more of the Settings fields is enabled, depending upon which communications protocols you selected. Use the table below to complete the communications settings for this CMS.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Options</td>
<td>Candle recommends that you retain the default setting (convert to upper case) for installation testing purposes.</td>
</tr>
</tbody>
</table>
**Table 10. Communication Settings for this CMS (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Settings</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides. You are configuring the hub CMS now on this machine, enter the hostname or IP address of this machine.</td>
</tr>
<tr>
<td>Port number</td>
<td>The TCP/IP listening port for the CMS. Candle recommends that you use port number 1918; however, if you must change it, enter the new port number (Candle recommends numbers 1025 to 65535). You must specify the same port number for the hub CMS, all remote CMSs reporting to it, and a hot-standby CMS, if one is defined.</td>
</tr>
<tr>
<td>SNA Communication Settings: Hub CMS</td>
<td></td>
</tr>
<tr>
<td>Network Name</td>
<td>Your site’s SNA network identifier.</td>
</tr>
<tr>
<td>LU Name</td>
<td>The LU name for this CMS. This LU name corresponds to the Local LU Alias in your SNA communications software.</td>
</tr>
<tr>
<td>LU6.2 LOGMODE</td>
<td>The name of the LU6.2 logmode. Candle recommends that you use the default name shown: CANCTDCS.</td>
</tr>
<tr>
<td>TP Name</td>
<td>The Transaction Program name for this CMS.</td>
</tr>
<tr>
<td>IP.PIPE Communication</td>
<td>The information below assumes that you have read “Configuring OMEGAMON XE Across a Firewall” on page 37. If you have not yet reviewed that section, do so now before proceeding. When you are ready, enter the following under IP.PIPE Settings:</td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides. You are configuring the hub CMS now on this machine, enter the hostname or IP address of this machine.</td>
</tr>
<tr>
<td>Port number</td>
<td>The listening port for the CMS. Candle recommends that you use port number 1918; however, if you must change it, enter the new port number (Candle recommends numbers 1025 to 65535). You must specify the same port number for the hub CMS, all remote CMSs reporting to it, and a hot-standby CMS, if one is defined.</td>
</tr>
</tbody>
</table>
Configuring the CMS

10. Click OK.
   The Seed CMS dialog is displayed.

11. Select the location of the CMS.

12. Click OK. You will be greeted with a dialog that says that the CMS is not currently running and that, if you choose to continue, it will be started.

### Table 10. Communication Settings for this CMS  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition File</td>
<td>(Required only by sites with firewalls that use address translation.) The name of a partition text file. Either accept the default (c:\Candle\CMS\kdcpartition.txt) or enter a new name; for example: c:\Candle\CMS\hubpart.txt. To create entries in the partition file, do the following: 1. Click Modify. The Edit Partition File dialog is displayed. 2. Click Add. The Add Partition dialog is displayed; you are prompted for Host name and Partition Name.</td>
</tr>
<tr>
<td></td>
<td>For Hostname, enter a hostname (or IP address) that uniquely identifies this CMS host in the other partition. If hostname is specified, it must resolve to an IP address for this CMS host that is valid in that partition. (If your site uses multiple Network Interface Cards (NICs), you may specify additional hostnames, separated by a space.)</td>
</tr>
<tr>
<td></td>
<td>For partition name, enter the partition name of the OMEGAMON XE components that need to communicate with this CMS. When you are finished, click OK.</td>
</tr>
<tr>
<td></td>
<td>If you make a mistake and wish to remove your entry, highlight the entry, then click Remove. If you wish to make a change in the entry, highlight the entry, then click Edit. The Edit Partition File dialog re-displays and you can make changes. When you are finished, click OK.</td>
</tr>
<tr>
<td></td>
<td>If necessary, you can edit the file directly by clicking Edit File. The partition file is displayed. Candle recommends that you do not directly edit this file unless instructed to do so by Candle support personnel.</td>
</tr>
<tr>
<td></td>
<td>Click OK to exit the Hub CMS Configuration dialog and continue.</td>
</tr>
<tr>
<td>Partition Name</td>
<td>(Required only by sites with firewalls that use address translation.) The name of the partition that this CMS resides in (up to 32 alphanumeric characters).</td>
</tr>
</tbody>
</table>
13. Click **OK**.

The Select Product to Seed CMS dialog is displayed.

The components you chose to install are automatically selected on this dialog.

Seeding adds product-provided situations, templates, and other sample data to the CMS’s Enterprise Information Base (EIB) tables. This can take up to 5 minutes, depending on the number of products you installed.

**Note:** The Generic Configuration is to seed the cf component of the CMS and is required for OMEGAMON XE for WebSphere MQ Configuration.

Click **OK** to begin the seeding process.

14. When seeding is complete, read the Information dialog or dialogs that display next. You are about to begin the agent configuration portion of installation. Click **Next**.
15. If you chose a remote type CMS, the Remote CMS Configuration dialog is displayed:

![Remote CMS Configuration Dialog](image)

16. Use the following table to complete the Remote CMS Configuration dialog:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides. You are configuring a remote CMS now. Enter the hostname or IP address of the associated hub CMS that this remote CMS reports to.</td>
</tr>
<tr>
<td>Port number</td>
<td>The TCP/IP listening port for the CMS. You must specify the same port number for the hub CMS, all remote CMSs reporting to it, and a hot-standby CMS, if one is defined.</td>
</tr>
<tr>
<td><strong>SNA Communication Settings: Remote CMS</strong></td>
<td></td>
</tr>
<tr>
<td>Network Name</td>
<td>Your site’s SNA network identifier.</td>
</tr>
<tr>
<td>LU Name</td>
<td>The LU name for this CMS. This LU name corresponds to the Local LU Alias in your SNA communications software.</td>
</tr>
</tbody>
</table>
### Configuring the CMS

**Table 11. Communication Settings for Remote CMS (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU6.2 LOGMODE</td>
<td>The name of the LU6.2 logmode. Candle recommends that you use the default name shown: CANCTDCS.</td>
</tr>
<tr>
<td>TP Name</td>
<td>The Transaction Program name for this CMS.</td>
</tr>
</tbody>
</table>

**IPPIPE Communication**

The information below assumes that you have read “Configuring OMEGAMON XE Across a Firewall” on page 37. If you have not yet reviewed that section, do so now before proceeding. When you are ready, enter the following under IPPIPE Settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Hostname or IP Address | The hostname or IP address of the machine where the primary hub CMS resides.  
You are configuring a remote CMS now. Enter the hostname or IP address of the associated hub CMS that this remote CMS reports to. |
| Port number    | The listening port for the CMS.  
You must specify the same port number for the hub CMS, all remote CMSs reporting to it, and a hot-standby CMS, if one is defined. |
17. Click **OK**.

18. Depending on the Protocol for this CMS selection you made on the previous dialog, one of several seeding prompts displays. For example, if you selected the Protocol “SNA only”, you are prompted:

### Table 11. Communication Settings for Remote CMS  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Partition File   | (Required only by sites with firewalls that use address translation.) The name of a partition text file. Either accept the default (c:\Candle\CMS\kdcpartition.txt) or enter a new name; for example: c:\Candle\CMS\hubpart.txt. To create entries in the partition file, do the following: 1. Click **Modify**. The Edit Partition File dialog is displayed. 2. Click **Add**. The Add Partition dialog is displayed; you are prompted for Hostname and Partition Name.  
  - For Hostname, enter a hostname (or IP address) that uniquely identifies this CMS host in the other partition. If hostname is specified, it must resolve to an IP address for this CMS host that is valid in that partition. (If your site uses multiple NICs, you may specify additional hostnames, separated by a space.)  
  - For partition name, enter the partition name of the OMEGAMON XE components that need to communicate with this CMS. When you are finished, click **OK**.  
If you make a mistake and wish to remove your entry, highlight the entry, then click **Remove**. If you wish to make a change in the entry, highlight the entry, then click **Edit**. The Edit Partition File dialog re-displays and you can make changes. When you are finished, click **OK**.  
If necessary, you can edit the file directly by clicking **Edit File**. The partition file is displayed. Candle recommends that you do not directly edit this file unless instructed to do so by Candle support personnel.  
Click **OK** to exit the Hub CMS Configuration dialog and continue. |
| Partition Name   | (Required only by sites with firewalls that use address translation.) The name of the partition that this CMS resides in (up to 32 alphanumeric characters). |
| Entry Options    | Candle recommends that you retain the default setting. |

101
Start and seed the Remote CMS after the installation is complete.

Afterwards, when you finish the Setup program, you will need to verify that the hub CMS to which this Remote reports is running then use Manage Candle Services to perform the Seed CMS action for the remote.

19. Click **OK** to continue.
Configuring Agent-to-CMS Communication

Complete this step only if you are configuring agents on this machine.

In this step you will configure agent-to-CMS communication. You will:
- Identify the primary CMS that the agents will report to.
- Define the communication method that the agents will use.
- Designate a secondary CMS that the agents will report to if the primary CMS becomes unavailable.

The Configuration Defaults for Connecting to a CMS dialog opens:

1. Do one of the following:
   - If the agent will access the CMS through a firewall, check “Connection must pass through firewall”.
     - The IPPIPE protocol is automatically selected for Protocol 1. You must use IPPIPE if the agent resides outside a firewall. The remaining two Protocol fields are disabled; only IPPIPE may be used.
     - If your site uses NAT between the agent and the CMS, check “Address Translation Used”.

   [Image of Configuration Defaults for Connecting to a CMS dialog]
Configuring Agent-to-CMS Communication

- If the agent will not communicate with the CMS across a firewall, select up to three communications protocols (Protocol 1, Protocol 2, and Protocol 3):
  - TCP/IP
  - SNA
  - IPPIPE

  The agent will use Protocol 1, if it is available. If not, it will use Protocol 2. If that is not available, it will use Protocol 3.

2. If you wish to specify a secondary CMS, select “Optional: Secondary CMS Connection.”
   1. On the right half of the dialog, select up to three communications protocols (Protocol 1, Protocol 2, and Protocol 3) for the secondary CMS:
      - TCP/IP
      - SNA
      - IPPIPE
   2. Click OK.

   A dialog opens with the following message:

   **Secondary CMS Connection is an advanced feature that can be difficult to configure properly. Candle recommends that you contact our consulting services for assistance to ensure that the feature is implemented correctly.**

   3. Click OK.
3. The second Configuration Defaults for Connecting to a CMS dialog opens:

4. Specify protocols as you did for the primary CMS. Use the following table to complete the second Configuration Defaults for Connecting to a CMS dialog:

Table 12. Second Configuration Defaults for Connecting to a CMS Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you’re configuring TCP/IP communication, enter the following under Configure Primary CMS: IP Settings</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides.</td>
</tr>
<tr>
<td>Port number</td>
<td>The TCP/IP listening port for the agent.</td>
</tr>
<tr>
<td></td>
<td>Candle recommends that you use port number 1918; however, if you must change it, enter the new port number (Candle recommends numbers 1025 to 65535).</td>
</tr>
<tr>
<td>If you’re configuring SNA communication, enter the following under Configure Primary CMS: SNA Settings</td>
<td></td>
</tr>
<tr>
<td>Network Name</td>
<td>Your site’s SNA network identifier.</td>
</tr>
</tbody>
</table>
Table 12. Second Configuration Defaults for Connecting to a CMS Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU Name</td>
<td>The LU name for this agent. This LU name corresponds to the Local LU Alias in your SNA communications software.</td>
</tr>
<tr>
<td>LU6.2 LOGMODE</td>
<td>The name of the LU6.2 logmode. Candle recommends that you use the default name shown: CANCTDCS.</td>
</tr>
<tr>
<td>TP Name</td>
<td>The Transaction Program name for this agent.</td>
</tr>
<tr>
<td>Hostname or IP Address</td>
<td>The hostname or IP address of the machine where the primary hub CMS resides.</td>
</tr>
<tr>
<td>Port number</td>
<td>The listening port for the agent. Candle recommends that you use port number 1918; however, if you must change it, enter the new port number (Candle recommends numbers 1025 to 65535).</td>
</tr>
<tr>
<td>Partition Name</td>
<td>(Required only by sites using address translation.) The name of the partition that this agent resides in (up to 32 alphanumeric characters).</td>
</tr>
<tr>
<td>For Warehouse Proxy Only</td>
<td>If you are configuring Warehouse Proxy, you must also specify a partition file, designating a partition name and hostname. Refer to Table 10, “Communication Settings for this CMS,” on page 95 for more information.</td>
</tr>
<tr>
<td>Entry Options:</td>
<td>Candle recommends that you retain the default setting.</td>
</tr>
</tbody>
</table>

5. Click **OK**.

6. If you selected “Optional: Secondary CMS Connection” in Step 2. on page 104, a third Configuration Defaults for Connecting to a CMS dialog is displayed.

1. Enter the hostname or the IP address of the secondary CMS for TCP/IP or IPPPIPE connections. For SNA, enter Network Name, LU Name, LU 6.2 Logmode, and TP name.

2. Click **OK**.
Completing Installation

In this step you will complete the installation.

The InstallShield Wizard Complete dialog is displayed.

1. If you want to view the readme file, make sure “Display the README file” is selected.

2. If you want to view a report of errors found during installation and the corresponding warnings, make sure “View warnings and errors found during configuration” is selected.

3. Click **Finish**.

   The Manage Candle Services window will open, and if previously selected, the readme file and error report will open.
Configuring the Agents

Complete this step only if you installed agents on this machine.

In this step you will complete the configuration of the agents you installed locally using default configuration data provided with the product.

Never attempt to start an agent until you have completed this default configuration process.

At the Manage Candle Services window,

1. Select (highlight) the agent name.
2. Right-click and select “Configure Using Defaults” from the drop-down menu.

This completes configuration for the following agents:

- OMEGAMON XE for Windows Servers monitoring agent
- OMEGAMON XE for WebSphere MQ Configuration agent

3. For all other agents, turn to the appropriate product-specific instructions below to complete the agent configuration. The complexity of the additional configuration process varies, depending on the agent.
Configuring the Agents

When you have completed the additional configuration procedure in the sections listed below, return to this chapter and continue with the installation in “Installing OMEGAMON DE” on page 110.

AF/Remote ...................................................... 146
BEA WebLogic Server ........................................... 148
Microsoft SQL Server ........................................... 150
DB2 UDB .......................................................... 160
eBA Solutions .................................................... 161
OMEGAMON XE for WebSphere MQ Monitoring ............. 162
OMEGAMON XE for WebSphere Integration Brokers .......... 164
Novell NetWare .................................................. 166
Peregrine ServiceCenter ........................................ 167
R/3 ................................................................. 169
Remedy ARS ...................................................... 178
Tuxedo .............................................................. 180
Universal Agent .................................................. 185
Warehouse Proxy ................................................ 190
WebSphere Application Server ................................ 197
WebSphere InterChange Server ................................ 199
Installing OMEGAMON DE

Complete this step only if you are installing OMEGAMON DE.

1. Insert the OMEGAMON DE CDROM into your CDROM drive. Installation begins automatically. (If the installer does not start, go to CD directory WINDOWS and run setup.exe. If setup.exe initialization fails, you do not have enough disk space to decompress the setup files.)

   The OMEGAMON DE InstallShield Wizard dialog opens.

2. Read the text that welcomes you to the installation, and click Next to continue.

   OMEGAMON DE will be installed.

3. At the screen that appears informing you of the completion of installation, click Finish.
Rebooting and Starting Candle Services

Candle servers and agents run as Windows system services. Use Manage Candle Services to start the Candle services installed on this machine. Some services will start automatically when you reboot the machine, if they are configured for auto-start; however, you may need to start some services manually.

Always start the services in the following order:

1. CMS
2. Agents
3. CandleNet Portal Server
(Always stop the services in the reverse order.)

Follow these steps:

1. Reboot.
2. For each service:
   1. From the Manage Candle Services window, locate the service and be sure it has been configured. Never attempt to start a Candle service which has not been configured.
   2. Select (highlight) the service name.
   3. Right-click and select “Start Service” from the drop-down menu.
   4. Wait for the Status to show “Started”.
   5. Close the Manage Candle Services window.
Starting the CMW

In this step you will start the CMW, if you installed it on this machine. (If you did not install a CMW on this machine, you may wish to start a CMW installed on another machine to verify that agents on this machine are running properly.)

Follow these steps:

1. From the desktop, select “Start > Programs > Candle OMEGAMON XE > Candle Management Workstation”.
   
   The startup and configuration dialog for the CMW is displayed. For example:

   ![CMW Startup Dialog](image)

   2. Select the “CMS” tab.

   3. Identify the CMS you want to connect to as follows:
      - If your site is using TCP/IP or IPPipe for CMW-to-CMS communication:
        A. In the Socket Family Port Numbers block, the port number you specified during the installation is displayed. Click the Add TCP/IP button and enter the host machine name or IP address where your CMS is installed.
        B. In the Socket Families block, click “IP” if your site is using TCP/IP or “IP pipe” if your site is using IPPipe.
Starting the CMW

C. Click **OK**.

D. If the CMW must communicate across a firewall, specify the Partition
   ID (partition name) that the CMW resides in.
   - If your site is using SNA for CMW-to-CMS communication:
     A. Click the **Add SNA** button and enter the following:

     **Table 13. Add SNA Fields**

     | Network Name       | The SNA network ID of the machine where the CMS is installed. |
     |--------------------|-------------------------------------------------------------|
     | LU Name            | The CMS LU name.                                            |
     | LU 6.2 LOGMODE     | The LU6.2 logmode name assigned to the CMS.                 |
     | TP Name            | The Transaction Program name of the CMS that this CMW connects to. |

4. Click **OK**.

5. Select the “Logon” tab.

6. Enter a logon ID. You may enter a password or leave the password field blank.

7. Click the **Add...** button under the Profile field and enter a name for the connection profile (up to 32 characters). The startup parameters currently in effect will be saved in this profile. You may define up to 10 connection profiles.

