



OpenEdge Management and OpenEdge Explorer: Getting Started

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

A (and design), Actional, Actional (and design), Allegrix, Allegrix (and design), Apama, Apama (and Design), Business Empowerment, DataDirect (and design), DataDirect Connect, DataDirect Connect64, DataDirect Technologies, DataDirect XQuery, DataXtend, Dynamic Routing Architecture, EasyAsk, EdgeXtend, Empowerment Center, Fathom, IntelliStream, Neon, Neon New Era of Networks, O (and design), ObjectStore, OpenEdge, PeerDirect, Persistence, POSSENET, Powered by Progress, PowerTier, Progress, Progress DataXtend, Progress Dynamics, Progress Business Empowerment, Progress Empowerment Center, Progress Empowerment Program, Progress OpenEdge, Progress Profiles, Progress Results, Progress Software Developers Network, Progress Sonic, ProVision, PS Select, SequeLink, Shadow, ShadowDirect, Shadow Interface, Shadow Web Interface, SOAPStation, Sonic, Sonic ESB, SonicMQ, Sonic Orchestration Server, Sonic Software (and design), SonicSynergy, SpeedScript, Stylus Studio, Technical Empowerment, WebSpeed, and Your Software, Our Technology—Experience the Connection are registered trademarks of Progress Software Corporation or one of its subsidiaries or affiliates in the U.S. and/or other countries. AccelEvent, Apama Dashboard Studio, Apama Event Manager, Apama Event Modeler, Apama Event Store, AppsAlive, AppServer, ASPen, ASP-in-a-Box, BusinessEdge, Cache-Forward, DataDirect Spy, DataDirect SupportLink, DataDirect XML Converters, Future Proof, Ghost Agents, GVAC, Looking Glass, ObjectCache, ObjectStore Inspector, ObjectStore Performance Expert, Pantero, POSSE, ProDataSet, Progress ESP Event Manager, Progress ESP Event Modeler, Progress Event Engine, Progress RFID, PSE Pro, SectorAlliance, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Sonic Business Integration Suite, Sonic Process Manager, Sonic Collaboration Server, Sonic Continuous Availability Architecture, Sonic Database Service, Sonic Workbench, Sonic XML Server, The Brains Behind BAM, WebClient, Who Makes Progress, and Your World. Your SOA. are trademarks or service marks of Progress Software Corporation or one of its subsidiaries or affiliates in the U.S. and other countries. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Any other trademarks or trade names contained herein are the property of their respective owners.

OpenEdge Management Third Party Acknowledgements:

OpenEdge Management includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation. All rights reserved (Xalan XSLT Processor), Copyright © 1999-2002 The Apache Software Foundation. All rights reserved (Xerces), Copyright © 1999-2000 The Apache Software Foundation. All rights reserved (Xerces), and Copyright © 2000-2002 The Apache Software Foundation. All rights reserved (Jakarta-Oro). The names “Apache,” “Xerces,” “Jakarta-Oro,” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. Products derived from this software may not be called “Apache” or “Jakarta-Oro,” nor may “Apache” or “Jakarta-Oro” appear in their name, without prior written permission of the Apache Software Foundation. For written permission, please contact apache@apache.org. Software distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License agreement that accompanies the product.

OpenEdge Management includes software developed by Sun Microsystems, Inc. Copyright © 2003 Sun Microsystems, Inc. All Rights Reserved. and Copyright © 1994-2006 Sun Microsystems, Inc. All Rights Reserved. Software distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the Licenses for the specific language governing rights and limitations under the License agreement that accompanies each product.

OpenEdge Management includes software Copyright 1994-2000 Sun Microsystems, Inc. All Rights Reserved. -Neither the name of or trademarks of Sun may be used to endorse or promote products including or derived from the Java Software technology without specific prior written permission; and Redistributions of source or binary code must contain the above copyright notice, this notice and the following disclaimers: This software is provided “AS IS,” without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN MICROSYSTEMS, INC. OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

OpenEdge Management includes Sonic and ObjectStore software which include software developed by the ModelObjectsGroup (<http://www.modelobjects.com>). Copyright © 2000-2001 ModelObjects Group. All rights reserved. The name “ModelObjects” must not be used to endorse or promote products derived from the SSC Software without prior written permission. Products derived from the SSC Software may not be called “ModelObjects”, nor may “ModelObjects” appear in their name, without prior written permission. For written permission, please contact djacobs@modelobjects.com.

OpenEdge Management includes Sonic software which includes files that are subject to the Netscape Public License Version 1.1 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/NPL>. Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License. The Original Code is Mozilla Communicator client code, released March 31, 1998. The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by Netscape are Copyright © 1998-1999 Netscape Communications Corporation. All Rights Reserved.

OpenEdge Management contains copyright material licensed from AdventNet, Inc. <http://www.adventnet.com>. All rights to such copyright material rest with AdventNet.

OpenEdge Management includes the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

OpenEdge Management includes Sonic and ObjectStore software which include the JMX Technology from Sun Microsystems, Inc. Use and Distribution is subject to the Sun Community Source License available at <http://sun.com/software/communitysource>.

OpenEdge Management includes software Copyright © 2001-2003 James House. All rights reserved. Software distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License agreement that accompanies the product. This product uses and includes within its distribution, software developed by the Apache Software Foundation (<http://www.apache.org/>).

OpenEdge Management includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

OpenEdge Management includes Sonic software, which includes code licensed from Mort Bay Consulting Pty. Ltd. The Jetty Package is Copyright © 1998 Mort Bay Consulting Pty. Ltd. (Australia) and others..



March 2009

Last updated with new content: Release 10.2A

Product Code: 4496; R10.2A

For the latest documentation updates see the [OpenEdge Product Documentation category](http://www.psdn.com/library/kbcategory.jspa?categoryID=129) on PSDN (<http://www.psdn.com/library/kbcategory.jspa?categoryID=129>).

Contents

Preface	Preface-1
1. Introducing OpenEdge Management and OpenEdge Explorer	1-1
Working with OpenEdge Management	1-2
Understanding OpenEdge Management system architecture.....	1-2
Deploying OpenEdge Management	1-3
Configuring resources on a remote AdminServer	1-6
Configuring remote resources with OpenEdge Explorer.....	1-6
Configuring and monitoring remote resources with OpenEdge Management	1-6
Resources that support remote monitoring	1-7
More about monitoring scripted and managed databases	1-10
Choosing an OpenEdge Management deployment strategy	1-12
Working with OpenEdge Explorer	1-13
2. Setting Up OpenEdge Management or OpenEdge Explorer for the First Time	2-1
Using the management console	2-2
Preparing to set up OpenEdge Management or OpenEdge Explorer	2-3
Completing the initial setup process	2-4
Setting up OpenEdge Explorer	2-4
Setting up OpenEdge Management	2-4
Starting OpenEdge Management or OpenEdge Explorer	2-5
Entering the default user name and password	2-6
Choosing initial configuration options	2-7
Setting initial configurations for OpenEdge Explorer.....	2-7
Setting initial configurations for OpenEdge Management	2-8
Setting up the Getting Started page for OpenEdge Management	2-15
Understanding managed and scripted databases.....	2-15
Defining OpenEdge Management monitors for previously scripted databases	2-15
Defining OpenEdge Management monitoring and trending options for file systems and disks	2-18
Submitting the Getting Started page for OpenEdge Management	2-19

3. Using the Console	3-1
Starting OpenEdge Management or OpenEdge Explorer	3-2
Logging on	3-2
Using the management console	3-4
Viewing the contents of a container	3-5
Accessing functions from the menu bar	3-6
Viewing additional details	3-7
Navigating the console	3-8
Sorting in the console list frame	3-10
Checking resource status	3-11
Changing the console display	3-13
Refreshing the console	3-13
Expanding or collapsing resource categories	3-13
Returning to the previous page in the console	3-14
Displaying a page in a new window	3-14
Accessing Help	3-14
Additional console details	3-15
4. Setting up remote resource monitoring and configuration	4-1
Remote monitoring and configuration requirements	4-2
Setting up for remote monitoring or configuration	4-3
Setting up the first machine	4-3
Setting up the second machine	4-6
Verifying that OpenEdge Management or OpenEdge Explorer can see the remote container	4-7
Remote monitoring configuration utility command-line options	4-8
Disabling remote monitoring	4-9
Uninstalling if remote monitoring is configured	4-10
5. Administering OpenEdge Management and OpenEdge Explorer	5-1
Reviewing the configuration	5-2
Updating licensing information	5-4
Updating configuration options	5-5
Adding users as administrators or operators	5-7
Managing the authorized users list	5-7
Customizing the operator role	5-8
Adding a new user	5-10
Changing passwords and descriptions	5-11
Changing the Admin password	5-11
Deleting users	5-12
Changing configuration settings	5-13
Changing general configuration settings	5-13
Changing OpenEdge Management e-mail alerts settings	5-14
Changing OpenEdge Management resource monitoring settings	5-15
Setting the OpenEdge Management graph cache	5-16
Setting OpenEdge Management user preferences	5-20
Setting the OpenEdge Management page refresh option	5-20
Changing the OpenEdge Management SNMP Adapter settings	5-22
Setting OpenEdge Management resource monitor defaults	5-23
Using the command-line interface	5-25
Using the OpenEdge Management environment window	5-26
Starting, querying, and stopping from the command line	5-26
Dumping, backing up, and restoring the configuration database	5-27
Accessing command-line help	5-29
Setting the log level for the AdminServer log file	5-30

6. Setting up Secure Communications.	6-1
Transferring data securely with the HTTPS protocol	6-2
Using the demo certificate or your own certificate	6-2
Understanding common SSL terminology	6-3
Getting started: using the demo certificate	6-5
Configuration update errors or warnings.	6-5
Identifying trusted clients.	6-5
Reconnecting after updates	6-6
Changing Web server settings	6-7
Using advanced HTTP and HTTPS options with the Web server	6-8
Changing OpenEdge Management Trend Database settings	6-10
Using advanced HTTPS options when trending remotely.	6-11
Using the procertm utility.	6-13
Using SSL	6-16
Detecting a certificate from an unknown Certificate Authority.	6-16
Using your own certificate	6-19
Using the keytool utility	6-20
Step 1: Creating a keystore repository	6-20
Step 2: Generating a certificate request	6-23
Step 3: Importing the CA Certificate	6-24
Step 4: Importing the signed certificate to the store	6-25
Index	Index-1

Figures

Figure 1-1:	Single-host OpenEdge Management installation	1-3
Figure 1-2:	Multiple-host OpenEdge Management installation	1-4
Figure 1-3:	Multiple-host installation with shared OpenEdge Management Trend Database 1-5	
Figure 1-4:	Remote monitoring of resources on one machine	1-8
Figure 1-5:	Monitoring of resources on two machines	1-9
Figure 1-6:	Monitoring scripted databases on another machine	1-11
Figure 2-1:	Autostart OpenEdge Management option	2-9
Figure 2-2:	Trend database location	2-9
Figure 2-3:	SNMP Adapter settings	2-13
Figure 2-4:	Defining monitors for external OpenEdge databases	2-16
Figure 2-5:	Database Migration Utility	2-16
Figure 2-6:	Defining monitors for file systems and disks	2-18
Figure 2-7:	OpenEdge Management Configuration success	2-19
Figure 3-1:	OpenEdge Management Resources page	3-5
Figure 3-2:	Container view in the detail frame	3-5
Figure 3-3:	OpenEdge Management user name details	3-7
Figure 3-4:	Collapsed Library categories in OpenEdge Management list frame ...	3-8
Figure 3-5:	Expanded Library categories in OpenEdge Management list frame ...	3-9
Figure 3-6:	Email actions in OpenEdge Management Library→ Actions	3-9
Figure 3-7:	OpenEdge Management Actions category	3-10
Figure 3-8:	Resources sorted by status	3-10
Figure 3-9:	OpenEdge Management Resource statuses	3-11
Figure 3-10:	OpenEdge Explorer Resource statuses	3-11
Figure 5-1:	Options in OpenEdge Management list frame	5-5
Figure 5-2:	Options in OpenEdge Explorer list frame	5-5
Figure 5-3:	Refresh Pages page	5-20
Figure 5-4:	Set OpenEdge Management Environment window	5-26
Figure 5-5:	Command-line help for -stop	5-29
Figure 6-1:	Security Alert dialog in Internet Explorer	6-16
Figure 6-2:	Certificate details	6-17
Figure 6-3:	Creating a keystore	6-22