8. Click **OK** to start the CMW.

For complete information about customizing the CMW, refer to the online help. Also see *Administering OMEGAMON Registered Products: CandleNet Portal*. 
Using KIB_CLEAN=Y, if Necessary

Overview

Migrating a CMS will often be accompanied by a CMS Node ID change for the affected CMS. When a Node ID is changed, the relationship between the node ID name of the CMS and other attached components, such as reporting IRAs, are affected by the name change. The most common problem is that the older (now defunct) node ID name relationships can appear for the new CMS, when managed systems or managed system list displays are used.

To eliminate unwanted entries, a feature has been added to newer CMW clients that can automatically discard unwanted references to the older node ID. This feature is invoked by using an environment variable setting for the CMW session being started. It is called KIB_CLEAN=Y. With this environment variable set, the CMW will proactively clean up the CMS node list table where bad node ID entries may still exist. The invocation of the CMW with the environment variable setting needs to run only once, after a migration with a node ID change has taken place.

Procedure to start the CMW to clean node IDs

To start a CMW session that is to perform the node list cleanup of unwanted node list entries follow the steps below:

1. Start the CMW.
2. When the CMW’s initial dialog appears select the Advanced tab.
3. On this notebook page you will find two edit input fields. The first one is labeled “Variable” and the other is labeled “Value”. Type in KIB_CLEAN

   in the edit area labeled Variable, then the letter Y

   in the edit area labeled Value.
4. At anytime after step 3 is completed, clicking the OK button will start the CMW and apply the node list garbage collection.
Using KIB\_CLEAN=Y, if Necessary

**Note:** Remember to clear out the fields under the Advanced tab the next time the CMW is started as the node list cleanup has already taken place and becomes unnecessary afterward.
To start the CandleNet Portal desktop interface, proceed as follows.

1. From the Windows desktop, select “Start > Programs > Candle OMEGAMON XE > CandleNet Portal”.

2. When the Logon dialog opens, enter your logon ID and click OK to start CandleNet Portal.
   If the CMS is set for “☑ Security: Validate User”, enter the network domain or password assigned to your user ID on the CMS. If this configuration option has not been set, you will neither be required nor be able to use the password when you log on.

**Note:** We recommend a minimum Windows display setting of 1024 by 768 pixels.
Starting CandleNet Portal Browser Mode

In this step you will start the CandleNet Portal interface from your Internet Explorer browser.

The first time you start CandleNet Portal browser mode, support components are installed. Subsequent startups are much faster.

Before beginning, checking if no CLASSPATH has been set
Verify that you have no CLASSPATH environment variable defined on your Windows machine. From the command prompt, type

```
set classpath
```


If you have a CLASSPATH environment variable defined, it is possible but unlikely that previously-specified Java directories or .jar files may be incompatible with the level required by CandleNet Portal and could affect performance.

As a precaution, you can assign the contents of your CLASSPATH environment variable to a new environment variable. This backup copy will be useful if problems develop later.

Starting CandleNet Portal

1. Start Internet Explorer 5.5 or higher.

CandleNet Portal checks the JRE level on your machine.

The first time you access CandleNet Portal from a web browser, support components are installed on your web browser.

2. In the Address field, type the URL for the CandleNet Portal browser client installed on your Web server.

The URL for the Candle Web server is: http://systemname:1920///cnp/client, where systemname is the host name of the machine where the CandleNet Portal Server and browser component are installed.

3. Click the “Download and Install CandleNet Portal” link to proceed.

4. Click OK.

5. Check “Always trust content from Candle Corporation”, then click Yes to proceed.
Support files are copied to your web browser. When installation is complete, a link displays at the top of the screen.

6. Select the “Click here to start using CandleNet Portal” link to proceed.

7. When the Logon dialog opens, enter your logon ID and click OK to start CandleNet Portal.

If the CMS is set for “Security:Validate User”, enter the network domain or password assigned to your user ID on the CMS. If this configuration option has not been set, you will neither be required nor be able to use a password when you log on.

*Note:* We recommend a minimum Windows display setting of 1024 by 768 pixels.

**What To Do Next**

- If you are the CandleNet Portal administrator at your site, refer now to the manual *Administering OMEGAMON Products: CandleNet Portal*, which contains information about additional configuration for CandleNet Portal browser mode.

- If you are a user and want to learn how to use CandleNet Portal, see the online Help or the manual *Using OMEGAMON Products: CandleNet Portal*. 
Configuring the ODBC Data Source, if Necessary

If your Candle product uses the Candle Warehouse Proxy for warehousing historical data and you installed your CandleNet Portal Server on a different machine than the one on which you installed the Warehouse Proxy, complete this step.

This step, which configures the Candle Data Warehouse data source, is the same step as required when you configure the Warehouse Proxy itself. Configure the ODBC data source used by your site’s CandleNet Portal Server to match the one used by your site’s Warehouse Proxy. See “Warehouse Proxy” on page 190.

Ensure that the appropriate ODBC driver is installed on the machine where the CandleNet Portal Server is installed. If it is not installed, consult your database documentation about installing the driver.

Follow these steps:

1. Access Manage Candle Services from the machine on which you installed the CandleNet Portal Server.

2. On the Manage Candle Services main dialog, highlight “CandleNet Portal Server”, right-click and select “Reconfigure”.

3. Your current CandleNet Portal Server configuration settings are displayed on the CandleNet Portal Server Configuration dialogs. Click OK to page through these.

4. Respond Yes to the prompt:

   Would you like to configure a “Candle Data Warehouse’ ODBC data source (uid-> Candle pswd-> Candle) for historical data collection?

   Manage Candle Services launches the Windows ODBC Administrator.

5. Configure the Candle Data Warehouse ODBC data source as follows:

   A. Select the “System DSN” tab and click the Add button. The Create New Data Source dialog is displayedSelect the appropriate driver for the third-party database you have installed to receive data from the Warehouse Proxy.

   **Note:** Candle has tested and supports the Warehouse Proxy on Windows with the following database client software:

   –Microsoft SQL Server (versions 6.7, 7.0)
Configuring the ODBC Data Source, if Necessary

B. Click **Finish**. Remaining configuration steps differ depending on the driver you have selected.

C. Keep the following important notes in mind as you complete the configuration:

– Name the ODBC data source:

**Candle Data Warehouse**

*Note:* Candle Data Warehouse is case-sensitive and must be typed exactly as shown.

– Specify a user name of “candle” (or a login ID of “candle” and a password of “candle”).

*Note:* Microsoft SQL Server users: Do not select “Use Trusted Connection” if it is presented as an option.

6. Review the displayed configuration information and test the data source. Historical data collection will not function without a working ODBC database connection to the Candle Data Warehouse data source.

7. When the tests complete successfully, click **OK** on all dialogs until you close the ODBC Administrator application.

8. Respond **Yes** to the prompt that reads:

    Press Yes to complete the configuration process ...

9. Close Manage Candle Services and read subsequent instructions before starting.
Enabling Security (optional)

This step applies only to the hub CMS if it was or will be configured for “Security:Validate User”, which requires users to enter a password as part of the user ID when logging on to CandleNet Portal or the CMW.

How security works

Initially, the CandleNet Portal Server has only one valid user ID, “sysadmin”. This enables the administrator to log on and create other users.

If you are using the CMW, the first user who connects to a new CMS becomes the default CMW system administrator. After that initial logon, any CMW user who is authorized to add CMW users can do so using the CMW Administration > Users folder.

If you want users to also enter a password, the same user IDs must be added to the user accounts on the network domain or on the host where the CMS is installed.

Enforcing logon validation

1. Create a Windows user ID for each CandleNet Portal or CMW user ID.
   - The Windows user ID must exactly match the CMS user ID.
   - On a Windows hub CMS: Windows user IDs are validated by the Microsoft WIN32 LogonUser API which checks the user ID and password in the following sequence:
     A. With the local machine
     B. With the domain controller if the local machine is part of a domain
     C. With any domain controller that has established a trusted relationship with the local domain
   
   Regardless of where you define the Windows user ID used for logging on to a Windows hub CMS, no Administrator authority is required. The minimum requirement is the user ID must be granted the “Log on locally” user rights policy on the hub CMS machine. Refer to your Windows documentation to learn how to configure security.

2. Once you have configured the CMS with security turned off, log onto the CMW and create at least one valid CMW user ID for this CMS.

3. Reconfigure the CMS to enable security, as follows:
Enabling Security (optional)

1. On the machine where the CMS is installed, “Start > Programs > Candle OMEGAMON XE > Manage Candle Services”.
2. Right-click “Candle Management Server” and select “Reconfigure” from the pop-up menu.
3. In the Candle Management Server Configuration dialog, check “Security: Validate User”, then click OK.
4. Restart the CMS.
Uninstalling Candle Components

If you want to uninstall an OMEGAMON XE component, follow these steps.

Note: This procedure requires that you redo the basic configuration steps that were performed earlier in this chapter.

1. From the desktop select “Start > Settings > Control Panel > Add/Remove Programs”.
2. Select Candle OMEGAMON XE.
3. Click Change/Remove.
   The Candle OMEGAMON XE Setup Maintenance Program welcome dialog opens.
4. To uninstall particular components (but not the entire Candle OMEGAMON XE installation) select Modify.
5. Click Next.
   The Add or Remove Features dialog opens.
6. Click the + sign next to each main feature to expand the tree.
7. Deselect (uncheck) each product or type of support that you want to uninstall.
8. Click Next.
   The Start Copying Files dialog appears. This dialog displays a list of features or types of support that will be uninstalled.
9. Review the list and click Back if you want to go back and change it. If you want to start uninstalling the features or types of support that are listed, click Next.
10. At this point, you will need to redo the configuration (for the features and types of support you are not uninstalling) that was performed earlier. Go to “Initial Configuration Steps” on page 78.
Uninstalling Candle Components
Introduction


The instructions in this chapter assume that you have installed and configured the CMS using the procedure in “Configuring the CMS” on page 94.

The instructions in this chapter also assume that you have a basic understanding of SOAP, XML and XML Namespaces, and the Web Services Description Language (WSDL).

For complete information about customizing the SOAP interface for your site, refer to Administering OMEGAMON Products: CandleNet Portal.

Chapter contents

Defining Hubs ................................................. 126
Adding Users ................................................ 130
Verifying the Configuration ........................... 131
Defining Hubs

In this step you will use the Manage Candle Services dialog to activate the SOAP server and define hubs with which the SOAP server may communicate.

Follow these steps:

1. From the Windows Start button, open the Manage Candle Services dialog as follows: “Programs > Candle OMEGAMON XE > Manage Candle Services”. The Manage Candle Services dialog opens, showing the Candle components you have installed. For example:

   ![Manage Candle Services Dialog]

   - **CandleNet Portal**
   - **CandleNet Portal Server**
   - **DB2 Universal Database Server**
   - **Universal Agent**
   - **DB2 Universal Database Client**
   - **Windows NT Monitoring Agent**
   - **Candle Management Server**

2. Right-click “Candle Management Server”.
3. Select “Advanced” from the pull-down menu.
4. Select “Configure SOAP Server Hubs”.

Defining Hubs

In this step you will use the Manage Candle Services dialog to activate the SOAP server and define hubs with which the SOAP server may communicate.

Follow these steps:

1. From the Windows Start button, open the Manage Candle Services dialog as follows: “Programs > Candle OMEGAMON XE > Manage Candle Services“. The Manage Candle Services dialog opens, showing the Candle components you have installed. For example:

   ![Manage Candle Services Dialog]

   - **CandleNet Portal**
   - **CandleNet Portal Server**
   - **DB2 Universal Database Server**
   - **Universal Agent**
   - **DB2 Universal Database Client**
   - **Windows NT Monitoring Agent**
   - **Candle Management Server**

2. Right-click “Candle Management Server”.
3. Select “Advanced” from the pull-down menu.
4. Select “Configure SOAP Server Hubs”.
Defining Hubs

The SOAP Server Hubs Configuration dialog is displayed:

5. Click **Add Hub**....
   The Hub Specification dialog is displayed:

6. Select the communications protocol from the Protocol drop-down menu.

7. Specify an alias name in the Alias field (For example: “SOAP”).

8. Do one of the following:
   - If you are using TCP/IP or TCP/IP Pipe communications, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP Address</td>
<td>The host name or TCP/IP address of the host machine.</td>
</tr>
</tbody>
</table>
Defining Hubs

If you are using SNA communications, specify the following:

Table 15. SNA Fields in Hub Specification Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>Your site’s SNA network identifier.</td>
</tr>
<tr>
<td>LU Name</td>
<td>The LU name for the CMS. This LU name corresponds to the Local LU Alias in your SNA communications software.</td>
</tr>
<tr>
<td>LU6.2 LOGMODE</td>
<td>The name of the LU6.2 logmode. Default: CANCTDCS.</td>
</tr>
<tr>
<td>TP Name</td>
<td>The Transaction Program name for the CMS.</td>
</tr>
</tbody>
</table>

9. Click **OK**.
Defining Hubs

The server tree is displayed. For example:
Adding Users

In this step you will define users on each hub and specify each user’s access rights (query or update).

Follow these steps:

1. Select the server (click anywhere within the server tree displayed), if necessary.

2. Under Add User Data, enter the user name.
   
   User IDs must be identical to those specified for CMS logon validation. Access is restricted to only that CMS to which a user has access.

   *Note:* If no user IDs are supplied, all users will be given permission to update data.

3. Click the type of user access (“Query” or “Update”).

4. Click **Add User**.
   
   The server tree is updated, showing the user and type of access.

5. To delete a user:
   
   Select (highlight) the user name from the tree and click **Delete Item**.

6. To delete a hub:
   
   Click anywhere within the hub’s tree and click **Clear Tree**.
Verifying the Configuration

In this step you will verify that SOAP has been properly configured by starting the SOAP client and making a request using the command line utility kshsoap.

Follow these steps:

1. Open a DOS window.

2. Change to the c:\candle\cms directory.

3. In the current directory, create a Notepad file named “SOAPREQ.txt” containing the following SOAP request:

   ```xml
   <CT_Get><object>ManagedSystem</object></CT_Get>
   ```

   Or if security has been enabled:

   ```xml
   <CT_Get><userid>logonid</userid><password>password</password><object>ManagedSystem</object></CT_Get>
   ```

4. Create another Notepad file named “URLS.txt” containing URLs that will receive the SOAP request. For example:

   ```
   http://hostname:1920///cms/soap
   ```

5. Enter this command:

   ```
   kshsoap SOAPREQ.txt URLS.txt
   ```

   (SOAPREQ.txt is the name of the file that contains the SOAP request and URLS.txt is the name of the file that contains the URLs.)

   The kshsoap utility processes the SOAPREQ.txt file and displays the output of the SOAP request in the DOS window. The SOAP request is sent to each URL listed in URLS.txt, and the SOAP response from each URL displays in the DOS window.

   For complete information about using the SOAP interface, refer to Administering OMEGAMON Products: CandleNet Portal.
Verifying the Configuration
Advanced CMS Configuration

Introduction

This chapter discusses advanced CMS configuration topics, such as how and when to use the advanced configuration options: Hot Standby, the Candle System Backup and Restore Utility, and unattended installation and configuration.

Chapter contents

Hot Standby Feature (optional)  ...................................................... 134
Candle System Backup and Restore Utility ...................................... 139
Unattended (Silent) Installations ....................................................... 143
CMS Name (seeding error 171) ......................................................... 144
Hot Standby Feature (optional)

Introduction
The Hot Standby feature lets you define a standby hub CMS. If the primary CMS hub should fail, OMEGAMON XE will automatically switch hub functions to the standby hub.

The standby hub must be installed on UNIX, Windows XP Professional Edition, or Windows 2000. OMEGAMON XE automatically reconnects all remote CMSs, agents, and CMWs to the standby hub.

Activation of this feature is only necessary in enterprises that must maintain 24 X 7 uptime.

Setting up Hot Standby
Perform the following tasks to successfully implement the Hot Standby feature.

Task 1: Installing CMS software
Before you can configure one CMS hub to be a hot standby for another CMS hub, install and configure the necessary CMS software on both machines.

Install and configure the CMS software on the second machine exactly as you did on the first, however, each CMS must always have a unique CMS name (the term “mirror CMS” encapsulates this concept). Insure that attributes and catalogs are at the same level on both the primary and alternate CMS hubs before proceeding.

Task 2: Configuring each CMS for Hot Standby
Configure the Hot Standby option on the primary CMS hub, the alternate CMS hub, and on all remote CMSs that reports to the primary CMS hub.

Note: The primary and alternate CMS hubs should be configured to be mirrors of each other.

Perform this task from the Manage Candle Services dialog as follows:
1. Highlight the CMS in the dialog.
2. Right-click and select “Reconfigure” from the menu.
   The Candle Management Server Configuration dialog is displayed.
Task 3: Configuring tables to be replicated, if necessary

Certain Candle applications require you to configure the CMS tables that will be replicated when the Hot Standby is initiated. For these applications, the tables must be selected in advance. None are selected by default. To check, proceed as follows:

1. Use the CMW to log on to the primary CMS.
2. From the Managed Systems - Details View, select the CMS, right-click and select the “Migrate Tables” action.
   The Copy tables to CMS dialog is displayed.
3. Select from the list of eligible tables, the tables to be copied to the backup CMS when the Hot Standby operation is performed.

Task 4: Configuring agents

Configure the Hot Standby option on all agents that connect to the primary CMS hub. Perform this task from the Manage Candle Services dialog as follows:

1. Highlight the agent in the dialog.
2. Right-click and select “Reconfigure” from the menu.
   The Agent Configuration Defaults dialog is displayed.
3. Click **Configure Backup CMS** and fill in the appropriate configuration values for the alternate CMS hub on Windows 2000.

This dialog is shown in “Configuring the CMS” on page 94.
Task 5: Configuring the CMW

1. The Hot Standby tab of the Candle Management Workstation - Startup dialog must be filled in with the names of the primary and hot-standby CMSs.

The Managed System Name is the CMS name you supplied on the first dialog described in “Configuring the CMS” on page 94.