Tables

Table 3–1:	Resource status legend	3–11
Table 3–2:	Console control bar icons	3–13
Table 4–1:	Remote Monitoring Configuration Utility options	4–8
Table 4–2:	Additional Remote Monitoring Configuration Utility options	4–8
Table 5–1:	Configuration option availability	5–5
Table 5–2:	Command-line options for starting and stopping	5–26
Table 6–1:	Distinguished name string components	6–21

Preface

This Preface contains the following sections:

- [Purpose](#)
- [Audience](#)
- [Organization](#)
- [Using this manual](#)
- [Typographical conventions](#)
- [Examples of syntax descriptions](#)
- [OpenEdge messages](#)

Purpose

This manual describes how to get started using OpenEdge® Management and OpenEdge Explorer.

Audience

This manual is intended for users and administrators of OpenEdge Management and OpenEdge Explorer.

Organization

[Chapter 1, “Introducing OpenEdge Management and OpenEdge Explorer”](#)

Provides an introduction to working with OpenEdge Management and OpenEdge Explorer. Included are details about OpenEdge Management architecture, deployment options, and remote monitoring. Also provided is a feature comparison between OpenEdge Management and OpenEdge Explorer.

[Chapter 2, “Setting Up OpenEdge Management or OpenEdge Explorer for the First Time”](#)

Describes how to select initial configuration options and how to start OpenEdge Management or OpenEdge Explorer.

[Chapter 3, “Using the Console”](#)

Describes the management console, common to both OpenEdge Management and OpenEdge Explorer.

[Chapter 4, “Setting up remote resource monitoring and configuration”](#)

Provides information about how to set up resources for remote monitoring by OpenEdge Management and remote configuration by OpenEdge Explorer.

[Chapter 5, “Administering OpenEdge Management and OpenEdge Explorer”](#)

Provides information about administering OpenEdge Management and OpenEdge Explorer after installation: reviewing or changing configuration options, setting up users as operators or administrators, setting other preferences if applicable, and using the command-line interface.

[Chapter 6, “Setting up Secure Communications”](#)

Describes how to set up OpenEdge Management to use the HTTPS protocol with the OpenEdge Management Trend Database (when trending to a remote database) and how to set up both OpenEdge Management and OpenEdge Explorer to use the HTTPS protocol with the Web server. The chapter explains the process of creating a keystore; requesting, obtaining, and then importing a signed certificate; and then adding the signed certificate to the keystore.

Using this manual

OpenEdge provides a special purpose programming language for building business applications. In the documentation, the formal name for this language is *ABL (Advanced Business Language)*. With few exceptions, all keywords of the language appear in all UPPERCASE, using a font that is appropriate to the context. All other alphabetic language content appears in mixed case.

References to ABL compiler and run-time features

ABL is both a compiled and interpreted language that executes in a run-time engine that the documentation refers to as the *ABL Virtual Machine (AVM)*. When documentation refers to ABL source code compilation, it specifies *ABL* or *the compiler* as the actor that manages compile-time features of the language. When documentation refers to run-time behavior in an executing ABL program, it specifies *the AVM* as the actor that manages the specified run-time behavior in the program.

For example, these sentences refer to the ABL compiler's allowance for parameter passing and the AVM's possible response to that parameter passing at run time: "ABL allows you to pass a dynamic temp-table handle as a static temp-table parameter of a method. However, if at run time the passed dynamic temp-table schema does not match the schema of the static temp-table parameter, the AVM raises an error." The following sentence refers to run-time actions that the AVM can perform using a particular ABL feature: "The ABL socket object handle allows the AVM to connect with other ABL and non-ABL sessions using TCP/IP sockets."

References to ABL data types



ABL provides built-in data types, pre-defined class data types, and user-defined class data types. References to built-in data types follow these rules:

- Like most other keywords, references to specific built-in data types appear in all UPPERCASE, using a font that is appropriate to the context. No uppercase reference ever includes or implies any data type other than itself.
- Wherever *integer* appears, this is a reference to the INTEGER or INT64 data type.
- Wherever *decimal* appears, this is a reference to the DECIMAL data type.
- Wherever *numeric* appears, this is a reference to the INTEGER, INT64, or DECIMAL data type.

References to pre-defined class data types appear in mixed case with initial caps, for example, `Progress.Lang.Object`. References to user-defined class data types appear in mixed case, as specified for a given application example.