If the Primary and Standby fields of this dialog are left blank, then the Switch Hub action can not be performed.

To have the CMW restart automatically after a takeover and connect to the secondary CMS, check the box at the bottom of the window.

**Note:** The information you supply on this dialog is associated with a logon profile.
2. The CMS tab of the Candle Management Workstation - Startup dialog must be filled in with the information necessary to communicate with both the primary and hot-standby CMS hubs.

![Hot Standby Feature](image)

**Testing Hot Standby**

The control to manually initiate the Hot Standby feature is accessed from the CMW Managed Systems container. After all Hot Standby configuration is implemented, log on to the primary CMS. From the Managed Systems - Detail View, select a CMS, right-click and select the “Switch Hub” action.

*Note:* Both the alternate and the primary CMS hubs must be running.

**How Hot Standby works**

Hot Standby switches remote agents, CMSs, and CMWs to the hot standby in the following instances:

- When there is a failure on the acting primary hub CMS
- When the switch is initiated by a user on a CMW

There is no automatic switch done when the primary comes back up. Hot Standby expects the primary CMS hub and the alternate (hot-standby) CMS
Hot Standby Feature (optional)

hub to be at the same capacity. Internally Hot Standby considers them peers and doesn't distinguish in terms of a primary and a secondary. Rather it handles them as acting-primary and acting-secondary. Both CMS hubs will alternate between being acting-primary and acting-secondary.

By default the algorithm that Hot Standby follows to determine which is the acting-primary CMS hub is to query the two CMSs to determine how long they have been up. The CMS hub that has been up the longest wins. There could be cases where your CMW is connected to a CMS which it thinks is the primary at a given time. This can happen for example when there is a disconnect between the primary and secondary or even during startup. In such cases when the Hot Standby tasks reconnect to their peers they make an independent determination as to who should be the acting-primary and acting-secondary. The algorithm above is followed.
Introduction

The Candle System Backup and Restore Utility is a Candle Windows 2000 tool that backs up your Candle registry entries and can be used to perform two distinct tasks:

- Perform “push” installs. This means the utility provides a convenient way to replicate OMEGAMON XE (version CT350) from an image installed and configured on one machine. For example, a typical use would be to replicate 3 or 4 identical CMW setups.

- Back up your OMEGAMON XE (version CT350) image then select an instance, from among two or more instances of OMEGAMON XE installed in different directories on the same machine, to make it the “active” instance. For example, you could switch between version CT350 and version CT300 of OMEGAMON XE.

Note: This utility does not back up the CandleNet Portal Server database and presentation files. For details, see the CandleNet Portal Migration chapter in “Administering OMEGAMON Products: CandleNet Portal.”

CCC versions supported with this utility

The Candle System Backup and Restore Utility works with only versions CT200 98R2 or above of CCC.

Always use the latest version of the Candle System Backup and Restore Utility, in this case, the one that is installed when you install OMEGAMON XE (version CT350).

Rules for replicating

Adhere to the following rules to successfully replicate a OMEGAMON XE on Windows 2000 image from one machine to another:

- Machine number 2 (and 3, and 4, etc.) must be configured exactly like machine number 1 (the machine on which you create the original image).

- Machines must use the same directory names, such as OMEGAMON XE directory names, Windows system directory names, and default directory names used by various agents.
Candle System Backup and Restore Utility

For example, if the OMEGAMON XE is installed into C:\Candle on machine number 1 then it must be installed into C:\Candle on all machines. (It is always a good idea to use the Candle default names.)

- Install on machine number 1 exactly (and only) the Candle components that you want to replicate.

Other requirements for replicating
You will need a 32-bit zip utility capable of handling long filenames.

Replicating an OMEGAMON XE instance to one or more machines
Once you have installed and configured an image of a CMW (or any OMEGAMON XE (version CT350) image on Windows XP Professional Edition or Windows 2000) that you want to replicate, follow these steps to copy it to another machine:

1. Using Explorer or a similar utility, go to the \INSTALL subdirectory of the directory where you installed the OMEGAMON XE software directory. For example:
   C:\Candle35\INSTALL
2. Run the Kinregbu.exe program.
   The Candle System Backup and Restore Utility dialog displays.
3. Select the “Backup” option and click OK.
   This ensures that your most recent customizations are preserved.
4. On the same machine, go back to the root directory where you downloaded the OMEGAMON XE software. For example:
   C:\Candle35
   Use a 32-bit zip utility to zip up the entire directory. Be sure to include all subdirectories and preserve the directory structure in the zip file you create.
5. Transport the zip file to the new machine. Use the same 32-bit zip utility to unzip the file (preserving the same directory structure).
6. Using Explorer or a similar utility, go to the \INSTALL subdirectory of the directory where you installed the OMEGAMON XE software directory. For example:
   C:\Candle35\INSTALL
7. Run the Kinregbu.exe program.
   The Candle System Backup and Restore Utility dialog displays.
8. Choose the “Restore” option and click **OK**.
9. Reboot the machine. This completes the replication process.

**Running Multiple OMEGAMON XE Releases on a Single Machine**

Candle recommends running only one release of OMEGAMON XE per machine. This is called the “active” instance. However, if you have enough space, you can install an additional OMEGAMON XE into a different directory.

For example, you might already have a CCC (version CT350) running at your site that you wish to retain. If you have the disk space, you can install a OMEGAMON XE (version CT350) into a different directory, instead of upgrading (installing over) your previous version.

*Note*: *Since previous versions of CCC did not support this capability, the sequence of installed versions is very important. Always install the lower version of CCC first.*

When you install a OMEGAMON XE (version CT350) into a new directory on a machine with an older version installed in another directory, the version CT350 installation process backs up the existing registry values and removes them from the registry, then updates the registry with the version CT350 registry values. It also backs up and removes the previous release’s Program folder.

To continue the example of maintaining both an OMEGAMON XE (version CT350) and an older version on the same machine-- after installing and configuring OMEGAMON XE (version CT350), follow these steps to switch back to the previous version.

1. Using Explorer or a similar utility, go to the \INSTALL subdirectory of the directory where the previous release resides. For example:
   ```
   C:\Candle\INSTALL
   ```
2. Run the Kinregbu.exe program.
   The Candle System Backup and Restore Utility dialog displays.
3. Select the “Switch” option and click **OK**.
Candle System Backup and Restore Utility

The Utility backs up the registry values of the active OMEGAMON XE (in this case, OMEGAMON XE (version CT350) and removes them from the registry. The Program folder for version CT350 is also backed up and removed.

The Utility updates the registry with the previous release’s registry values and activates the previous release.

4. Reboot the machine. This completes the restore process.
Unattended (Silent) Installations

Included on the product CD, in the WINDOWS subdirectory, is a file called SILENT.TXT. This is a driver file for silent (unattended) installation and configuration of OMEGAMON XE (version CT350) products that run on Windows XP Professional Edition or Windows 2000.

Complete instructions for using this file are contained within it. SILENT.TXT is provided for sites that want to distribute OMEGAMON XE using a system management tool, such as Microsoft's SMS or Tivoli.

After any silent installation is completed, additional configuration may be required. See the configuration instructions in SILENT.TXT for more detail.
CMS Name (seeding error 171)

This error message generally occurs when a CMS is not up and running or perhaps the wrong "CMS Name" was keyed in—often users enter the host name instead of the CMS name.

Where to find the CMS name

On distributed systems, the Hub CMS Name is assigned to CMS_NODEID.

If the hub CMS executes on Windows, you can view this value using “Manage Candle Services > right-click the CMS > Browse Settings”. Also visible in the KBBENV file in the CMS directory.

If the hub CMS executes on UNIX, this value is visible in the KBBENV file located in the $candlehome/tables/<CMS_Name> subdirectory.

If the hub CMS executes on OS/390 or z/OS, the CMS name is specified during RTE configuration. If you view the RTE values, you will see the CMS name which by default is set to the RTENAME.

On OS/390 and z/OS, CMS_NODEID is defined in the KDSENV member of RKANPAR.
Additional Agent Configuration

Introduction

This chapter contains advanced configuration steps required for certain monitoring agents and alert managers. Do not attempt to start the monitoring agent or alert manager before completing the steps in this chapter.

Chapter contents

AF/Remote .......................................................... 146
BEA WebLogic Server ........................................... 148
Microsoft SQL Server ............................................ 150
Oracle ................................................................. 154
Sybase ................................................................. 158
DB2 UDB ............................................................... 160
eBA Solutions ......................................................... 161
OMEGAMON XE for WebSphere MQ Monitoring ............ 162
OMEGAMON XE for WebSphere Integration Brokers ......... 164
Novell NetWare ....................................................... 166
Peregrine ServiceCenter ........................................... 167
R/3 ............................................................... 169
Remedy ARS ......................................................... 178
Tuxedo ................................................................. 180
Universal Agent ...................................................... 185
Warehouse Proxy .................................................... 190
WebSphere Application Server ................................... 197
WebSphere InterChange Server .................................. 199
Windows Management Web Service ........................... 204
The Alert Manager for AF/REMOTE on Windows has its own manager. You will use this application to configure and monitor the status of individual AF/REMOTE agents.

To access the AF/REMOTE Alert Manager from the Manage Candle Services window:

1. Highlight “AF/REMOTE Adapter”, right-click then select “Configure Using Defaults”.

2. Click Yes at following prompt:
   Continue with detail configuration of AF/REMOTE Alert Adapter?

3. If necessary, click Yes on subsequent dialogs until the AF/REMOTE Alert Adapter Manager displays.

Use the AF/REMOTE Alert Adapter Manager to configure:
- One AF/REMOTE Alert Adapter for each AF/REMOTE session you want to monitor.
Additional Agent Configuration

- One AF/REMOTE Alert Emitter per AF/REMOTE REXX Management component.

Online Help is included for each dialog of the AF/REMOTE Alert Adapter Manager.

See the Alert Adapter for AF/REMOTE Configuration and Customization Guide for complete configuration information.

Troubleshooting

When no AF/Remote monitoring data appears
If no AF/Remote monitoring data appears after starting the CandleNet Portal or CMW, check to see that support for Alert Adapter for AF/Remote was selected when you selected the products for installation.

1. Open the Manage Candle Services window and check the list of installed products for Alert Adapter for AF/Remote.

2. If Alert Adapter for AF/Remote has not been selected, start another installation process, proceeding without changing or removing any of the items that were previously installed.

3. At Step 5. on page 76, leave selected “Alert Adapter for AF/Remote”.

4. Proceed through the rest of the installation process without changing or removing any of the items that were previously installed.
The JMX collector needs information about the location and configuration of the WebLogic server instance it will be monitoring. It also needs to know on what port the BEA WebLogic Server agent is listening for it.

**Configuring the collector**

To configure the collector:

1. In Manage Candle Services, right-click the WebLogic JMX collector and select Configure Using Defaults.
   The Configure OMEGAMON XE for BEA WebLogic Server dialog appears.

2. In the Configuration Parameters for KWLAgent area, enter the listening port for the agent if necessary. By default, this is 17500.
   If you do not have this information, contact your CandleNet Command Center administrator.

3. In the Configuration Parameters for WebLogic area:
   - For Host, type the name of the host on which the monitored server instance is installed. By default, this is `localhost`.
   - For Port, type the number of the admin port for the WebLogic server. By default, this is 7001.
   - For User ID, type a valid user ID for this server.
   - For Password, type the password associated with the user ID.
   - For Display name, type the name you want used as the node name or managed system name for this WebLogic server in the CandleNet Portal Navigation tree.
     If you do not specify a name, this parameter takes the value `WebLogic_hostname-portnumber` (for example, Server1-7001).
   - For WebLogic JAR location, type the path to the directory in which the `weblogic.jar` file for the appropriate version resides (for example, `d:\weblogic`) or use the Browse button to browse to the directory.
For Java jvm.dll path, use the Browse button to select the directory in which the .dll for the appropriate JRE for the version of BEA WebLogic Server on this host resides (1.3.x for WebLogic 7 and 1.4.x for WebLogic 8).

For JRE v. 1.3.x, use the jvm.dll in the classic directory. For v. 1.4.x, use the jvm.dll in the client directory.

If you do not have the required information, contact your BEA WebLogic Server administrator.

4. Click **OK** to configure the collector with the provided values.

5. Return to “Rebooting and Starting Candle Services” on page 108 to complete the installation.
Microsoft SQL Server

This section contains instructions for completing the configuration of the Microsoft SQL Server database monitoring agent.

Follow these steps:

1. From Manage Candle Services, highlight the agent, right-click and select “Configure Using Defaults”.
   The Configure Database Agents dialog displays the discovered database servers in the Database Servers Available list.

2. From the Database Servers Available list, select the database servers you want to monitor and move them to the Servers to Monitor list.
   If a database server you want to monitor is not listed, click New to manually add an undiscovered database server to the Database Servers Available list.
   
   **Note:** When removing an entry from the Servers to Monitor list, be aware that entries originally discovered by the configuration program can be moved back to the Database Servers Available list; entries that were manually added using the New button are discarded.

3. If you want to edit an entry in the Servers to Monitor list, highlight the entry and click Edit. The Database Server Properties dialog opens.

4. The Database Server Properties dialog prompts you for the necessary database server configuration information.
   This dialog displays known configuration information about the database server and allows you to define login and password information. The default user ID is “candle”. The default password is “candle”.
   Supply the necessary information then click OK.
   You are returned to the Configure Database Agents dialog.

5. Once all database servers to be configured are listed under Servers to Monitor, click OK to perform the configuration and return to the Manage Candle Services window.

**Granting select permissions for SQL Server**

The database administrator performs the following procedure to grant the Microsoft SQL Server database agent access to all views that OMEGAMON
XE requires. Now you will create a user ID for Microsoft SQL Server and grant permission to the new user ID:

1. Start > Programs > Microsoft SQL Server > Enterprise Manager to open the SQL Server Enterprise Manager window.

2. In the Tree tab, select “Logins” from the Security folder (“Console Root > Microsoft SQL Servers > SQL Server Group > WindowsName > Security > Logins”).

3. Right-click “Logins” and select “New Login” from the pop-up menu.

4. In the General tab, type the name as `candle`

5. In the Authentication area, choose the radio button for “SQL Server Authentication” and enter a password.

6. Click the Database Access tab, then give permission to every database you have now.
   This is done by checking the boxes under Specify which databases can be accessed by this login.

7. Click **OK**.

8. In the Confirm Password dialog that opens, retype the password you entered for the user ID and click **OK**.
   The SQL Server Enterprise Manager will show the new user ID in the Logins list.

**Configuring the Microsoft SQL Server security mode**

For the Candle user ID “candle” to work properly, make the following configuration changes to Microsoft SQL Server:

1. Microsoft SQL Server must be configured to run under either “mixed” security mode or Windows 2000 integrated security mode.

2. The Candle user ID “candle” must be assigned to either the “SQLAdmin” or “Administrators” Windows user group so that it is recognized as having “sa” authority by Microsoft SQL Server.

   **Note:** *After you have configured the correct security mode in Microsoft SQL Server and assigned the Candle user ID to the appropriate user group, recycle Microsoft SQL Server for the change to take effect.*
Microsoft SQL Server

The first time Microsoft SQL Server runs under integrated or mixed mode, Microsoft SQL Server will automatically grant “sa” authority to those users who are assigned the “Administrators” or “SQLAdmin” role under Windows. Refer to Microsoft’s SQL Server *Administrator Companion* online document for configuration information.

**Startup for the agent for Microsoft SQL Server**

Configure the agent for Microsoft SQL Server’s Collector so that it can log on to Microsoft SQL Server using the Candle user ID you defined previously. Proceed as follows:

1. From the Windows Control Panel, open the Services container.
2. Locate and highlight the Candle “Collector” service for this instance of the monitoring agent (this component is automatically created at the time you configure the monitoring agent for Microsoft SQL Server) and click **Startup**.

3. A Service dialog (similar to the following) is displayed.

![Service dialog](image)

Select the Log On As: option “This Account”, and supply the Candle user ID and password that you previously created for logging on to the Microsoft SQL Server database.
4. Click **OK** to save and exit this dialog, then close the Windows Control Panel. After completing this procedure, the monitoring agent for Microsoft SQL Server can be successfully started.

5. When you have completed agent configuration, return to “Installing OMEGAMON DE” on page 110.
Oracle

This section contains instructions for completing the configuration of the Oracle database monitoring agent.

Follow these steps:

1. From the Manage Candle Services window, highlight the agent, right-click and select “Configure Using Defaults”. The Configure Database Agents dialog displays.

The configuration program displays available database servers it discovers in the Database Servers Available list.

2. Select the database servers you want to monitor and move them to the Servers to Monitor list.
   If a database server you want to monitor is not listed, click **New** to manually add an undiscovered database server to the Database Servers Available list.

   **Note:** *When removing an entry from the Servers to Monitor list, be aware that entries originally discovered by the configuration program can be moved back to the Database Servers Available list; entries that were manually added using the New button are discarded.*

3. If you want to edit an entry in the Servers to Monitor list, highlight the entry and click **Edit**. The Database Server Properties dialog displays.
4. The Database Server Properties dialog prompts you for the necessary database server configuration information.

![Database Server Properties dialog](image)

This dialog displays known configuration information about the database server and allows you to define login and password information. The default user ID is “candle”. The default password is “candle”.

Supply the necessary information then click **OK**.

You are returned to the Configure Database Agents dialog.

5. Once all database servers to be configured are listed under Servers to Monitor, click **OK** to perform the configuration and return to the Manage Candle Services window.