Typographical conventions

This manual uses the following typographical conventions:

Convention	Description
Bold	Bold typeface indicates commands or characters the user types, provides emphasis, or the names of user interface elements.
<i>Italic</i>	Italic typeface indicates the title of a document, or signifies new terms.
SMALL, BOLD CAPITAL LETTERS	Small, bold capital letters indicate OpenEdge key functions and generic keyboard keys; for example, GET and CTRL .
KEY1+KEY2	A plus sign between key names indicates a simultaneous key sequence: you press and hold down the first key while pressing the second key. For example, CTRL+X .
KEY1 KEY2	A space between key names indicates a sequential key sequence: you press and release the first key, then press another key. For example, ESCAPE H .
Syntax:	
Fixed width	A fixed-width font is used in syntax statements, code examples, system output, and filenames.
<i>Fixed-width italics</i>	Fixed-width italics indicate variables in syntax statements.
Fixed-width bold	Fixed-width bold indicates variables with special emphasis.
UPPERCASE fixed width	Uppercase words are ABL keywords. Although these are always shown in uppercase, you can type them in either uppercase or lowercase in a procedure.
	This icon (three arrows) introduces a multi-step procedure.
	This icon (one arrow) introduces a single-step procedure.
Period (.) or colon (:)	All statements except DO, FOR, FUNCTION, PROCEDURE, and REPEAT end with a period. DO, FOR, FUNCTION, PROCEDURE, and REPEAT statements can end with either a period or a colon.
[]	Large brackets indicate the items within them are optional.
[]	Small brackets are part of the ABL.
{ }	Large braces indicate the items within them are required. They are used to simplify complex syntax diagrams.
{ }	Small braces are part of the ABL. For example, a called external procedure must use braces when referencing arguments passed by a calling procedure.

Convention	Description
	A vertical bar indicates a choice.
...	Ellipses indicate repetition: you can choose one or more of the preceding items.

Examples of syntax descriptions

In this example, `ACCUM` is a keyword, and *aggregate* and *expression* are variables:

Syntax

```
ACCUM aggregate expression
```

`FOR` is one of the statements that can end with either a period or a colon, as in this example:

```
FOR EACH Customer NO-LOCK:
  DISPLAY Customer.Name.
END.
```

In this example, `STREAM` *stream*, `UNLESS-HIDDEN`, and `NO-ERROR` are optional:

Syntax

```
DISPLAY [ STREAM stream ] [ UNLESS-HIDDEN ] [ NO-ERROR ]
```

In this example, the outer (small) brackets are part of the language, and the inner (large) brackets denote an optional item:

Syntax

```
INITIAL [ constant [ , constant ] ]
```

A called external procedure must use braces when referencing compile-time arguments passed by a calling procedure, as shown in this example:

Syntax

```
{ &argument-name }
```

In this example, `EACH`, `FIRST`, and `LAST` are optional, but you can choose only one of them:

Syntax

```
PRESELECT [ EACH | FIRST | LAST ] record-phrase
```

In this example, you must include two expressions, and optionally you can include more. Multiple expressions are separated by commas:

Syntax

```
MAXIMUM ( expression , expression [ , expression ] ... )
```

In this example, you must specify MESSAGE and at least one *expression* or SKIP [(*n*)], and any number of additional *expression* or SKIP [(*n*)] is allowed:

Syntax

```
MESSAGE { expression | SKIP [ ( n ) ] } ...
```

In this example, you must specify { *include-file*, then optionally any number of *argument* or *&argument-name* = "*argument-value*", and then terminate with }:

Syntax

```
{ include-file  
  [ argument | &argument-name = "argument-value" ] ... }
```

Long syntax descriptions split across lines

Some syntax descriptions are too long to fit on one line. When syntax descriptions are split across multiple lines, groups of optional and groups of required items are kept together in the required order.

In this example, WITH is followed by six optional items:

Syntax

```
WITH [ ACCUM max-length ] [ expression DOWN ]  
    [ CENTERED ] [ n COLUMNS ] [ SIDE-LABELS ]  
    [ STREAM-IO ]
```

Complex syntax descriptions with both required and optional elements

Some syntax descriptions are too complex to distinguish required and optional elements by bracketing only the optional elements. For such syntax, the descriptions include both braces (for required elements) and brackets (for optional elements).

In this example, ASSIGN requires either one or more *field* entries or one *record*. Options available with *field* or *record* are grouped with braces and brackets:

Syntax

```
ASSIGN  { [ FRAME frame ] { field [ = expression ] }
        [ WHEN expression ] } ...
        | { record [ EXCEPT field ... ] }
```

OpenEdge messages

OpenEdge displays several types of messages to inform you of routine and unusual occurrences:

- **Execution messages** inform you of errors encountered while OpenEdge is running a procedure; for example, if OpenEdge cannot find a record with a specified index field value.
- **Compile messages** inform you of errors found while OpenEdge is reading and analyzing a procedure before running it; for example, if a procedure references a table name that is not defined in the database.
- **Startup messages** inform you of unusual conditions detected while OpenEdge is getting ready to execute; for example, if you entered an invalid startup parameter.

After displaying a message, OpenEdge proceeds in one of several ways:

- Continues execution, subject to the error-processing actions that you specify or that are assumed as part of the procedure. This is the most common action taken after execution messages.
- Returns to the Procedure Editor, so you can correct an error in a procedure. This is the usual action taken after compiler messages.
- Halts processing of a procedure and returns immediately to the Procedure Editor. This does not happen often.
- Terminates the current session.

OpenEdge messages end with a message number in parentheses. In this example, the message number is 200:

```
** Unknown table name table. (200)
```

If you encounter an error that terminates OpenEdge, note the message number before restarting.

Obtaining more information about OpenEdge messages

In Windows platforms, use OpenEdge online help to obtain more information about OpenEdge messages. Many OpenEdge tools include the following Help menu options to provide information about messages:

- Choose **Help**→**Recent Messages** to display detailed descriptions of the most recent OpenEdge message and all other messages returned in the current session.
- Choose **Help**→**Messages** and then type the message number to display a description of a specific OpenEdge message.
- In the Procedure Editor, press the **HELP** key or **F1**.

On UNIX platforms, use the OpenEdge pro command to start a single-user mode character OpenEdge client session and view a brief description of a message by providing its number.



To use the pro command to obtain a message description by message number:

1. Start the Procedure Editor:

```
OpenEdge-install-dir/bin/pro
```

2. Press **F3** to access the menu bar, then choose **Help**→**Messages**.
3. Type the message number and press **ENTER**. Details about that message number appear.
4. Press **F4** to close the message, press **F3** to access the Procedure Editor menu, and choose **File**→**Exit**.

Introducing OpenEdge Management and OpenEdge Explorer

OpenEdge Management helps you to monitor the availability and performance of supported OpenEdge resources. You can also set configuration properties and view the status and log file data for certain resources.

OpenEdge Explorer provides the functionality currently available in Progress Explorer, but within the OpenEdge Management console, which runs in a Web browser. You can set resource configuration properties, start or stop, and view the status of log files for various OpenEdge resources. You can use OpenEdge Explorer either in the console without OpenEdge Management, or with OpenEdge Management if you have OpenEdge Management installed.

The following sections provide information to help you get started using OpenEdge Management and OpenEdge Explorer:

- [Working with OpenEdge Management](#)
- [Configuring resources on a remote AdminServer](#)
- [Choosing an OpenEdge Management deployment strategy](#)
- [Working with OpenEdge Explorer](#)

Working with OpenEdge Management

As you work with OpenEdge Management, it is helpful to understand its architecture and deployment options, as described in the following sections:

- [Understanding OpenEdge Management system architecture](#)
- [Deploying OpenEdge Management](#)

Understanding OpenEdge Management system architecture

OpenEdge Management consists of the following parts:

- A Web-based management console, which provides a central location for viewing and configuring resources that are monitored by OpenEdge Management
- Components to monitor supported OpenEdge resources
- A database called the OpenEdge Management Trend Database that stores all data collected by agents for use in reporting
- The OpenEdge Management process, running as a thread in the AdminServer
- The PsePro (fathom.odt) database, which stores monitoring plans and resource definitions
- OpenEdge Explorer, which allows you to set or modify configuration properties for certain resources, as well as to view their status and log file data. OpenEdge Explorer provides the same functionality as Progress Explorer, but from within a graphical user interface console on a Web browser, allowing direct access from an installation on UNIX.

Note: Progress Explorer continues to be available in OpenEdge Releases 10.1C03 or later, and 10.2A01; it does not, however, run on Windows 2008. Therefore, if you are running OpenEdge in the Windows 2008 platform, you can use OpenEdge Explorer, which provides the same features as Progress Explorer but runs in a Web browser.

Deploying OpenEdge Management

You can deploy OpenEdge Management by installing it on:

- A single host
- Multiple hosts

Deploying OpenEdge Management on a single host

The simplest way to deploy OpenEdge Management is to install it on a single host where only local resources are to be monitored. A local resource is a system, network, file, or OpenEdge server resource that exists on the same host as OpenEdge Management.

A database on the same host as OpenEdge Management is a *managed database*, provided that the database is recognized by the AdminServer also running OpenEdge Management. OpenEdge Management can also monitor scripted databases, which are not under AdminServer control, whether on the same host as OpenEdge Management or on other machines.

In the scenario shown in [Figure 1–1](#), all components of OpenEdge Management exist on the same host, Machine A.

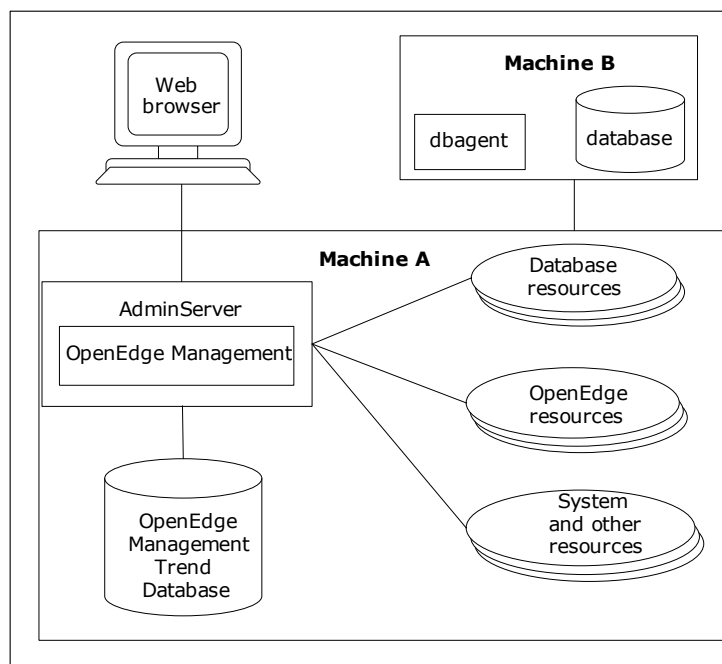


Figure 1–1: Single-host OpenEdge Management installation

OpenEdge Management is running inside the AdminServer on Machine A. The OpenEdge Management Trend Database and all monitored resources are also on Machine A.

On Machine B are a dbagent and a scripted database, which is running outside of the AdminServer on Machine A.

Deploying OpenEdge Management on multiple hosts

A slightly more complex way to deploy OpenEdge Management is to install it on each host where resources are to be monitored. In this scenario, each install of OpenEdge Management will monitor only those resources local to the host on which it is installed. Each install of OpenEdge Management uses its own OpenEdge Management Trend Database, as illustrated in Figure 1–2.