**Installing Oracle V$Dynamic performance tables**

If you have not already done so, create the public synonyms and views of the Oracle V$Dynamic performance tables that the monitoring agent for Oracle requires to report performance data. The catalog.sql script you will need is in your Oracle_HOME\rdbms\admin directory.
Oracle

Granting select permissions for Oracle

The database administrator performs the following procedure to grant the monitoring agent for Oracle access to all views that OMEGAMON XE requires under the Oracle release listed:

Table 16. Parameters for Oracle Monitoring Agent Access to Views

<table>
<thead>
<tr>
<th>Oracle v7.1.4</th>
<th>The Oracle logon must be SYS, which has all required authority.</th>
</tr>
</thead>
</table>
| Oracle v7.1.6 | The database administrator must issue the following SQL statement, where “oralogin” is the database connect login used by the monitoring agent for Oracle. The default login is “candle”.
grant select any table to “oralogin”.
| Oracle v7.2 and higher | The database administrator must run the Candle-provided korgrant.sql script as described in the following procedure. |

Use this procedure to run the korgrant.sql script for Oracle 7.2 and higher.

1. Open a command prompt, and change the current directory to the directory where korgrant.sql resides. This script is in the directory where you downloaded the agent. The default is:
\candle\cma

2. Enter the following MSDOS commands to set environment variables for Oracle SQLPlus or an alternate tool you use to issue SQL statements:

```plaintext
SET ORACLE_SID=sid
SET ORACLE_HOME=home
```

where:

- sid is the Oracle instance. Oracle instances are case-sensitive.
- home is the home directory of the Oracle instance.

3. Start Oracle SQLPlus or an alternate tool you use to issue SQL statements.

4. Log into Oracle as a user that has Oracle DBA privileges.

5. Add your Oracle database connect login as Oracle database user (in this example, the user ID is “candle”). The command is:

```
create user candle identified by candle
```

6. Log out of Oracle SQLPlus (or the alternate tool you use) and return to the MSDOS prompt. Change the current directory to the directory where korgrant.sql resides.
7. Start Oracle SQLPlus or an alternate tool you use to issue SQL statements.

8. Grant select permissions by typing:

```
@korgrant oralogin
```

where `oralogin` is your Oracle database connect login. The default login is “candle”. The output is logged to the korgrant.log file in the Oracle home directory. If all went well, this log records the tables to which the monitoring agent for Oracle has been granted select permissions.

9. When you are sure that these permissions have been successfully granted, the monitoring agent for Oracle can be successfully started.

10. When you have completed the agent configuration, return to “Installing OMEGAMON DE” on page 110.
Sybase

This section contains instructions for completing the configuration of the Sybase database monitoring agent.

Follow these steps:

1. From the Manage Candle Services window, highlight the agent, right-click and select “Configure Using Defaults”. The Configure Database Agents dialog displays.
   This configuration program displays available database servers it discovers in the Database Servers Available list.

2. Select, from the Database Servers Available list, the database servers you want to monitor and move them to the Servers to Monitor list.
   If a database server you want to monitor is not listed, click New to manually add an undiscovered database server to the Database Servers Available list.
   
   **Note:** When removing an entry from the Servers to Monitor list, be aware that entries originally discovered by the configuration program can be moved back to the Database Servers Available list; entries that were manually added using the New button are discarded.

3. If you want to edit an entry in the Servers to Monitor list, highlight the entry and click Edit. The Database Server Properties dialog displays.
   The Database Server Properties dialog prompts you for the necessary database server configuration information.
   This dialog displays known configuration information about the database server and allows you to define login and password information. The default user ID is “candle”. The default password is “candle”.

4. Supply the necessary information then click **OK**.
   You are returned to the Configure Database Agents dialog.

5. Once all database servers to be configured are listed under Servers to Monitor, click **OK** to perform the configuration and return to the Manage Candle Services window.

**Granting select permissions for Sybase**

The database administrator performs the following procedure to grant the Sybase monitoring agent access to all views that OMEGAMON XE requires.
1. Open a Windows command prompt.

2. Enter the following command, where “candle” is your Candle home directory:
   
   ```
   cd \candle\cma
   ```

3. Use the ISQL command to log into the Sybase server as user “sa”:

4. Enter the following command to configure the Candle user. Note that this command is case-sensitive.
   
   ```
   sp_addlogin candle, password
   ```
   
   where `candle` is the Candle user ID and `password` is the password assigned to the Candle user. By default, the Candle user ID is “candle”.

5. Enter the following command to add the Candle user to the master database. Note that the command is case-sensitive.
   
   ```
   sp_adduser candle
   ```
   
   where `candle` is the Candle user ID.

   If the Candle user is not “candle”, edit the koygrant.sql file and change “candle” to the Candle user ID.

6. Enter the following command. Note that the command is case-sensitive:
   
   ```
   ISQL -U sa -P password -S servername -i koygrant
   ```
   
   where:

   - `password` is the password for user “sa”.
   - `servername` is the database server name.

   The command runs the koygrant.sql script to change the grant permission tables in the master database.

7. When you have completed configuration of agents you are installing at this time, return to “Installing OMEGAMON DE” on page 110.
Overview

DB2 UDB requires a user ID that has DB2 SysAdmin, SysCtrl, or SysMaint authority to start the agent. DB2 UDB does not require advanced configuration.

You can run multiple copies of the DB2 UDB client agent by specifying different database instance names.

You must have installed DB2 UDB and rebooted before configuring the agent.

Configuring the DB2 UDB agent

Follow these steps from Manage Candle Services:

1. Right-click DB2 Universal Database Server and select “Configure Using Defaults”.

2. Right-click DB2 Universal Database Client Template and select “Configure Using Defaults”.

3. When you are prompted for the instance name, enter it.

   If this is a new DB2 UDB installation, the instance is named DB2. You can see a list of the instance names in your DB2 UDB installation in the DB2 Control Center: “Start > Programs > IBM DB2 > General Administration Tools > Control Center” (or enter

   \texttt{SET DB2}

   at the command prompt).

   A new DB2 Universal Database Client entry is added to the list with the instance name in the Task/Subsystem column.

4. Right-click the new DB2 Universal Database Client instance and select “Configure Using Defaults”.


eBA Solutions

Overview

The eBA Solutions monitoring agent requires the same JRE that is packaged with ETEWatch. Since the agent and the ETEWatch Manager Server are installed on the same machine, the agent reads from the Windows registry to obtain the JRE information it needs.

The eBA Solutions agent also requires either JDBC or ODBC connectivity to the ETEWatch database, so install and configure a JDBC or ODBC driver on the machine on which you install the monitoring agent. Contact your database vendor for the appropriate JDBC or ODBC driver. If you are using an ODBC driver, create a System DSN for access to the database.

You will see the following prompt when you configure the ETEWatch agent:

![Prompt for configuring ETEWatch agent](image)

Procedure

Proceed as follows:

- If you are using the JDBC driver, enter the JDBC driver path or class name, for example:
  
  c:\oracle\jdbc\classes111.zip

  and click OK.

- If you are using an ODBC driver, leave this field blank and click OK.

This completes the configuration.
OMEGAMON XE for WebSphere MQ Monitoring

This section contains instructions for completing configuration of the OMEGAMON XE for WebSphere MQ Monitoring agent.

The OMEGAMON XE for WebSphere MQ Monitoring agent monitors a single WebSphere MQ queue manager. If you want to monitor multiple queue managers, create one instance of the OMEGAMON XE for WebSphere MQ Monitoring agent for each queue manager.

Default monitoring options

Candle provides a default set of monitoring options for the OMEGAMON XE for WebSphere MQ Monitoring agent. These are stored in the agent’s .cfg file which is read at agent startup time.

Default objects must exist

Before starting the OMEGAMON XE for WebSphere MQ Monitoring agent, WebSphere MQ default objects such as SYSTEM.DEFAULT.MODEL.QUEUE, must exist. If they do not exist in your environment, create them before starting the agent.

Initial configuration procedure

1. From the Manage Candle Services window, select an instance of the WebSphere MQ Monitoring Agent then right-click and select “Configure Using Defaults”.

2. You are prompted to edit the agent’s .cfg. file. (The Primary agent’s file is named mq.cfg.)
   - If your site has a default queue manager specified, the agent’s default .cfg file will operate successfully with no modifications. Click No. The agent will be configured using defaults. If necessary, you can customize this file later after you have verified successful installation.
   - If your site does not have a default queue manager specified, or if you are configuring this agent to monitor a queue manager other than the default, click Yes. A Notepad session opens. Supply the WebSphere MQ queue manager name in the MANAGER NAME() and MGRNAME() parameters of the .cfg file, then save and close the Notepad session. Click Yes at the next prompt to continue.
You are returned to the Manage Candle Services window. This completes initial configuration, the agent is ready to start.

**Customizing monitoring options**

If necessary, you can change the monitoring options for the OMEGAMON XE for WebSphere MQ Monitoring agent at any time by editing the agent’s .cfg file. For example, if you wish to collect historical monitoring data, you must set HISTORY(YES) in the agent’s .cfg file.

- For information on historical data collection, see the *Historical Data Collection Guide for OMEGAMON XE and CandleNet Command Center*.
- For information on the various monitoring options for the OMEGAMON XE for WebSphere MQ Monitoring agent and the commands to enable them, see the *OMEGAMON XE for WebSphere MQ Monitoring User’s Guide*.

To access a .cfg file for a configured OMEGAMON XE for WebSphere MQ Monitoring agent:

1. From the Manage Candle Services main dialog, select the instance of the WebSphere MQ Monitoring Agent then right-click and select “Reconfigure”.

**Creating an instance of the agent**

To create an additional instance of the OMEGAMON XE for WebSphere MQ Monitoring agent:

1. From the Manage Candle Services main dialog, select “WebSphere MQ Monitoring Agent” then right-click and select “Create Instance”.
2. When prompted, supply a name for the new instance (no blanks are allowed) then click **OK**.
3. The name you supply appears in the Task/Subsystem column of the Manage Candle Services window. Proceed with “Initial configuration procedure” on page 162.
OMEGAMON XE for WebSphere Integration Brokers

This section contains instructions for completing configuration of the OMEGAMON XE for WebSphere Integration Brokers agent.

To customize the agent configuration data for your site, consult IBM's documentation for its broker products and Candle's OMEGAMON XE for WebSphere Integration Brokers User's Guide for more information.

Reconfiguring after an upgrade installation

If it is being upgraded from a previous version, the OMEGAMON XE for WebSphere Integration Brokers agent must be reconfigured after the upgrade installation. This is because there are new environmental parameters that must be set. If this is not done, the agent will not be able to find the message file to be able to log messages, and the agent will abnormally terminate soon after starting it.

1. In the Manage Candle Services window, right click the monitoring agent and select "Reconfigure".
   No values need to be changed, but the step must be performed to reconfigure the agent.

Authorizing the agent

In this section you will set user ID authorization required for running the OMEGAMON XE for WebSphere Integration Brokers agent. Windows user IDs must be members of groups “mqm,” “mqbrkrs,” and “Administrators” to start and stop the OMEGAMON XE for WebSphere Integration Brokers agent and receive broker data.

Follow these steps:

1. Log on to Windows as a System Administrator, if necessary.

2. Create a user ID for the agent, if necessary. The agent’s user ID must:
   - Have authority to subscribe to broker event publications.
   - Belong to groups “mqm” (this must be the primary group), “mqbrkrs,” and “Administrators”.

3. From the Start button, select “Programs > Administrative Tools > User Manager“.
4. Click the user ID in the upper window. The User Properties dialog opens.

5. Click the Groups button (bottom left corner). The Group Memberships dialog opens.

6. Check the “Member of” list and add groups “mqm,” “mqbrkrs,” and “Administrators.”

7. Exit the dialogs and close the User Manager window.

8. In Manage Candle Services, right-click the agent and select “Change Startup”.

9. In the “log on as” section, change from using the system account to specify the user ID and password for the account you created above.

If the agent runs as a Windows Service using the system account, it cannot subscribe successfully to broker event publications. When the agent does not receive broker event publications, data in OMEGAMON XE for WebSphere Integration Brokers reports will be missing or inaccurate. (Specifically, the Broker Events workspace will display no data.)

Additionally, depending on your site's ACL entries, you may be required to authorize the agent to receive broker event publications in the Control Center or Message Brokers Toolkit. You do not have to perform this step if your site uses the IBM defaults. However, if ACL entries in the Topics tab of the Control Center or Message Brokers Toolkit have been modified such that subscribe access to topics beginning with $SYS/Broker has been restricted, this step is required.

An ACL entry for topics beginning with $SYS/Broker must be added to set “Subscribe” access to “Allow” for the user ID of the agent. The principal for the ACL entry should give the user ID of the agent, or it can give a group to which the agent's user ID belongs, such as “mqbrkrs.” The ACL entry must be deployed to all brokers to be monitored by the OMEGAMON XE for WebSphere Integration Brokers agent. This change will allow the agent to receive the broker event publications.
Novell NetWare

This section describes tasks that must be completed before the monitoring agent for Novell NetWare can operate successfully.

Installing required maintenance on Novell NetWare (version 5.0)

If you plan to monitor a Novell NetWare (version 5.0) system, make sure you have installed the latest Novell maintenance before proceeding.

At the time of this writing, required maintenance can be ordered from Novell by referencing:

Novell internal entry DEFECT000214526

**Note:** Install the required Novell (version 5.0) maintenance before starting the monitoring agent for Novell NetWare or the Novell NetWare server abends with a message that the HOSTMIB.NLM is failing. After installing and loading the updated HOSTMIB.NLM, verify that the correct HOSTMIB.NLM is loaded. You can do this by typing MODULES HOSTMIB.NLM at the server console prompt.

Special considerations for the monitoring agent for Novell NetWare

**Discovery behavior at startup**

The monitoring agent for Novell NetWare automatically discovers all NetWare servers in the same subnet shortly after the agent comes online. This is the default discovery behavior of the agent.

**Customizing discovery behavior**

If your enterprise utilizes a wide area network and requires one monitoring agent for Novell NetWare to discover NetWare servers on several subnets, the discovery behavior of the agent can be customized to do so. This customization is done from the CMW. For more information, see the OMEGAMON XE for NetWare User’s Guide included with this release.
Peregrine ServiceCenter

Use the following procedure to configure the Peregrine ServiceCenter Alert Manager:

1. When configuring this agent, you must first respond to the following prompt:

   **WHAT IS THE HOST NAME WHERE THE PEREGRINE SERVER IS RUNNING?**

   Enter the host name or address where the Peregrine server is running. Then select either **OK** to continue or **Cancel** to abort the configuration.

2. Next prompt:

   **WHAT IS THE PORT NUMBER OF THE PEREGRINE SERVER?**

   Enter the port number used by the Peregrine server. Then select either **OK** to continue or **Cancel** to abort the configuration.
Next prompt:

![Configuring Alert Adaptor for Peregrine ServiceCenter]

4. A Candle program monitors the Peregrine log for customer-defined situations and communicates them to the agent via the port number you specify here. Enter the port number to be used, in the range of 1025 to 65535.

5. Then select either **OK** to finish configuring the agent or **Cancel** to abort the configuration.
This section describes how to configure the components of your system to monitor the R/3 multilayered client and server architecture.

The monitoring agent for R/3 can be installed either locally, on the R/3 server, or remotely on any Windows XP Professional Edition or Windows 2000 host in your network that meets the agent’s requirements. The monitoring agent uses a TCP/IP connection to communicate with the R/3 System when making Remote Function Calls.

Ensuring the LIBRFC32.dll File is on your workstation

The monitoring agent for R/3 requires the file librfc32.dll to be installed on the Windows workstation before the agent can be started.

Note: Determine if the SAPGUI is installed on the workstation where you will be running the agent.

If the SAPGUI is installed then librfc32.dll is already installed and you can proceed to: “Password encryption (optional)” on page 170.

If the SAPGUI is not installed then perform the following steps to install the RFC files from the SAP Presentation CD.

1. Create a directory on your Windows workstation for proprietary R/3 software modules.

2. Open a Windows command prompt, and move to the directory you created in step 1.

3. Copy the files rfc.car and car.exe from the directory \sdk\nt\i386 on the R/3 Presentation CD to the directory you created in step 1.

Note: The rfc.car file is in a proprietary SAP compressed format that you uncompress by using the car.exe utility.

4. In the command prompt you opened in step 2, run the car.exe utility to extract the RFC files:

   CAR -x -f RFC.CAR

The “car” command extracts the RFC files from the rfc.car file. Note that this process creates the file librfc32.dll in the directory rfcsdk\lib under the directory you created in step 1.
**Note:** If you need help running car.exe, use the following command to obtain more information:

```
CAR
```

5. Move the file librfc32.dll that you extracted in the preceding step to the directory where you downloaded the agent. The default is:

```
\Candle\Cma
```

6. Delete file rfc.car.

**Password encryption (optional)**

The password used by the monitoring agent for R/3 when it logs onto the R/3 system can be plain text or you can optionally encrypt the password and store it to a file. This section explains how to encrypt the password.

If you choose not to encrypt the password, you can proceed to: “Installing remote function modules into R/3” on page 172.

**Using the KSAPWD.BAT file to encrypt passwords**

The batch file KSAPWD.BAT lets you encrypt the password used by the monitoring agent for R/3 to log on to the R/3 system.

The KSAPWD.BAT file is simply a batch file that calls the R/3 password utility KSAR3PWD.EXE with the requested parameters on Windows.

**Parameters**

All parameters for this utility have the format “Keyword(value)”. The complete set of parameters needs to be surrounded in double quotes. You can separate each parameter from the next parameter by using one or more commas, one or more spaces, or not separate them at all. A keyword can be specified in full, but only the first character is required. Any number of characters from one character to the full length of the keyword is acceptable. Mixed case letters are also acceptable.

The table that follows lists the parameters used by KSAR3PWD.EXE.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD(pppppp)</td>
<td>Encrypt the password “pppppp”.</td>
</tr>
</tbody>
</table>
Example of encrypting the R/3 login password

If you decide to use encryption, use the following procedure to encrypt the password used by the monitoring agent for R/3 when it logs onto the R/3 system.

1. Open a Windows command prompt.
2. Change the current directory to the directory where you downloaded the agent. The default is:
   \Candle\Cma
3. Here are two examples.
   - To cause the password “candle” to be encrypted and written to the default file name, type the following and press Enter:
     
     KSAPWD.BAT PASSWORD(candle)
     
     The encrypted password is written to the KSA.PWD file in the current directory.
   - To cause the password “other” to be encrypted and written to a file named FRED, type the following and press Enter:
     
     KSAPWD.BAT “PASSWORD(other) OUTPUT(FRED)”
     
     The encrypted password is written to the FRED file in the current directory.
4. Note the name of the file you create. You will supply this name on the R/3 Agent Configuration dialog in the Password File field.

Table 17. Parameters for KSAR3PWD.EXE (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUTPUT(ffffff)</td>
<td>Write the encrypted password to file “ffffff”. The default file name is KSA.PWD in the current directory.</td>
</tr>
<tr>
<td></td>
<td>A value of STDOUT may be specified for “ffffff” to cause the encrypted password to be displayed to standard output instead of being written to a file.</td>
</tr>
</tbody>
</table>
Installing remote function modules into R/3

Use the following procedure to install the remote function modules into the R/3 system.

**Note:** This procedure installs skeleton remote function module code. The actual code is installed by the monitoring agent for R/3 when it starts up. The installed code will not be visible within R/3 and may not be modified or generated.

1. Open a Windows command prompt.
2. Change the current directory to the directory where you downloaded the agent. The default is:
   
   \Candle\Cma

3. Copy file RSAV300.can to the Transport System data directory \
   \usr\sap\trans\data. For example:
   
   copy RSAV300.CAN \usr\sap\trans\data

4. Copy file KSAV300.can to the Transport System cofiles directory \
   \usr\sap\trans\cofiles. For example:
   
   copy KSAV300.can \usr\sap\trans\cofiles

5. Verify that the following R/3 names are not already used:
   - Development Class name ZCAN
   - Function Group name Y210
   - Function Modules that begin with Y_210
   - Transactions that begin with YC
   - Module Pool SAPMY210
   - Tables or Structures that begin with Y210
   - Authorizations that begin with Y300_
   - Message Group name YC

   **Note:** If these names are already used, you need to either rename them or contact Candle for another Transport Data file.

6. Execute the following commands:
   
   tp addtobuffer COANKSAV300 SID
   pf=\usr\sap\trans\bin\PROFILE_NAME
tp import CANKSAV300 SID client nnn U16
pf=\usr\sap\trans\bin\PROFILE_NAME

where:

- **SID** is the target R/3 system ID.
- **PROFILE_NAME** is the tp profile file name.
- **nnn** is the target client number.

Alternately you may use the R/3 STMS transaction to import the CANKSAV300 transport request. Ensure that the “Import Transport Request Again” and the “Overwrite Objects in Unconfirmed Repairs” options are checked on the Import Options tab of the Import Transport Request dialog.

**Defining the R/3 user**

The R/3 user ID you specify is used by the monitoring agent for R/3 to log on to the R/3 System.

The R/3 user ID you specify must have sufficient authority to execute the Remote Function Call (RFC) code that was installed by importing the RSAV300.can file. Use the following procedure to verify the user authorization for that user ID.

1. Use transaction SU01 to define a CPIC R/3 user ID.

   **Note:** The password that is set for this user ID can be either plain text or optionally encrypted to a file as explained in “Password encryption (optional)” on page 170.

2. Ensure that this R/3 user ID has sufficient authority to execute the Remote Function Call (RFC) code that was installed by importing the CANKSAV300 transport. The Candle-supplied user profile named Y300AUTHS contains the minimum required authority and can be assigned without change to this R/3 user ID.

   You will supply the user ID on the R/3 Agent Configuration dialog in the R/3 Logon User ID field.

**Verifying that the COLLECTOR_FOR_PERFORMANCE job is**
scheduled

Use transaction SM37 to verify that the COLLECTOR_FOR_PERFORMANCE batch job is set up as described in the R/3 installation documentation and SAP OSS Note 16083.

The actual jobname may be different on your system.

Removing remote function modules from R/3

Should you ever choose to remove the monitoring agent for R/3 from your system, use this procedure to remove the remote function modules from your R/3 system.

1. Open a Windows command prompt.
2. Change the current directory to the directory where you downloaded the agent. The default is: \Candle\Cma
3. Copy file RSAD300.CAN to the Transport System data directory \usr\sap\trans\data. For example:
   `copy RSAD300.CAN \usr\sap\trans\data`
4. Copy file KSAD300.CAN to the Transport System cofiles directory \usr\sap\trans\cofiles. For example:
   `copy KSAD300.CAN \usr\sap\trans\cofiles`
5. Execute the following commands:
   ```
   tp addtobuffer CANKSAD300 SID pf=\usr\sap\trans\bin\PROFILE_NAME
   tp import CANKSAD300 SID client nnn U16 pf=\usr\sap\trans\bin\PROFILE_NAME
   ```
   where:
   - SID is the target R/3 system ID.
   - PROFILE_NAME is the tp profile file name.
   - nnn is the target client number.

   Alternately you may use the R/3 STMS transaction to import the CANKSAV300 transport request. Ensure that the “Import Transport Request Again” and the “Overwrite Objects in Unconfirmed Repairs” options are checked on the Import Options tab of the Import Transport Request dialog.
6. Proceed to “Configuring an instance of the R/3 Agent” on page 175.

Configuring an instance of the R/3 Agent

The monitoring agent for R/3 is configured using a Template. A Template allows you to define one or more agents of a specified type.

To configure a new instance of the monitoring agent for R/3, proceed as follows.

1. From the Manage Candle Services window, highlight the R/3 Monitoring Agent Template, right-click and select “Configure Using Defaults”.

The R/3 Monitoring Agent dialog displays

![R/3 Monitoring Agent dialog]

2. Enter the three-character R/3 system identifier (SID).

The name you supply will be used to identify this instance of the R/3 monitoring agent and will appear in the Task/Subsystem column of the Manage Candle Services window.

Click **OK** to continue.

3. The R/3 Agent Configuration dialog displays. The system name you supplied appears in the upper left area of the dialog (in our example, the system name is CAN).
Enter the following values in the R/3 Agent Configuration dialog:

- **Host name:**
  - Primary: Enter the hostname of the R/3 central instance. Defaults to the hostname where the agent is running.
  - Alternate 1: Enter a second choice for hostname in case the Primary host becomes unavailable.
  - Alternate 2: Enter a third choice for hostname in case both the Primary and Alternate 1 hosts become unavailable.

- **System number:** Enter the two-character R/3 system number. It defaults to 00.

- **Client number:** Enter the R/3 client number for the RFC logon to R/3. Defaults to 000.

- **User ID:** Enter the R/3 user ID for the RFC logon to R/3. It defaults to SAPCPIC.

One of the following options for Password:
– Password: Enter the R/3 password for the user ID you specified. Defaults to ADMIN.

– Password File: The name of the file that an encrypted password can be read from. (Refer to “Password encryption (optional)” on page 170.) If the password file is not in the same directory as the R/3 monitoring agent, specify the full path and file name of the password file.

• RFC Trace: Select this checkbox to activate RFC tracing.
• View RFC Trace: Press this button to view the RFC trace.

4. Click OK to save the configuration values.
   Your values are saved in the system registry, and the agent now starts as a system service.

5. You can, if you wish, create another instance of the monitoring agent for R/3. Use a unique System Name for each R/3 monitoring agent you create using the R/3 Monitoring Agent Template.

6. When you have completed configuration of agents you are installing at this time, proceed to “Installing OMEGAMON DE” on page 110.
Remedy ARS

Use the following procedure to configure the Remedy ARS Alert Manager:

1. When configuring this agent, you must first respond to the following prompt:

   ![Configuration Prompt 1]

   2. Enter the host name or address where the Remedy server is running. Then select either **OK** to continue or **Cancel** to abort the configuration. Next prompt:

   ![Configuration Prompt 2]

   3. Enter the Remedy user ID to be used for logging into the Remedy database. Then select either **OK** to continue or **Cancel** to abort the configuration.
Next prompt:

4. Enter the password for the user ID specified in the previous dialog. Note that this entry is obscured when typed. Then select either OK to continue or Cancel to abort the configuration.

Next prompt:

5. A Candle program monitors the Remedy log for customer-defined situations and communicates them to the agent via the port number you specify here. Enter the port number to be used, in the range of 1025 to 65535.

6. Then select either OK to finish configuring the agent or Cancel to abort the configuration.
Overview

The monitoring agent for Tuxedo is configured using a “Template”. A Template allows you to define one or more agents of a specified type. There are two types of Tuxedo agent: local or remote. Templates are provided for each type.


- **Tuxedo Remote Monitoring Agent**: installs on a TUXEDO Workstation Client machine running Windows XP Professional Edition or Windows 2000. (This agent can be used to monitor a Tuxedo Application Server running on a platform other than Windows.) This workstation requires that the Tuxedo Client Workstation software be installed prior to installing the agent.

*Note:* The remote Tuxedo monitoring agent cannot be used in a PeopleSoft environment. If your Tuxedo Server is being used for PeopleSoft, please use the native version of the Tuxedo monitoring agent.

Each Tuxedo agent (local or remote type) collects information from a single MIB (Management Information Base). There is one MIB per TUXEDO domain, therefore each Tuxedo agent collects information about one TUXEDO domain. If you want to collect information about multiple TUXEDO domains that are running on the same machine, install and configure one agent for each domain you want to monitor.

You can install both local and remote Tuxedo agents in any combination.

*Note:* It is necessary that the Windows system Path environment include the Tuxedo bin subdirectory to allow the agent to run as a service.

Configuring the monitoring agent for Tuxedo on Windows XP Professional Edition or Windows 2000

To configure a new Monitoring Agent for Tuxedo, proceed as follows:

1. From the Manage Candle Services main dialog, choose the appropriate Tuxedo template:
Select “Tuxedo Local Monitoring Agent – Template” if you installed the agent on the Tuxedo Application Server machine.

Select “Tuxedo Remote Monitoring Agent – Template” if you installed the agent on the Tuxedo Workstation Client machine.

Then right-click and select “Configure Using Defaults”.

2. Depending upon your previous selection, one of the following dialogs displays.

![Tuxedo Local Monitoring Agent dialog](image1)

![Tuxedo Remote Monitoring Agent dialog](image2)

This dialog prompts you for a unique name for this instance of the agent.

3. Supply a name that will be used to distinguish between Tuxedo monitoring agents installed on the same machine. We suggest you use the domain name of the TUXEDO application to be monitored. For example, “FS” could identify a Financial application; “HR” could identify an Human Resources application.

The name you supply becomes the first part of the agent’s managed system name and will be visible on many OMEGAMON XE displays.

4. Click **OK** to continue configuring the agent.
5. The Monitoring Agent for Tuxedo Configuration dialog prompts you for system-specific information.

The following values are required to configure the agent.

Table 18. Tuxedo Monitoring Agent Configuration Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUXCONFIG</td>
<td>The complete name and path of the binary configuration file for the TUXEDO domain that this monitoring agent will monitor. Note: This is the compiled binary TUXCONFIG configuration file that is generated when you first run tmloadcf.exe to parse the ASCII UBBCONFIG configuration file. For example: <code>D:\FDM700\Appserv\FDM700MS\PSTUXCFG</code> For more information see <code>tmloadcf(1)</code> in the BEA TUXEDO Reference Manual.</td>
</tr>
<tr>
<td>TUXDIR</td>
<td>The complete name and path of the home directory where the BEA TUXEDO software is installed. For example: <code>D:\Tuxedo</code></td>
</tr>
</tbody>
</table>

- If your Tuxedo Application uses BEA Message Queues, you can specify Tuxedo Queues that you want the agent to monitor.

**Note:** PeopleSoft applications that use Tuxedo do not support the BEA Message Queue feature.
6. To specify message queues, click the **Queue Config** button and the Tuxedo Queue Monitoring Configuration dialog is displayed.

Supply the following information to identify a message queue.

**Table 19. Tuxedo Monitoring Agent Queue Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuxedo Queue Name</td>
<td>The name of a Tuxedo Application Queue Space to be monitored. For example:</td>
</tr>
<tr>
<td></td>
<td><strong>QSPACE</strong></td>
</tr>
<tr>
<td>Tuxedo Queue Configuration File</td>
<td>The complete name and path of the Queue Device (which is a file name). For example:</td>
</tr>
<tr>
<td></td>
<td><strong>D:\Tuxedo65\apps\msq\QUE</strong></td>
</tr>
<tr>
<td>Tuxedo Queue Logical Machine Identifier</td>
<td>The LMID associated with the Tuxedo Queue named above. For example:</td>
</tr>
<tr>
<td></td>
<td><strong>SITE1</strong></td>
</tr>
</tbody>
</table>

7. To specify information about another queue, click **Add Queue**.

8. When you are finished supplying queue information, click **Done** to return to the Monitoring Agent for Tuxedo Configuration dialog.
If you are configuring a remote Tuxedo monitoring agent, select the “Advanced Configuration” checkbox (on the Monitoring Agent for Tuxedo Configuration dialog) and supply values for the following:

**Table 20. Tuxedo Monitoring Agent Advanced Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Specific Data</td>
<td>If Tuxedo security is set to “USER.AUTH.” then each individual user must be authenticated in addition to providing the application password. Specify the User-specific data here that will be passed to an authentication service. Often, the data is a per-user password. The data is automatically encrypted when passed over the network from Tuxedo Workstation Clients.</td>
</tr>
<tr>
<td>Application User Name</td>
<td>Specify the name that represents the caller. Often, the name is the same one used to log on to the operating system.</td>
</tr>
<tr>
<td>Application Password</td>
<td>If Tuxedo security is set to “APP_PW.” then every client must provide an application password as part of joining the application. Specify the password that the agent requires.</td>
</tr>
<tr>
<td>Client Name</td>
<td>The name of the Tuxedo Workstation Client, installed on this machine, with which the agent will communicate.</td>
</tr>
</tbody>
</table>

9. When you are finished, click **OK**. This completes the configuration. The agent is ready to start.

**Authority required for the Tuxedo monitoring agent on Windows**

On Windows XP Professional Edition or Windows 2000, the monitoring agent for Tuxedo can be started by the same user ID that booted the TUXEDO domain or by any user ID with administrator privileges.
Universal Agent

The Universal Agent is a generic agent that may be configured to monitor any type of data collected at your site. In this section you will complete the configuration of the Universal Agent using default configuration data and start the agent.

This section also contains instructions for:
- Customizing the Universal Agent startup parameters.
- Running multiple instances of Universal Agent.

To complete the default configuration of Universal Agent and start the agent, follow these steps:

1. If the Manage Candle Services window is not displayed, open it from the Start button as follows: “Programs > Candle OMEGAMON XE > Manage Candle Services”.

2. From the Manage Candle Services window, select (highlight) “Universal Agent”.

3. Right-click and select “Configure Using Defaults” from the popup menu. This prompt is displayed:

   Do you want to update the file KUMENV prior to configuration of Universal Agent.

4. Click Yes and OK to display the defaults supplied in the kunenv configuration file. For installation testing purposes, Candle recommends that you complete the configuration of the agent using these defaults. You may reconfigure the agent at any time to customize this data for your site.

   “KUMENV defaults” on page 186 shows the default parameters, for your reference.

5. Close the Notepad session. This prompt is displayed:

   The KUMENV edit session is complete. Press Yes to configure the agent. Press No to skip configuration of the agent.

6. Click Yes.

   For complete information about customizing Universal Agent for your site, refer to the Universal Agent User’s Guide.
Universal Agent

KUMENV defaults

*  Universal Agent Environment Variable Configuration File
*  KBB_SIG1=-dumpoff -asyncoff
  KIB_MAXCOLS=127
  *  Force specific non-standard tcpip domain name
  KUM_TCPIP_DOMAIN_NAME=
  *  Needed for multi-home system (more than one network interface)
  KDCB0_HOSTNAME=
  KUM_DCH_HOSTNAME=
  KUM_DP_HOSTNAME=
  KUM_DCH_HOST=
  KUMP_DCH_HOST=
  *  UA Startup automatic start DP options
  *  (ASFS,APIS,FILE,SOCK,HTTP,SNMP,POST,WEB,ODBC)
  KUMA_STARTUP_DP=asfs
  *  Location of UA output such as CAT, ATR, ODI, and so on
  KUM_WORK_PATH=C:\Candle\CMA\WORK
  *  DP Initialization Parameter File Path
  KUMP_INIT_CONFIG_PATH=C:\Candle\CMA\WORK
  *  *  DP Metafile Definition Parameters
  KUMP_META_PATH=C:\Candle\CMA\METAFILES
  KUMP_META_SERVER=
  *  *  SNMP DP Parameters
  KUMP_SNMP_MONITOR_TRAP=Y
  KUMP_SNMP_NET_DISCOVERY=Y
  KUMP_SNMP_NET_DISCOVER_ENTERPRISE=N
  KUMP_SNMP_MANAGE_LOCAL_NETWORK=Y
  *  KUMP_SNMP_DEBUG_TRAP=N
  KUMP_SNMP_DEBUG_DISCOVERY_ROUTE=N
  KUMP_SNMP_DEBUG_DISCOVERY_ENTERPRISE=N
  KUMP_SNMP_DEBUG_DISCOVERY_NETWORK=N
  KUMP_SNMP_DEBUG_MIB_MANAGER=N
  KUMP_SNMP_DEBUG_MIB_IO=N
  *  *  Trace Specification -- Do not modify commented examples.
  *  No error tracing.  KBB_RAS1=-none-
  *  Trace general errors.  KBB_RAS1=ERROR
  *  Trace Universal Agent request processing.  KBB_RAS1=ERROR
    (UNIT:kuma STATE ERROR) (UNIT:kumfa ALL)
  *  Trace Data Provider request processing.  KBB_RAS1=ERROR (UNIT:kump ALL)
    KBB_RAS1=ERROR ^>C:\Candle\CMA\logs\KUMRAS1.LOG
  ********************************************************

Customizing startup parameters

You may also customize Universal Agent startup parameters.

Follow these steps:

1. From the Start button, select:
“Programs > Candle OMEGAMON XE > Manage Candle Services“.

The Manage Candle Services window opens.