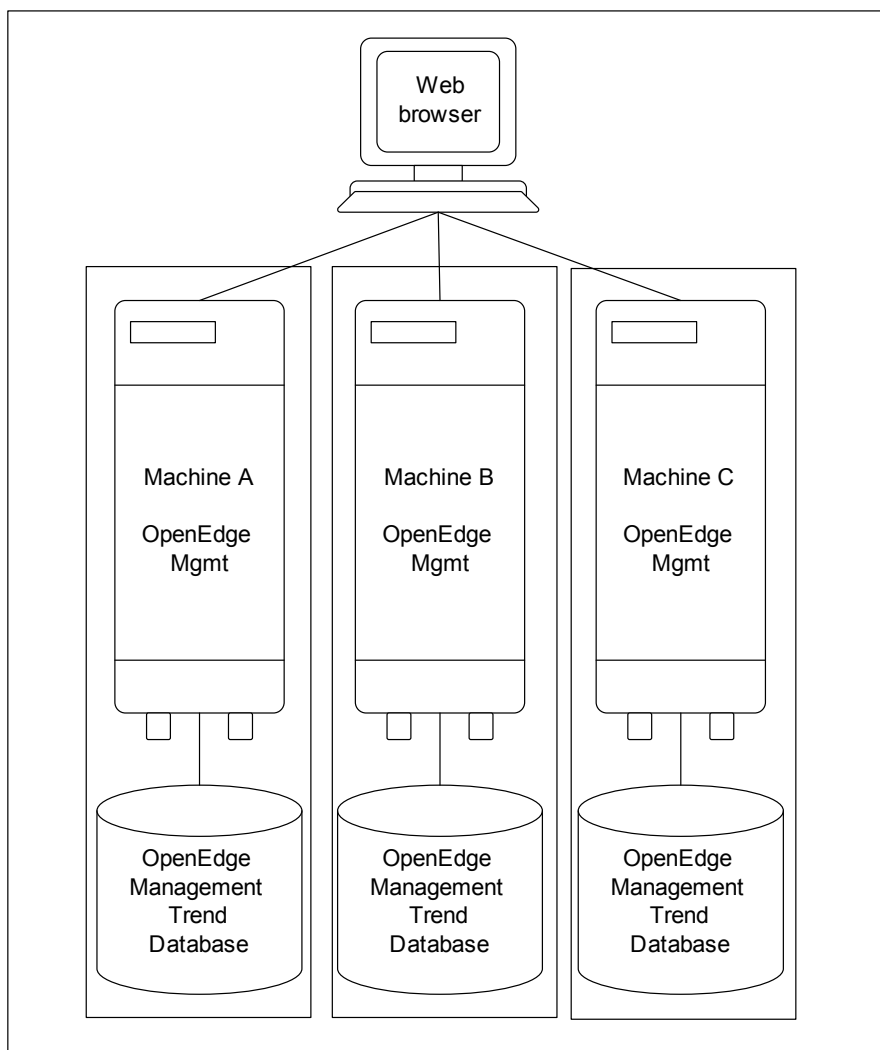


Figure 1–2: Multiple-host OpenEdge Management installation

Figure 1–2 illustrates three separate installs of OpenEdge Management, one each on Machine A, B, and C. Each install uses its own OpenEdge Management Trend Database, and each install is monitoring only local resources. A possible negative aspect of the deployment shown in Figure 1–2 is that you have multiple OpenEdge Management Trend Databases.

As an alternative, you could configure each install of OpenEdge Management to use a shared OpenEdge Management Trend Database, as shown in [Figure 1–3](#).

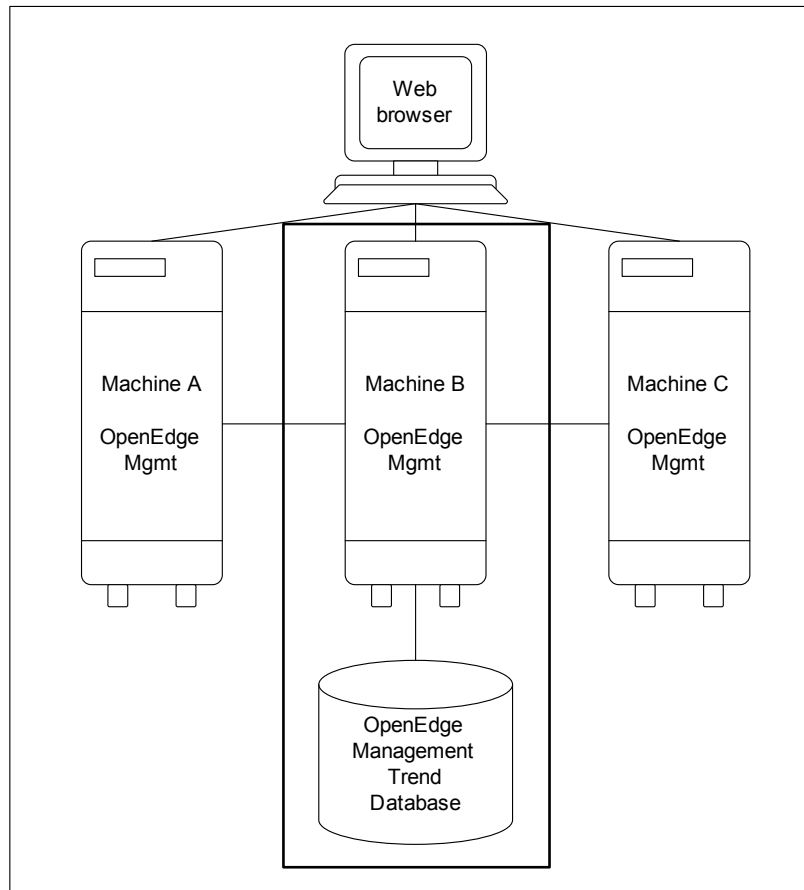


Figure 1–3: Multiple-host installation with shared OpenEdge Management Trend Database

[Figure 1–3](#) illustrates three separate installs of OpenEdge Management, one each on Machine A, B, and C. Each install is sharing a single OpenEdge Management Trend Database on Machine B, and each install is monitoring only local resources.

In the deployments shown in [Figure 1–2](#) and [Figure 1–3](#), there is a separate install of OpenEdge Management on each host where resources are to be monitored. Neither takes advantage of OpenEdge Management's remote resource monitoring.

Configuring resources on a remote AdminServer

You can use OpenEdge Explorer to set configuration properties for resources running on a remote AdminServer. If you have OpenEdge Management installed, you can also monitor remote resources.