2. Select “Candle Universal Agent”. (If the agent is running, right-click and select “Stop Service” to stop it.)

3. Right-click and select: “Change StartupParms”.

The StartupParms dialog displays.

Enter the desired startup parameters, separating each by a comma, and leaving no spaces (as shown in the figure above).

Definitions for Universal Agent startup parameters are shown in Table 21.

<table>
<thead>
<tr>
<th>Startup Argument</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>No arguments</td>
<td>Universal Agent starts ASFS Data Provider within Universal Agent process</td>
</tr>
<tr>
<td>API</td>
<td>Starts API Server Data Provider within Universal Agent process</td>
</tr>
<tr>
<td>ASFS</td>
<td>Starts consolidated Data Provider within Universal Agent process (in other words, this argument is a combination of API, SOCK, and FILE) This is the default.</td>
</tr>
<tr>
<td>FILE</td>
<td>Starts File Data Provider within Universal Agent process</td>
</tr>
<tr>
<td>HTTP</td>
<td>Starts the HTTP Data Provider within Universal Agent process</td>
</tr>
<tr>
<td>ODBC</td>
<td>Starts the ODBC Data Provider within Universal Agent process</td>
</tr>
<tr>
<td>POST</td>
<td>Starts Post Data Provider within Universal Agent process</td>
</tr>
<tr>
<td>SOCK</td>
<td>Starts Socket Data Provider within Universal Agent process</td>
</tr>
</tbody>
</table>

Note: This argument is only valid on Windows XP Professional Edition or Windows 2000 systems.
Table 21. Universal Agent Startup Arguments (continued)

<table>
<thead>
<tr>
<th>Startup Argument</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Starts the SNMP Data Provider within Universal Agent process</td>
</tr>
</tbody>
</table>

4. Click **OK** to save the startup parameters you have entered, or click **Cancel** to close without saving. The Manage Candle Services window opens.

5. Select “Candle Universal Agent”, right-click and select “Start Service” to start the agent.

Be aware that the startup parameters you specify using this dialog are not persistent; they will not remain in effect when the agent is restarted.

Using the API Server Data Provider with Universal Agent

If you are using the API Server Data Provider, you need to have the UA API client package on the same machine as the client program or the machine on which you are compiling the program. The UA API client package consists of the following:

- A library containing the binary executables of the API functions and containing export function definitions for linking customer-created API client applications
- A C header file
- A set of command line interface programs

The client package was developed in standard C language and it requires only a common C runtime environment and TCP/IP with a socket interface.

To access the package, go to the `{Candle\cma` directory. Then copy the files in the table below to the target machine.

Table 22. API Client Package

<table>
<thead>
<tr>
<th>Part Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KUMPAPI.h</td>
<td>API C header file</td>
</tr>
<tr>
<td>KUMPAPI.lib</td>
<td>API function export library file</td>
</tr>
<tr>
<td>KUMPAPI.dll</td>
<td>API function runtime dynamic link library</td>
</tr>
<tr>
<td>KUMPBGNI</td>
<td>dp_BeginInput console command</td>
</tr>
</tbody>
</table>
If the client program is sending data from a machine that is not the host of the
data provider, or if you have changed the port on the host that the API server
is listening on, set the environment variables below, as applicable. You may
set these variables in the program or login script of the client host, or as part of
the machine’s configuration:

KUMP_API_DPAPI_HOST
KUMP_API_DPAPI_PORT

Using the SNMP Data Provider with Universal Agent

The SNMP-MANAGER TRAP report contains information on traps received
by the SNMP Data Provider. You must configure your SNMP agents to send
traps to the host of the SNMP Data Provider to receive data in this report.

Running multiple instances of Universal Agent

Be careful about the length of the instance name when creating multiple
instances of Universal Agent. The Manage Candle Services window allows
you to create instance names up to 20 characters; however, Universal Agent
limits the entire managed system name (instance name + hostname +
application name) to 32 characters and if the managed system name exceeds
32 characters, the instance name is truncated from the left. For example:
instance name ABCDEFGHIJKLMNOP would be truncated and the entire
managed system name would be
DEFGHIJKLMNOP_hostname:applicationVV.

If your site uses multiple instances, be sure to use short instance names to
avoid exceeding the 32-character limit.

Table 22. API Client Package (continued)

<table>
<thead>
<tr>
<th>Part Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KUMPDEFN</td>
<td>dp_Define console command</td>
</tr>
<tr>
<td>KUMPENDI</td>
<td>dp_EndInput console command</td>
</tr>
<tr>
<td>KUMPINPT</td>
<td>dp_InputData console command</td>
</tr>
<tr>
<td>KUMPPING</td>
<td>dp_Ping console command</td>
</tr>
<tr>
<td>KUMPRDFN</td>
<td>dp_Redefine console command</td>
</tr>
<tr>
<td>KUMPSHOW</td>
<td>dp_ShowMessage console command</td>
</tr>
</tbody>
</table>

If the client program is sending data from a machine that is not the host of the
data provider, or if you have changed the port on the host that the API server
is listening on, set the environment variables below, as applicable. You may
set these variables in the program or login script of the client host, or as part of
the machine’s configuration:

KUMP_API_DPAPI_HOST
KUMP_API_DPAPI_PORT

Using the SNMP Data Provider with Universal Agent

The SNMP-MANAGER TRAP report contains information on traps received
by the SNMP Data Provider. You must configure your SNMP agents to send
traps to the host of the SNMP Data Provider to receive data in this report.

Running multiple instances of Universal Agent

Be careful about the length of the instance name when creating multiple
instances of Universal Agent. The Manage Candle Services window allows
you to create instance names up to 20 characters; however, Universal Agent
limits the entire managed system name (instance name + hostname +
application name) to 32 characters and if the managed system name exceeds
32 characters, the instance name is truncated from the left. For example:
instance name ABCDEFGHIJKLMNOP would be truncated and the entire
managed system name would be
DEFGHIJKLMNOP_hostname:applicationVV.

If your site uses multiple instances, be sure to use short instance names to
avoid exceeding the 32-character limit.
Warehouse Proxy

Warehouse Proxy is an ODBC export server for warehousing historical data. It is a special agent that uses an ODBC connection to transfer historical data collected from other agents included with this release to a previously-installed and configured database. This data can then be analyzed further using third-party software.

Warehouse Proxy supports these database management systems:

- Microsoft SQL Server (version 7.0 and above) on a Windows 2000 Server

If you do not intend to use historical reporting or save historical data to a database for reference, then you do not need to install or configure the Warehouse Proxy.

For more information on configuring OMEGAMON XE for historical reporting, see the Historical Data Collection Guide for OMEGAMON XE and CandleNet Command Center.

About the Candle Warehouse Proxy

The Warehouse Proxy has some special requirements and restrictions. Be aware that:

- You can configure only one Warehouse Proxy in your site’s Candle network.

- Historical data collection can be configured to be stored at any combination of the CMS or the agents. To ensure that history data is received from all sources, you must configure a common shared network protocol between the Warehouse Proxy and the component that is sending history data to it (either from a CMS or from an agent).

For example, you might have a CMS configured to use both IP and IPPPIPE. In addition, one agent might be configured with IP and a second agent with IPPPIPE. In this example, the Warehouse Proxy would need to be configured to use both IP and IPPPIPE.

- Candle recommends that your site install and configure the database client software provided by the database vendor on the machine where you intend to configure Warehouse Proxy.
Warehouse Proxy

The machine where Warehouse Proxy resides must have TCP/IP access to, and must also be configured to have ODBC database connectivity to, the machine where the database is running.

- Warehouse Proxy accesses the database using TCP/IP and ODBC with a user ID and password of Candle.
- You must ensure that the appropriate ODBC driver is installed on the machine where the Warehouse Proxy is installed. If it is not installed, consult your database documentation about installing the driver.
- The name of the database to which the historical data will be written can be anything that you like, but if you want the data source to be in a special database, that database must be created before configuring the datasource. You will most likely want to create a special database first.
- The Warehouse Proxy can only successfully connect to a hub CMS. It is the user’s responsibility to configure the Proxy to point to a hub CMS. If the CMS named in the configuration is not a hub, the Proxy cannot perform its function.

Setting up the ODBC connection

The following tasks must be completed before the Warehouse Proxy can operate successfully. These tasks are best performed by your database System Administrator.

1. Set up the historical database with the required IDs and authorities
   If you have not already done so, decide which existing database will receive the historical data or create a new database for this purpose. Refer to your database documentation for instructions on creating a database.
   
   For the database that will receive historical data, define a database user name (or login name, depending on your software) called “candle” with a password of “candle”. (If you have already configured a database agent, this user name and password should already be defined in the database.)

   Note: “candle” is case-sensitive and must be typed exactly as shown.

   Grant the new Candle user name (or login name) the following database permissions.

   - Grant both “create table” and “alter table” authority. (Alter Table authority is included in Create Table authority when using Microsoft SQL Server).
Grant “database access” to the database that will contain the warehoused data.

Instructions may vary depending on your version of database software. Refer to your database documentation for instructions on granting authorities.

**Note:** Microsoft SQL Server Users: The Warehouse Proxy will be inserting many rows of data to the database, which will generate many rows of Transaction log data in the System logs table. It is the user’s responsibility to ensure that the Transaction log does not fill up or Warehousing, along with other database updates, will cease. Therefore, ensure that you allocate sufficient space to the Transaction log. Also, Candle recommends setting the Truncate Log on Checkpoint option for the historical database.

2. Install the Database Client.
   Install the ODBC driver on the machine where you will install the Warehouse Proxy. Refer to your database documentation for instructions.

3. Configure the Database Client to connect to the database.
   Configure an ODBC database connection from the database client to the database that will receive the historical data.

4. Test the ODBC database connection before continuing.
   Candle recommends that you test the connection with the testing tool provided by the database client software before installing or configuring the Warehouse Proxy. When testing the ODBC database connection, specify both a user name of “candle” and a password of “candle”.

   **Note:** “candle” is case-sensitive and must be typed exactly as shown.

   If you encounter difficulty with this process, consult the documentation that came with your database software.

---

**Configuring and registering the Warehouse Proxy**

To complete the configuration for Warehouse Proxy, proceed as follows.

1. From the Manage Candle Services window, select (highlight) “Warehouse Proxy”.

2. Right-click and select “Configure Using Defaults”.
   This message is displayed:
When configuring the Warehouse Proxy, remember that it must connect to a HUB CMS (not a remote CMS).

3. Click **OK** to continue.

   The first Agent Advanced Configuration for Warehouse Proxy window appears.

4. Enter appropriate values in the fields for the window.

5. Click the **OK** button.

   The second Agent Advanced Configuration for Warehouse Proxy window appears.

6. Enter appropriate values in the fields for the window.

7. Click the **OK** button.

   This message is displayed:

   **Would you like to configure your Candle Data Warehouse ODBC data source?**

8. Click **Yes**.
Manage Candle Services launches the Windows ODBC Data Source Administrator. For example:

9. Select the “System DSN” tab.

10. Configure the Data Source as follows:
   1. Name the ODBC data source: “Candle Data Warehouse”.
      Note that “Candle Data Warehouse” is case-sensitive and must be typed exactly as shown.
   2. When asked
      **How should SQL Server verify the authenticity of the login ID?**
      specify:
      **SQL Server authentication using a login ID and password entered by the user.**
   3. Enter the following:
Login ID: candle
Password: candle

Do not select “Use Trusted Connection” if it is presented as an option.

4. Review the displayed configuration information and test the data source. The Warehouse Proxy will not function without a working ODBC database connection to the Candle Data Warehouse datasource.

11. When the tests complete successfully, click OK in all dialogs until you close the ODBC Administrator application.

12. The Warehouse Proxy is ready to start.

Warehouse Proxy error reporting

Warehouse Proxy errors are reported in the Windows Event Viewer Application Log on the system running Warehouse Proxy.

Behavior of the Warehouse Proxy

Please note the following behaviors of the Warehouse Proxy at startup and shutdown.

Behavior at startup

The first time the Warehouse Proxy inserts a record into the WAREHOUSELOG table it incurs an error (because the table has not been created yet). The first time this occurs, or whenever the table is deleted by the customer, an error is reported in the Event Viewer stating something to the effect that the table does not exist. This error can be ignored.

The Warehouse Proxy attempts to test the connection to the Candle Data Warehouse. It will do this repeatedly at startup for a period of time, and will log errors when it is unable to connect. This condition may be observed where the Warehouse Proxy has been installed on the same system as the database to which it will connect. If both the database and the Warehouse Proxy are set to start automatically, the Warehouse Proxy may come up first and will retry the connection to the database until it is successful, or until its retry count has been exceeded.

Note: The Warehouse Proxy will not start successfully if it is unable to connect to the Candle Data Warehouse datasource.
**Warehouse Proxy**

**Behavior at shutdown**
Since the Warehouse Proxy connects to a hub CMS, the Warehouse Proxy should be brought down before bringing down the hub. If the hub is brought down first, the Warehouse Proxy may still be shut down, but it will take a number of minutes to do so as it will try to disconnect from the hub first.

Note that it is not necessary to recycle the Warehouse Proxy when recycling the hub. The Warehouse Proxy reconnects with the hub on an hourly basis therefore manually recycling the Warehouse Proxy is not necessary.
WebSphere Application Server

This section contains instructions for configuring the WebSphere Application Server monitoring agent. At installation time, you will complete an initial configuration of the agent. You can reconfigure the agent at any subsequent time to customize its operation.

This section contains configuration information only for the basic parameters that allow you to successfully start the agent. Advanced configuration information is provided in the OMEGAMON XE for WebSphere Application Server User's Guide.

After performing the basic steps (steps 1 to 3) for configuring the WebSphere Application Server agent (See “Configuring the Agents” on page 108.), follow these steps:

(This prompt is displayed:)

Do you want to update the file kwe.xml prior to configuration of Websphere Application Server Agent.

1. Click **Yes**.

The kwe.xml configuration file is displayed in Notepad.

2. Set the parameters as described in the OMEGAMON XE for WebSphere Application Server User’s Guide.

   Note this special information about the Agent ID field:

### Table 23. Agent ID Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent ID</td>
<td>A unique identifier for the WebSphere Application Server agent. You must specify an Agent ID if you intend to run multiple WebSphere Application Server agents on the same host system. The default configuration file is kwe.xml; however, if you specify an Agent ID in this field, the configuration process creates a unique configuration file for the WebSphere Application Server agent using the following naming convention: “kwe_agentID.xml”. If you intend to run only one WebSphere Application Server agent on the host, you may leave this field blank. Default: “ “ (none)</td>
</tr>
</tbody>
</table>


3. Close the Notepad session.
   This prompt is displayed:

   **The kew.xml edit session is complete. Press Yes to configure the agent.**
   **Press No to skip configuration of the agent.**

4. Click **Yes**.

   The configuration file is updated with your changes:
   
   C:\candle\cma\kwe\xml

   or

   C:\candle\cma\kwe\agentID.xml (if you specified an Agent ID).

   You may reconfigure the agent at any time to customize its operation for your site. Consult the **OMEGAMON XE for WebSphere Application Server User’s Guide** for complete information.
WebSphere InterChange Server

This section contains instructions for configuring the OMEGAMON XE for WebSphere InterChange Server monitoring agent to collect data from SNMP agents on server hosts.

It also contains instructions for configuring a WebSphere InterChange Server Data Source to monitor a WebSphere InterChange Server log and send the data to the OMEGAMON XE for WebSphere InterChange Server monitoring agent, and for customizing the batch files the agent uses to start WebSphere InterChange Server instances.

Configuring SNMP data collection

**Note:** One of the IBM SNMP agents provided with WebSphere InterChange Server must be configured to monitor each server image for which you want to collect data, and KICAgent must be configured as its SNMP Manager. For instructions on configuring the IBM SNMP agents, please refer to to the section entitled "Using the SNMP Agent Configuration Manager" in Chapter 1 of the IBM WebSphere InterChange Server System Administration Guide.

To configure the monitoring agent, follow these steps:

1. Click **OK** at the following prompt:
   
   Use the following program to complete any required configuration activities and to start Candle services, if necessary.

   The Manage Candle Services window opens, showing the agents you have installed.

   If you do not want to configure the agent at this time, you can launch Manage Candle Services from the Start menu at a later time by selecting **Programs (or All Programs on Windows XE) > Candle OMEGAMON XE > Manage Candle Services**.

2. Right-click the WebSphere InterChange Server Monitoring Agent and select Configure Using Defaults.
   
   The Configure WebSphere InterChange Server Monitoring Agent window opens.

3. In the **Poll Interval** field, specify in seconds the interval at which you want the monitoring agent to poll the IBM SNMP agents.
Specify an interval between 30 and 300 seconds (5 minutes). The default is 60 seconds (1 minute).

4. Click **Add** to add the first SNMP agent.
   The Data for WebSphere InterChange Server Host window opens.

5. Fill out the fields as follows:
   - For **Name or IP Address**, specify the host name or IP address of the IBM SNMP agent you want to monitor.
   - For **Port**, specify the port to which the IBM SNMP agent is assigned.
     By default, the port used by SNMP agents is 161.
   - For **Community**, specify the name used to contact the SNMP agent.
     If you do not specify a community name, the default community name *administrator* is used.

6. Click **OK** to add the entry to the list of monitoring SNMP agents.

7. Repeat steps 4–6 until you have listed all the IBM SNMP agents monitoring all the WebSphere InterChange Server instances for which you want to collect SNMP data.

8. Click **OK** to save the configuration information and close the window.
   Once you have initiated data collection, you do not need to reconfigure it again each time you start the monitoring agent. The agent maintains information about monitored IBM SNMP agents in a configuration file so that data collection will persist across restarts.

You can add additional SNMP agents, or stop monitoring for particular agents, at a later date, using Manage Candle Services. For more information, see the *OMEGAMON XE for WebSphere InterChange Server Getting Started Guide*.

### Changing the agent listening ports

The OMEGAMON XE for WebSphere InterChange Server monitoring agent uses two listening ports to communicate with the WebSphere InterChange Server Data Source: by default, the values for these two ports are 17600 and 17700. If one or both of these ports is already in use, you must specify an alternative value in the agent’s ENV file.
If you edit these variables, you must specify the same values in the configuration file for every data source that sends data to agent (see “Configuring a WebSphere InterChange Server Data Source” on page 201).

*Note:* Candle recommends that you do not change these ports unless absolutely necessary.

To change the listening ports:

1. In the Manage Candle Services window, right-click the WebSphere InterChange Server Monitoring Agent.
2. From pop-up menu select:
   ```
   Advanced > Edit ENV file...
   ```
   The KICENV file is opened in Notepad.
3. Edit one or both of the following variables:
   ```
   KUMP_API_DPAPI_PORT=17600
   KUMP_DPCONSOLE_PORT=17700
   ```

   *Note:* You cannot change the second port unless you also change the first.
4. Save the file and close Notepad.

### Configuring a WebSphere InterChange Server Data Source

To connect to OMEGAMON XE for WebSphere InterChange Server monitoring agent, a WebSphere InterChange Server Data Source need to be configured with:

- the host name of the monitoring agent
- the data port of the monitoring agent
- the console port of the monitoring agent

In addition, the data source needs to know:

- the name of the WebSphere InterChange Server instance whose log it monitors
- the name and location of the server log it is monitoring

To configure a WebSphere InterChange Server Data Source:

1. Click **OK** at the following prompt:
Use the following program to complete any required configuration activities and to start Candle services, if necessary.

The Manage Candle Services window opens, showing the Candle components you have installed.

If you do not want to configure the agent at this time, you can launch Manage Candle Services from the Start menu at a later time by selecting Programs (or All Programs on Windows XE) > Candle OMEGAMON XE > Manage Candle Services.

2. Right-click the WebSphere InterChange Server Data Source and select Configure Using Defaults from the pop-up menu.
   The Configure WebSphere InterChange Server Host window opens.

3. Fill out the fields as follows:
   - In the Agent Host field, specify the name of the host on which the monitoring agent is executing.
   - (optional) For Data Port, specify the port on which the monitoring agent is listening for WebSphere InterChange Server Data Sources. (This field should have the same value as the KUMP_API_DPAPI_PORT variable in the monitoring agent’s KICENV file.)
   - (optional) For Console Port, specify the port to which the WebSphere InterChange Server Data Source should send the log data. (This field should have the same value as the KUMP_DPCONSOLE_PORT variable in the monitoring agent’s KICENV file.)

   By default, the values of 17600 and 17700 are used for these two ports. However, if these ports are not available on the monitoring agent host, the agent must be configured with alternative port numbers and the same port numbers must be specified in each WebSphere InterChange Server Data Source configuration file. (For information on configuring the port numbers for the monitoring agent, see “Changing the agent listening ports” on page 200.)

4. Click Add to add the name and location of the WebSphere InterChange Server log you want to monitor.
   The Configure Data for WebSphere InterChange Server Data Source Window opens.

5. Fill out the fields as follows:
For **Base Folder**, specify the fully qualified name of the WebSphere InterChange Server base directory. For example:

\`\`C:\IBM\WebSphere\ICS4.2.2\`\`

For **Log File**, specify the path to the WebSphere InterChange Server log, relative to the base directory. For example:

"InterChangeServer.log"

For **Server Name**, specify the name of the server instance that owns the log.

6. Click **OK** to add the entry to the configuration table.

7. Click **OK** to close the window and save the configuration information.

**Configuring server startup**

OMEGAMON XE for WebSphere InterChange Server uses a batch file to execute the Take Action Start Server command. If you want to issue other commands (for example, start the persistent naming server) or run other batch files before the server starts, you can modify this file.

The file is named `start<servername>.bat`. It is located on the server host in `candle\CMA`, where candle is the base directory in which the WebSphere InterChange Server Data Source is installed.

The file contains a single line similar to the following:

\`\`C:\WebSphere\ICS4.2.2\bin\start_server.bat WICSTest\`\`

To edit the file:

1. On the server host, open the file in a text editor.

2. Insert any commands you want to add before the existing line.

3. Save and close the file.

You must edit the file on the host of each server you want to affect, or copy the edited file to the CMA directory of each host.
Windows Management Web Service

The Windows Management Web Service product is supported only on Windows XP Professional Edition.

In this section you will complete the configuration of the Windows Management Web Service.

Windows Management Web Service is a .NET web service that collects Windows Management Instrumentation (WMI) data. It works as an interface between WMI and clients that collect WMI information. It runs as a web service, meaning that clients communicate with it using web protocols such as HTTP. The Universal Agent WBEM Data Provider is one such client.

To complete the configuration, follow these steps:

1. From a command prompt, enter:
   
   `compmgmt.msc`

   The Computer Management dialog opens.

2. Right-click “Services and Applications > Internet Information Services > Web Sites > Default Web Site”.

4. When prompted for an alias, enter: KwnWeb

5. Click **Next** to continue.

6. When prompted for the pathname, enter the location of the Windows Management Web Service files:
   Candle\Cma\KwnWeb

7. Click **Next** to continue.

8. Select the appropriate access permissions.

9. Click **Next** to finish.
   The Windows Management Web Service is now ready for use.
$candlehome  The execution environment that you will create in which to install, execute, and maintain OMEGAMON XE.

A

Access Control List (ACL)  A list of the services available on a server, each with a list of the hosts permitted to use the service.

ACL   See Access Control List (ACL).

description   A location of data, usually in main memory or on a disk.

Adobe Acrobat Reader   An application that allows you to view various types of files.

affinity   A symbol for dependence on, or support of, a certain collection of agents that may be installed as a unit on a user’s system.

agent   An executable file that gathers and distributes information about system performance. There is always one agent per managed system.

alert   A warning message that appears at a console to indicate that an event has occurred that may require intervention.

Alert Adapter   An agent that monitors and relays alerts to OMEGAMON XE products.

Alert Emitter   A feature of an Alert Adapter that acts as an agent and relays OMEGAMON XE data to other products. The destination can be either Candle or third-party products.

Alert Manager   An agent that monitors non-Candle monitoring products for a remote system, subsystem, or application, and relays alert information to the CMS.

alias   One of several alternative hostnames with the same Internet address. For example, in the UNIX hosts database (/etc/hosts or NIS map) the first field on a line is the Internet address, the next is the official hostname (the "canonical name" or "CNAME"), and any others are aliases.

Hostname aliases often indicate that the host with that alias provides a particular network service. The assignment of services to computers can then be changed simply by moving an alias from one Internet address to another, without the clients needing to be aware of the change.

API   See Application Program Interface (API).
Application Program Interface (API)  The interface (calling conventions) by which an application program accesses operating system and other services. An API is defined at source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure the portability of the code. An API can also provide an interface between a high level language and lower level utilities and services which were written without consideration for the calling conventions supported by compiled languages. In this case, the API's main task may be the translation of parameter lists from one format to another and the interpretation of call-by-value and call-by-reference arguments in one or both directions.

argument  A value or reference passed to a function, procedure, subroutine, command or program, by the caller. There are many different conventions for passing arguments to functions and procedures including call-by-value, call-by-name, call-by-need. These affect whether the value of the argument is computed by the caller or the callee (the function) and whether the callee can modify the value of the argument as seen by the caller (if it is a variable). Arguments to a program are usually given after the command name.

attribute  A discrete characteristic or piece of information, or a property of that information, such as type, source, or severity, about a managed system.

CandleNet Portal users use attributes to build predicates.

authorization  The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

browser  A software application used to locate and display Web pages.

Candle Management Server (CMS)  The host data management component in an OMEGAMON XE environment. It sends out requests to, and receives data from, managed systems having a monitoring agent or Alert Adapter installed. It also sends the information it receives to the CandleNet Portal.

Candle Management Workstation (CMW)  A workstation that may be a component of an OMEGAMON XE environment. It provides a programmable workstation-based graphical user interface for OMEGAMON XE, and allows users to define and control all the monitoring and
automation that OMEGAMON XE products provide. The CMW uses symbol and color changes to reflect the status changes of every object you are monitoring.

**CandleNet Portal**  A Java-based programmable graphical user interface that allows the user to view, define and control all the monitoring and automation of the CT environment.

**CandleNet Portal Server**  A collection of software services for the CandleNet Portal that enables retrieval, manipulation, and analysis of data from agents. It connects to both the CandleNet Portal and the CMS.

**Candle Technologies (CT)**  An integrated, layered architecture consisting of data access, communication, and presentation components that enable cross-platform operation and integration of data for systems management applications.

**client**  An application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

**client and server**  An architecture in which the client (personal computer or workstation) is the requesting machine and the server is the supplying machine. Servers can be high-speed microcomputers, minicomputers or even mainframes. The client provides the user interface and may perform some or all of the application processing. A database server maintains the databases and processes requests from the client to extract data from or update the database. An application server provides additional business processing for the clients. Client and server architecture is the equivalent of a mainframe system on a network of smaller computers.

**CMS**  See **Candle Management Server (CMS)**.

**CMW**  See **Candle Management Workstation (CMW)**.

**command**  A character string which tells a program to perform a specific action. Most commands take arguments which either modify the action performed or supply it with input. Commands may be typed by the user or read from a file by a command interpreter. It is also common to refer to menu items as commands.

**command interpreter**  A program which reads textual commands from the user or from a file and executes them. Some commands may be executed directly within the interpreter itself, and others may cause it to load and execute other files.

**CT**  See **Candle Technologies (CT)**.

**database server**  A stand-alone computer in a local area network that holds and manages the database. It
implies that database management functions, such as locating the actual record being requested, is performed in the server computer.

**data server**  See *Candle Management Server (CMS)*.

**De-Militarized Zone (DMZ)**  DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers to internal networks. Internal DMZ Ethernets link local nodes with routers to the regional networks.

**development environment**  An integrated suite of tools to aid the development of software in a particular language or for a particular application. Usually, this consists of a compiler and editor and may also include one or more of a debugger, profiler, and source code manager.

**development tool**  See *development environment*.

**distributed database**  A collection of several different databases that looks like a single database to the user. An example is the Internet DNS.

**distributed environment**  A collection of (probably heterogeneous) automata whose distribution is transparent to the user so that the system appears as one local machine. This is in contrast to a network, where the user is aware that there are several machines, and their location, storage replication, load balancing and functionality is not transparent. Distributed systems usually use some kind of client and server organization.

**DLL**  See *Dynamically Linked Library (DLL)*.

**DMZ**  See *De-Militarized Zone (DMZ)*.

**DNS**  See *Domain Name System (DNS)*.

**domain**  A specific phase of the software life cycle in which a developer works. Domains define developers' and users' areas of responsibility and the scope of possible relationships between products.

**Domain Name System (DNS)**  An Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to *198.105.232.4*.

**Dynamically Linked Library (DLL)**  A library which is linked to application programs when they are loaded or run rather than as the final phase of compilation. This means that the same block of library code can be shared between several tasks rather than each task containing copies of the routines it uses. The executable is compiled with a library of stubs which allow link errors to
be detected at compile-time. Then, at runtime, either the system loader or the task's entry code must arrange for library calls to be patched with the addresses of the real shared library routines, possibly via a jump table. The alternative is to make library calls part of the operating system kernel and enter them via some kind of trap instruction. This is generally less efficient than an ordinary subroutine call. It is important to ensure that the version of a dynamically linked library is compatible with what the executable expects.

**E**

**EIB**  See Enterprise Information Base (EIB).

**EIB tables**  The set of tables that define your EIB.

**Enterprise Information Base (EIB)**  The central repository for all persistent data, including situations, user definitions such as report formats, managed-object definitions, and historical data.

**Enterprise object**  An aggregation that represents all of your enterprise. The CandleNet Portal automatically creates the Enterprise object at initial product start-up. The Enterprise object contains all of the managed systems in the enterprise that are running CT products.

**environment variable**  A variable that is bound in the current environment.

When evaluating an expression in some environment, the evaluation of a variable consists of looking up its name in the environment and substituting its value.

**event**  A change in the status of a situation being monitored.

**executable**  A binary file containing a program in machine language which is ready to be executed (run).

**F**

**filter**  A higher-order function which takes a predicate and a list and returns those elements of the list for which the predicate is true.

**firewall**  Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

**framework**  The component of an agent that provides an interval timer and manager objects for managing agents and requests.

**function**  A method of evaluating the information that an attribute supplies. The functions used in CandleNet Portal are

1. Average *AVG
2. Count *COUNT
3. Make time *TIME
4. Maximum *MAX
Gateway

An agent that communicates events to any management application.

historical data collection

A capability of reports that enables the user to access monitoring data in order to analyze past system performance.

host

A computer system that is accessed by a user working at a remote location. Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal.

hostname

The unique name by which a computer is known on a network, used to identify it in electronic mail, Usenet news, or other forms of electronic information interchange.

On the Internet, the hostname is an ASCII string which consists of a local part and a domain name. The hostname is translated into an Internet address either via the /etc/hosts file, NIS or by the DNS or resolver. It is possible for one computer to have several hostnames (aliases) though one is designated as its canonical name.

hub

A central host system that collects the status of the situations and policies running on your managed systems.

hub server

A centrally configured CMS. The hub server accepts data from other servers (the remote servers) and from agents.

individual managed object

A managed object that corresponds to a single resource at the user’s site.

installer

A utility program to ease the installation of another, probably larger, application. It is also possible for hardware to have an installer accompany it, to install any low level device drivers required.

instance

An individual object of a certain class. While a class is just the type definition, an actual usage of a class is called "instance". Each instance of a class can have different values for its instance variables.

Internet Protocol (IP)

The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation...
and re-assembly through the data link layer.

ior Interoperable Object Reference connects clients to the CNP Server. The IOR identifies a remote object, including such information as name, capabilities and how to contact. In the URL you may have an ior reference. This is because it goes through the web server and CandleNet Portal Server uses it to tell the client which ior to fetch. Once it does that, it extracts the host and port and tells the client where to route the request.

IP See Internet Protocol (IP).

J

Java Database Connectivity (JDBC) Part of the Java Development Kit which defines an application programming interface for Java for standard SQL access to databases from Java programs.

Java Runtime Environment (JRE) The part of the Java Development Kit (JDK) required to run Java programs. The JRE consists of the Java Virtual Machine, the Java platform core classes and supporting files. It does not include the compiler, debugger or other tools present in the JDK. The JRE is the smallest set of executables and files that constitute the standard Java platform.

JDBC See Java Database Connectivity (JDBC).

JRE See Java Runtime Environment (JRE).

K

keyword One of a fixed set of symbols built into the syntax of a language. Typical keywords would be if, then, else, print, goto, while, switch. There are usually restrictions about reusing keywords as names for user-defined objects such as variables or procedures. Languages vary as to what is provided as a keyword and what is a library routine, for example some languages provide keywords for input/output operations whereas in others these are library routines.

L

library A collection of subroutines and functions stored in one or more files, usually in compiled form, for linking with other programs. Libraries are one of the earliest forms of organized code reuse. They are often supplied by the operating system or software development environment developer to be used in many different programs. The routines in a library may be general purpose or designed for some specific function such as three dimensional animated graphics. Libraries are linked with the user's program to form a complete executable. The linking may be static linking or, in some systems, dynamic linking.
literal A constant made available to a process, by inclusion in the executable text. Most modern systems do not allow texts to modify themselves during execution, so literals are indeed constant; their value is written at compile-time and is read-only at runtime. In contrast, values placed in variables or files and accessed by the process via a symbolic name, can be changed during execution. This may be an asset. For example, messages can be given in a choice of languages by placing the translation in a file. Literals are used when such modification is not desired. Also see variable.

log CandleNet Portal records changes to situations and EIB objects in a log.

logical unit (LU) A primary component of SNA, an LU is a type of Network Addressable Unit that enables end users to communicate with each other and gain access to SNA network resources.

Logical Unit 6.2 (LU6.2) A type of logical unit that governs peer-to-peer SNA communications. LU6.2 supports general communication between programs in a distributed processing environment.

LU6.2 is characterized by a peer relationship between session partners, efficient use of a session for multiple transactions, comprehensive end-to-end error processing and a generic application program interface consisting of structured verbs that are mapped into a product implementation.

M

managed object A visual representation, typically an icon, of one or more situations being monitored on one or more managed systems. As the status of a situation changes, the appearance of a managed object icon on your workstation changes.

managed system Any system, such as UNIX, Windows, or OS/390, that a CT is monitoring. When a new instance of a type of managed system comes online for the first time, information about it is placed automatically in the Managed Systems icon in the CandleNet Portal main window. See also type of managed system.

monitoring agent A process that probes a managed system for data and can make a managed system look like a set of objects on a CandleNet Portal.

N

NAT See Network Address Translation (NAT).

Network Address Translation (NAT) A hardware device currently being developed and used to extend the Internet addresses already in use. NAT has been suggested as an alternative to
adopting IPv6 (IPng). It allows duplicate IP addresses to be used within a corporation and unique addresses outside.

**Network Interface Card (NIC)** An adapter circuit board installed in a computer to provide a physical connection to a network.

**NIC** See *Network Interface Card (NIC)*.

**node** A single computer within a network of computers.

**O**

**ODBC** See *Open DataBase Connectivity (ODBC)*.

**OMEGAMON** The name under which Candle delivers CT to its customers. See *Candle Technologies (CT)*.

**Open DataBase Connectivity (ODBC)** A standard database access method developed by Microsoft Corporation. The goal of ODBC is to make it possible to access any data from any application, regardless of which database management system (DBMS) is handling the data. ODBC manages this by inserting a middle layer, called a database driver, between an application and the DBMS. The purpose of this layer is to translate the application's data queries into commands that the DBMS understands. For this to work, both the application and the DBMS must be ODBC-compliant - that is, the application must be capable of issuing ODBC commands and the DBMS must be capable of responding to them.