To do this, you identify the resource's container. A *container* represents a named instance of an AdminServer that either is running OpenEdge Management or OpenEdge Explorer or has been configured to be monitored by OpenEdge Management. There is typically a one-to-one relationship between the host name and the container name, unless there are multiple AdminServers running OpenEdge Management or OpenEdge Explorer on the same host.

For more details about configuring and monitoring remote resources, see [Chapter 4, “Setting up remote resource monitoring and configuration.”](#)

Configuring remote resources with OpenEdge Explorer

When you add a resource to OpenEdge Explorer, you identify the location of the resource: in a local container or remote container.

You can set or modify configuration properties for a resource that is either local or remote, provided that:

- An AdminServer is available and running on the remote resource's host machine.
- You have run the Remote Monitoring Configuration Utility (fmconfig).

Configuring and monitoring remote resources with OpenEdge Management

With OpenEdge Explorer, you can configure resources running on a remote machine. With OpenEdge Management, you can configure and also monitor resources on a remote machine where OpenEdge Management is not installed.

This provides numerous benefits, the greatest of which is the ability to view the status of all your resources and alerts through a single OpenEdge Management console. Remote resource monitoring also simplifies deployment because OpenEdge Management need not be installed on each host where the resources are to be monitored.

For monitoring resources remotely, OpenEdge Management uses the SonicMQ broker, which is a very fast and reliable messaging system.

OpenEdge Management requires that you have an AdminServer running on the remote host where resources are to be monitored. Additionally, both OpenEdge Management on the local host and the AdminServer on the remote host must be configured using the OpenEdge Management Remote Monitoring Configuration Utility (fmconfig), as described in [Chapter 4, “Setting up remote resource monitoring and configuration.”](#)

Resources that support remote monitoring

You can deploy OpenEdge Management to monitor the following remote resources:

- **Databases** — Progress Version 9.1E04 (with the latest Hotfix) or later, OpenEdge Releases 10.0B, 10.1x, and 10.2x. OpenEdge Management uses the dbagent to monitor all database resources.
- **OpenEdge servers** — AppServer, WebSpeed, and NameServer.
- **System resources** — CPU, memory, disk, and file system.

Figure 1–4 shows a deployment in which OpenEdge Management is monitoring resources on a remote machine.

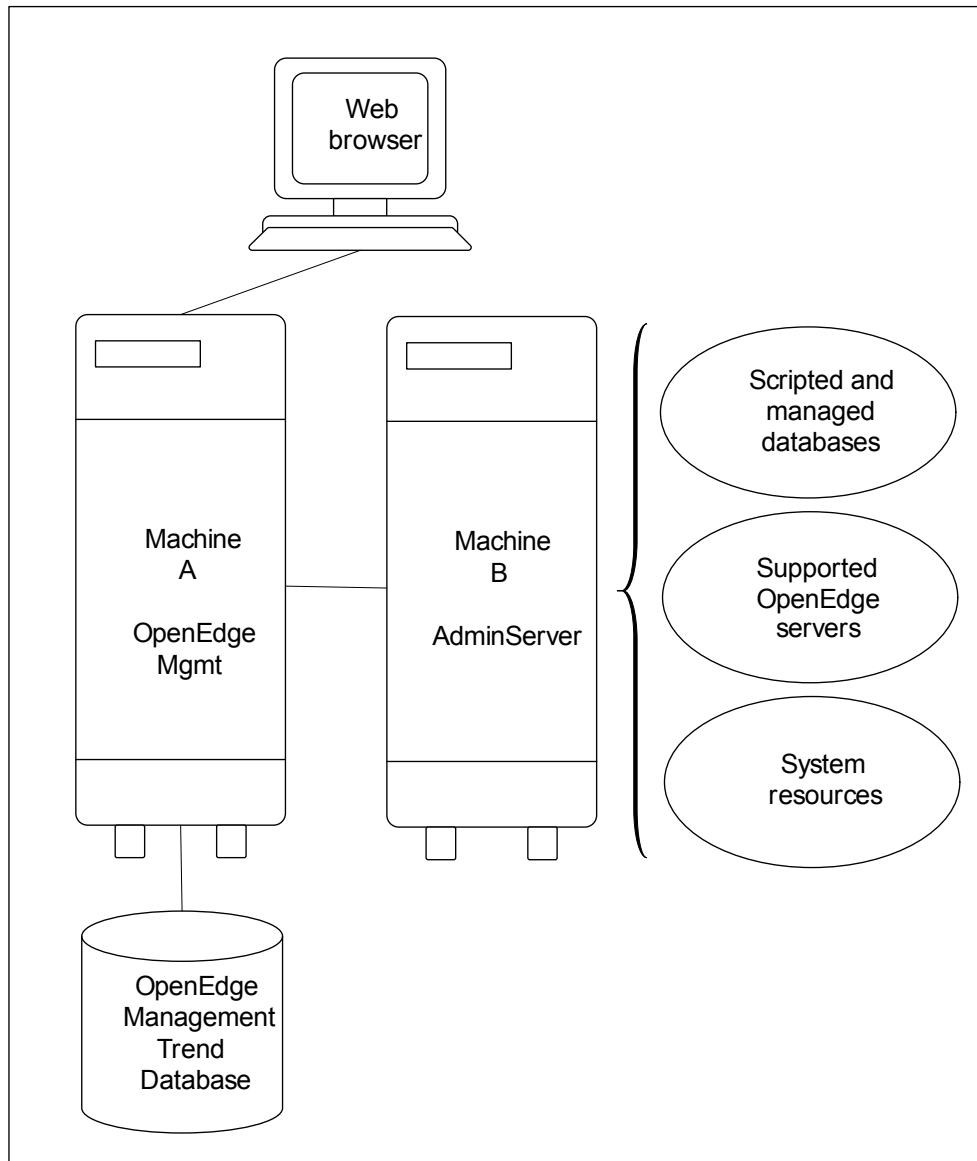


Figure 1–4: Remote monitoring of resources on one machine

The illustration shown in Figure 1–4 presents a single installation of OpenEdge Management on Machine A, which is monitoring the following resources on Machine B:

- **Scripted and managed databases** — A *scripted database* is a database whose broker cannot be managed by the AdminServer in any way. A *managed database* is a database that the AdminServer recognizes and manages.
- **Supported OpenEdge servers** — A supported OpenEdge server can be an AppServer, a NameServer, or a WebSpeed Transaction Server.
- **System resources** — System resources are CPU, disk, memory, and file system.