**operand** An argument of an operator or of a machine language instruction.

**operator** A symbol used as a function, with infix syntax if it has two arguments (such as +) or prefix syntax if it has only one (such as Boolean NOT). Many languages use operators for built-in functions such as arithmetic and logic.

**P**

**parameter** See *argument*.

**partition** In a firewall environment, a term used to designate either the public network (outside the firewall) or the private network (inside the firewall).

**pathname** The specification of a node (file or directory) in a hierarchical file system. The path is usually specified by listing the nodes top-down, separating the directories by the pathname separator ("/" in UNIX, ") in MS-DOS). A pathname may be an absolute pathname or a relative pathname. The part of the pathname of a file after the last separator is called the basename.

**permission** The ability to access (read, write, execute, traverse, etc.) a file or directory. Depending on the operating system, each file may have different permissions for different kinds of access and different users or groups of users.
**persistence**  An object that exists after the program that created it has ended. See persistent object.

**persistent data**  Data that exists from session to session. Persistent data is stored in a database on disk or tape.

**persistent object**  An object that continues to exist after the program that created it has been unloaded. An object’s class and current state must be saved for use in subsequent sessions.

**platform**  The underlying hardware or software for a system. The platform defines a standard around which a system can be developed. Once the platform has been defined, software developers can produce appropriate software and managers can purchase appropriate hardware and applications. The term is often used as a synonym of operating system.

**policy**  A collection of activities that provides the capability of automating responses to events or routine operator tasks.

**port number**  The “channel” that is used for one or more components to communicate with one another via a communications protocol. There are three recognized ranges of port numbers: The Well Known Ports from 0 through 1023, the Registered Ports from 1024 through 49151, and the Dynamic and Private Ports from 49152 through 65535. Candle’s reserved port number is 1918.

**predicate**  The major portion of a situation that functions to compare a system condition (attribute) to a value. Predicates are of the form:

\[
\text{system condition - compared to - value}
\]

An example of a predicate is

```
CPU usage - greater than - 90%
```

**product-provided situations**  CandleNet Portal-provided set of predefined situations for you to use as-is or to modify. Using product-provided situations makes it unnecessary to create your own.

**protocol**  A communications protocol is a set of rules or standard designed so that computers can exchange information with a minimum of errors.

**query**  A user’s (or agent’s) request for information, generally as a formal request to a database or search engine.

**relational operator**  Predicate operators that compare attributes to a compare value. The six relational operators are

1. Greater than
2. Less than
3. Equal to
4. Not equal to
5. Greater than or equal to
6. Less than or equal to

remote server Remote CMSs accept data from agents and report that data to a hub CMS. They are optional components of the CT environment that must communicate with a hub CMS first in order to send communication to a CandleNet Portal. It does so by collecting data from local agents and transmitting it to a hub CMS.

replication The process of creating and managing duplicate versions of a database. Replication not only copies a database but also synchronizes a set of replicas so that changes made to one replica are reflected in all the others. The beauty of replication is that it enables many users to work with their own local copy of a database but have the database updated as if they were working on a single, centralized database. For database applications where users are geographically widely distributed, replication is often the most efficient method of database access.

report Displays of data from managed systems. The data may be real-time or historical. Users filter the displays and produce charts.

root The superuser account that overrides file permissions. By extension, the privileged system-maintenance login on any operating system.

runtime The period of time during which a program is being executed, as opposed to compile time or load time.

runtime environment A collection of subroutines and environment variables that provide commonly used functions and data for a program while it is running.

S

seed data Product-specific catalog, attribute, and SQL data.

seeding The process of adding product-specific catalog, attribute, and SQL data (seed data) to a CMS. This process allows the CMS to recognize and acknowledge the product.

Simple Network Management Protocol (SNMP) A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a Management Information Base (MIB), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off or on, etc.)

situation A logical expression involving one or more system conditions (attributes) that the user wants to monitor that are of the form:
If - system condition - compared to - value - is true

An example of a situation is:

IF - CPU usage - GT - 90% - TRUE

IF and TRUE appear in every situation.

**Simple Object Access Protocol (SOAP)** A minimal set of conventions for invoking code using XML over HTTP.

**SNA** See *System Network Architecture (SNA)*.

**SNMP Gateway** An SNMP proxy agent that acts as a bridge between the hub CMS and third-party SNMP management application. It uses the native SNMP services of its host operating system to send SNMP traps (alerts) from the CMS to the third-party application. It translates GET and GETNEXT requests from the application to the CMS.

**SOAP** See *Simple Object Access Protocol (SOAP)*.

**SQL** See *Structured Query Language (SQL)*.

**state** An indication associated with an icon, color, and severity level of the status of a managed object at any particular point in time. The five predefined states that each managed object can reflect are:

- Unknown
- Critical
- Warning
- Not Monitored

You can customize the default colors and add new states as needed.

**status** The TRUE or FALSE condition of a situation assigned to a managed object.

**Structured Query Language (SQL)** An industry-standard language for creating, updating and querying relational database management systems.

**System Network Architecture (SNA)** An IBM communications network protocol that connects systems and programs under any operating system image and allows them to participate in distributed processing.

**system administrator** CandleNet Portal users who have full access to data, full authority to product functions, and who can authorize and establish access and privileges for other users. By default, the first user of CandleNet Portal is a system administrator.

**table** A construction that holds the data returned from an agent when the agent returns data to a CMS in response to a request. It has a one-to-one correspondence to the agent it represents.

**TCP/IP** See *Transmission Control Protocol/Internet Protocol (TCP/IP)*.
**template**  A model the developer uses to create managed objects. Every managed object you create inherits the characteristics and behaviors of its template.

**Transmission Control Protocol/Internet Protocol (TCP/IP)**. An open, highly portable communications protocol. TCP provides transport protocol functions which ensure that the total number of bytes sent is received correctly at the other end. IP provides the routing mechanism.

**type of managed system**  An operating system, subsystem, or application system type that a CT agent is monitoring. Situation attributes are restricted to a specific managed system type.

1. Details
2. Events
3. Graphic
4. Historical
5. Icons
6. Settings

Not all objects have every view.

**Web services**  A business and technology term encompassing the possibility of openly working with other businesses, developers, and programs through publicly-available open APIs.

**workspace**  A collection of panels (views) in CandleNet Portal that represent system and application conditions.

**value**  A predicate function that uses the raw value of an attribute. A value can be a number, text string, attribute, or modified attribute. Use this function with all relational operators.

**variable**  A symbol or name that stands for a value. Variables can represent numeric values, characters, character strings, or memory addresses. Also see literal.

**view**  A way of looking at information about an object. Each view displays information in a different format. CandleNet Portal has the following views:
access control list
ACL
   see access control list
address translation  37
Adobe portable document format  14
AF/Remote Alert Adapter
   configuring  146
   prerequisites  48
affinities  67
agents  27, 28
   configuring  108, 145
   default configuration  103
   platforms  29, 35, 47
   prerequisites  46, 48
   types  29
Alert Adapters  29
Alert Emitters  29
Alert Managers  29
API Server Data Provider  188
authorizing users for OMEGAMON XE for
   WebSphere MQ  63

BEA WebLogic Server monitoring agent
   prerequisites  48
browser mode  28, 32

Candle Command Center for MQSeries
   Configuration, renamed  21
Candle Command Center for MQSeries,
   renamed  21
Candle Management Server  27, 29
   communications settings  95, 99
   configuring  94, 133
   hub
   enabling security  121
   name
      where to find  144
   naming conventions  30
   platforms  27, 29, 34
   prerequisites  40
   remote  30
   seeding  97
   seeding error  171  144
   version  21, 44
Candle Management Workstation  27
   OMEGAVIEW Zoom  43
   platforms  35
   prerequisites  41
   starting  112, 114
   version  44
Candle System Backup and Restore
   Utility  139
      upgrading from previous versions  141
Candle Web site  13, 18
CandleNet Portal  26, 28
   compatible Candle products  19, 32
   components  32
   order of component installations  36
   platforms  43
   version  21
CandleNet Portal Browser Client  28, 32
   platforms  35
   software  46
   starting  117
   Web browser  46
CandleNet Portal Desktop Client  28, 32
   hardware  45
   platforms  35
CandleNet Portal Server  26, 32
   configuring  81
   creating database  76
installing Candle products on Windows (version CT350)

database product 23, 46, 70, 76
defining a server interface 85
defining interface 90, 93
hardware 45
Java Runtime Environment 45
platforms 35
user ID 121
Warehouse Proxy 36
CLASSPATH environment variable 117
CMS
see Candle Management Server
CMW
see Candle Management Workstation
COLLECTOR FOR PERFORMANCE batch job 173
communications
prerequisites 44, 47
protocols 81, 94, 104
historical data collection 190
settings for Candle Management Server 95, 99
community name, specifying 200
components
CandleNet Portal 32
OMEGAMON XE 26
order of installation 34
order of installations 34
planning which to install 33
selecting for installation 76
uninstalling 123
configuration
with remote Candle Management Server 31
configuring
AF/Remote Alert Adapter 146
agents 108, 145
Candle Management Server 94, 133
CandleNet Portal Server 81
DB2 Universal Database monitoring agent 160
eBA Solutions monitoring agent 161
Hot Standby 134
Microsoft SQL Server 150
Novell NetWare monitoring agent 166
ODBC data source 119
OMEGAMON XE for WebSphere Integration Brokers 164
OMEGAMON XE for WebSphere MQ Monitoring 162
OMEGAMON XE Web Services 125
verifying 131
Oracle monitoring agent 154
Peregrine ServiceCenter Alert Adapter 167
R/3 monitoring agent 169
Remedy ARS Alert Adapter 178
Sybase monitoring agent 158
Tuxedo monitoring agent 180
advanced settings 184
queue information 183
Universal Agent 185
startup parameters 186
Warehouse Proxy 190
for ODBC connection 191
WebSphere Application Server monitoring agent 197
Windows Management Web Service monitoring agent 204
conventions in documentation 16
creating
CandleNet Portal Server database 76
Customer Service and Satisfaction 18
customer support 18

database product 23, 70, 76
CandleNet Portal Server 46
DB2 UDB
see DB2 Universal Database
DB2 Universal Database 23
installing 56
troubleshooting 59
uninstalling 62
user ID 61
DB2 Universal Database monitoring agent configuring 160
prerequisites 48
db2admin user ID 59, 60
deactivating brokers 68
defining
CandleNet Portal Server interface 85, 90, 93
desktop mode 28, 32
documentation conventions 16
docs related 12
Domain Name Server 44
downloading
Java Runtime Environment 56
functions of OMEGAMON XE 26

G
Gateways 29

H
historical configuration 36
historical data warehousing 190
historical data 69
HOST file 56
hostname 83, 96, 99, 100, 105
hosts file 44
Hot Standby
configuring 134
overview 137
testing 137
upgrading hub Candle Management Server 69
hub Candle Management Server
enabling security 121

I
installer program
starting 75
IP 96, 99, 105
IP address 83, 96, 99, 100, 105
IPPIPE 96, 100, 106, 112
firewalls 37

J
Java Runtime Environment
downloading 56
versions 23, 45, 46
JRE
see Java Runtime Environment

K
KIB_CLEAN=Y 114
Kinregbu.exe program 140
KSAR3PWD.EXE 170
KUMENV defaults 186
Installing Candle Products on Windows (version CT350)

L

literals 16
LU name 83, 96, 99, 106
LU6.2 logmode 83, 96, 100, 106

M

Microsoft Data Engine
  migrating from 57
  not supported 23
Microsoft SQL Server 23
  configuring 150
Microsoft SQL Server monitoring agent
  prerequisites 49
migrated information when upgrading 66
migrating
  from Microsoft Data Engine 57
  preparations 65
monitoring agents 29
MSDE
  see Microsoft Data Engine
MSSQL
  see Microsoft SQL Server

N

naming conventions for Candle Management Server 30
NAT 84
network name 83, 96, 99, 105
NICs, multiple 84
Novell NetWare monitoring agent
  configuring 166
  prerequisites 49

O

ODBC connection
  for Warehouse Proxy 191
ODBC data source
  configuring 119
OMEGAMON DE
  overview 28
OMEGAMON XE
  components 26
  order of installation 34
  functions 26
  overview 26
OMEGAMON XE for WebSphere
  Application Server
    archiving existing historical data 69
OMEGAMON XE for WebSphere Integration
  Brokers
    archiving existing historical data 69
    configuring 164
    deactivating brokers 68
    prerequisites 50
OMEGAMON XE for WebSphere
  InterChange Server
    configuring a data source 201
    configuring the monitoring agent for
    SNMP data collection 199
OMEGAMON XE for WebSphere MQ
  Configuration
    authorizing users 63
    prerequisites 51
OMEGAMON XE for WebSphere MQ
  Integrator, renamed 22
OMEGAMON XE for WebSphere MQ
  Monitoring
    authorizing users 63
    configuring 162
    prerequisites 51
OMEGAMON XE for Windows,
  renamed 22
OMEGAMON XE Web Services
  configuring 125
  verifying 131
  defining hubs 126
  defining users 130
OMEGAVIEW Zoom 43
operating systems
  agents 29, 35, 47
  Candle Management Server 27, 29, 34
  Candle Management Workstation 35
  CandleNet Portal 43
  CandleNet Portal Desktop and Browser
    Clients 35

224 Installing Candle Products on Windows (version CT350)
CandleNet Portal Server 35
renamed 21
Windows 22
Oracle monitoring agent
access to views 156
configuring 154
prerequisites 52
order of component installations 34
CandleNet Portal 36

P

partition file 97, 101
partition name 83, 97, 101, 106
partition-naming strategy 37
password 61
PDF files, adding annotations 15
Peregrine ServiceCenter Alert Adapter
configuring 167
prerequisites 52
planning
upgrade and migration 66
which components to install 33
platforms
agents 29, 35, 47
Candle Management Server 27, 29, 34
Candle Management Workstation 35
CandleNet Portal 43
CandleNet Portal Desktop and Browser
Clients 35
CandleNet Portal Server 35
renamed 21
Windows 22
Poll Interval field 199
port number 83, 96, 99, 100, 105, 106
prerequisites 40
AF/Remote Alert Adapter 48
agents 46
hardware 48
BEA WebLogic Server monitoring
agent 48
Candle Management Server 40
Candle Management Workstation 41
CandleNet Portal 43
CandleNet Portal Browser Client
software 46
CandleNet Portal Desktop Client
hardware 45
CandleNet Portal Server
hardware 45
communications 44, 47
database product 46, 70
DB2 Universal Database monitoring
agent 48
eBA Solutions monitoring agent 49
Java Runtime Environment 45
Microsoft SQL Server monitoring
agent 49
Novell NetWare monitoring agent 49
OMEGAMON XE for WebSphere
Integration Brokers 50
OMEGAMON XE for WebSphere MQ
Configuration 51
OMEGAMON XE for WebSphere MQ
Monitoring 51
Oracle monitoring agent 52
Peregrine ServiceCenter Alert Adapter 52
R/3 monitoring agent 52
Remedy ARS Alert Adapter 52
Sybase monitoring agent 52
Tuxedo monitoring agent 52
Universal Agent 53
Warehouse Proxy 53
Web Pulse monitoring agent 53
WebSphere Application Server monitoring
agent 53
Windows Active Directory Servers
monitoring agent 55
Windows Management Web Service
monitoring agent 55
Windows Servers monitoring agent 55
preserving an existing installation 67
printing problems 14
product support
selecting 76
products

Index 225
renamed 21
selecting 76
products and versions compatible with this
release of CandleNet Portal 19
products compatible with this release of
CandleNet Portal 32

R
R/3 monitoring agent
configuring 169
prerequisites 52
readme file
displaying at end of installation 107
related documents 12
related information 13
Remedy ARS Alert Adapter
configuring 178
prerequisites 52
remote Candle Management Server 30
configuration 31
renamed products or platforms 21
retaining a prior level hub Candle
Management Server 67

S
scope of this book 12
security 121
seeding error 171 144
selecting
components for installation 76
product support 76
products 76
services
enabled 35
rebooting and starting 111
setup.exe installation program
starting 75
silent installations 143
SNA 47, 83, 96, 99, 105, 113, 128
SNMP 189
SNMP Gateways 29
SOAP Server
see OMEGAMON XE Web Services
starting
Candle Management Workstation 112, 114
CandleNet Portal Browser Client 117
installer program 75
services 111
stopping components 68
stopping Lotus Notes server, required 56
Sybase monitoring agent
access to views 158
configuring 158
prerequisites 52

T
TCP/IP 112, 127
TCP/IP network services
configuring for hostname 35
testing
Hot Standby 137
thin client 28
TP name 83, 96, 100, 106
Tuxedo monitoring agent
configuring 180
advanced settings 184
queue information 183
prerequisites 52

U
unattended installations 143
uninstalling
components 123
Universal Agent
configuring 185
startup parameters 186
prerequisites 53
upgrading
Candle System Backup and Restore
Utility 141
hub Candle Management Server
Hot Standby 69
in stages 66

226 Installing Candle Products on Windows (version CT350)
migrated information 66
preparations 65
preserving an existing installation 67
retaining a prior level hub Candle
Management Server 67
stopping components 68
WebSphere Application Server monitoring
agent 68
user ID 151, 155, 164
CandleNet Portal Server 121
R/3 173, 176
Windows 121, 164

V

tables 16
versions of products in this release 19

W

Warehouse Proxy 106
CandleNet Portal Server 36
configuring 190
for ODBC connection 191
firewalls 37
prerequisites 53
Web browser
CandleNet Portal Browser Client 46
Web Pulse monitoring agent
prerequisites 53
Web site, Candle 13, 18
WebSphere Application Server monitoring
agent
configuring 197
prerequisites 53
supplied CD 24
upgrading 68
Windows
platforms 22
user ID 60, 61, 121, 164
Windows Active Directory Servers
monitoring agent
prerequisites 55
Windows logon ID 56
Windows Management Web Service
monitoring agent
configuring 204
prerequisites 55
Windows Servers monitoring agent
prerequisites 55

Z

Zoom feature of OMEGAVIEW 43
Part Number: CT36RNA