You can extend the deployment model shown in [Figure 1–4](#) to multiple hosts, as shown in [Figure 1–5](#).

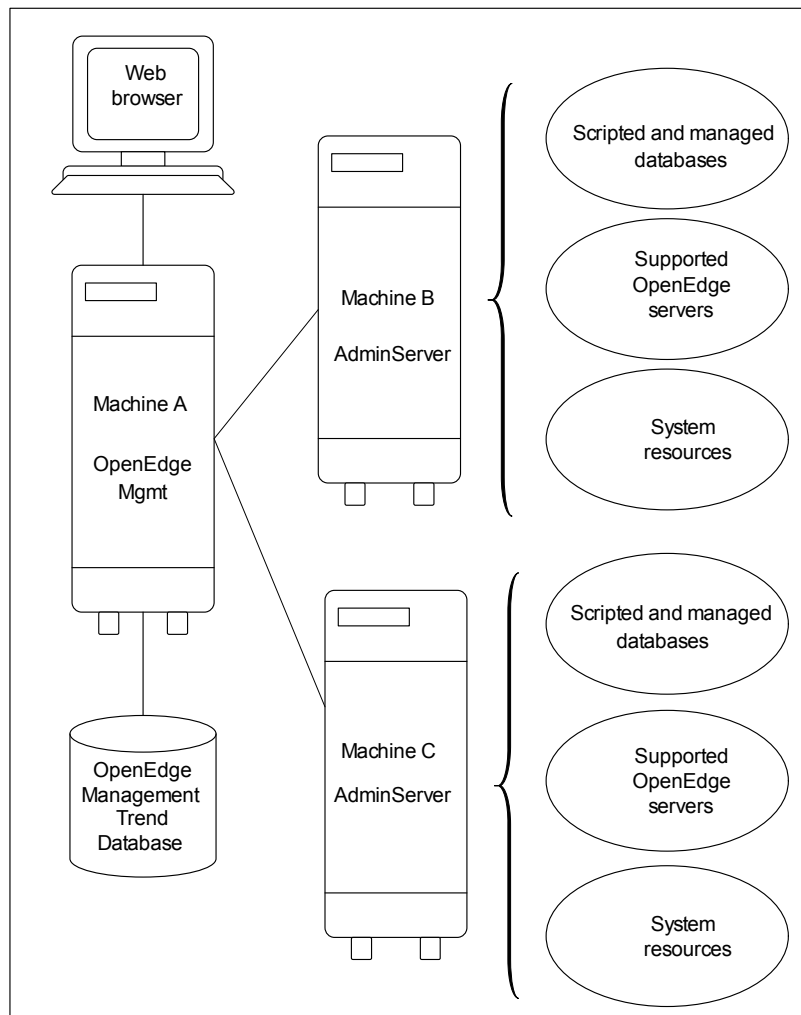


Figure 1–5: Monitoring of resources on two machines

The illustration shown in [Figure 1–5](#) presents a single install of OpenEdge Management on Machine A, which is monitoring databases (scripted and managed), supported OpenEdge servers, and system resources on Machine B and Machine C.

The number of remote hosts you monitor from the OpenEdge Management install on Machine A is limited only by the power of Machine A, the number of remote resources monitored, and the frequency with which they are polled.

This deployment model is very effective in that it allows you to install OpenEdge Management on a non-production machine—that is, a machine other than one where your OpenEdge or other critical application resources run. The benefit of this deployment model is that it minimizes the impact of using OpenEdge Management to monitor your production machines.

More about monitoring scripted and managed databases

You can configure OpenEdge Management to monitor both scripted and managed databases. Using the dbagent, OpenEdge Management can monitor a database that is running on the same host as OpenEdge Management or on a different host, regardless of whether the database is managed (recognized by the AdminServer) or scripted (not under AdminServer control).

Currently OpenEdge Management can monitor:

- A managed database (that OpenEdge Management has autodiscovered) running under a remote-enabled AdminServer.
- A scripted database that is running through a remote-enabled AdminServer.
- A scripted database that is running outside of the AdminServer in which OpenEdge Management is running. In this case, the AdminServer is not remote-enabled.

Monitoring a scripted database through a remote-enabled AdminServer

When OpenEdge Management monitors a scripted database that is running through a remote-enabled AdminServer, the scripted database communicates directly with that AdminServer, which then uses the Sonic infrastructure to communicate with OpenEdge Management. The advantage to setting up monitoring in this way is that the scripted database can connect right into an AdminServer that is remote-enabled for all resources; it is not necessary for the dbagent to open a separate port into OpenEdge Management.

You configure OpenEdge Management and the remote-enabled AdminServer by using the OpenEdge Management Remote Monitoring Configuration Utility. For details, see [Chapter 4, “Setting up remote resource monitoring and configuration.”](#)

Monitoring a managed database through a remote-enabled AdminServer

OpenEdge Management can monitor a managed database that has been autodiscovered running under a remote-enabled AdminServer.

Monitoring scripted databases outside the AdminServer running OpenEdge Management

OpenEdge Management can monitor scripted databases that are running outside of the AdminServer in which OpenEdge Management is running. In order to monitor a database that is scripted, you must create a remote database resource.

To monitor a scripted database once you migrate it, OpenEdge Management uses the dbagent installed with your OpenEdge database. This deployment is shown in [Figure 1–6](#).

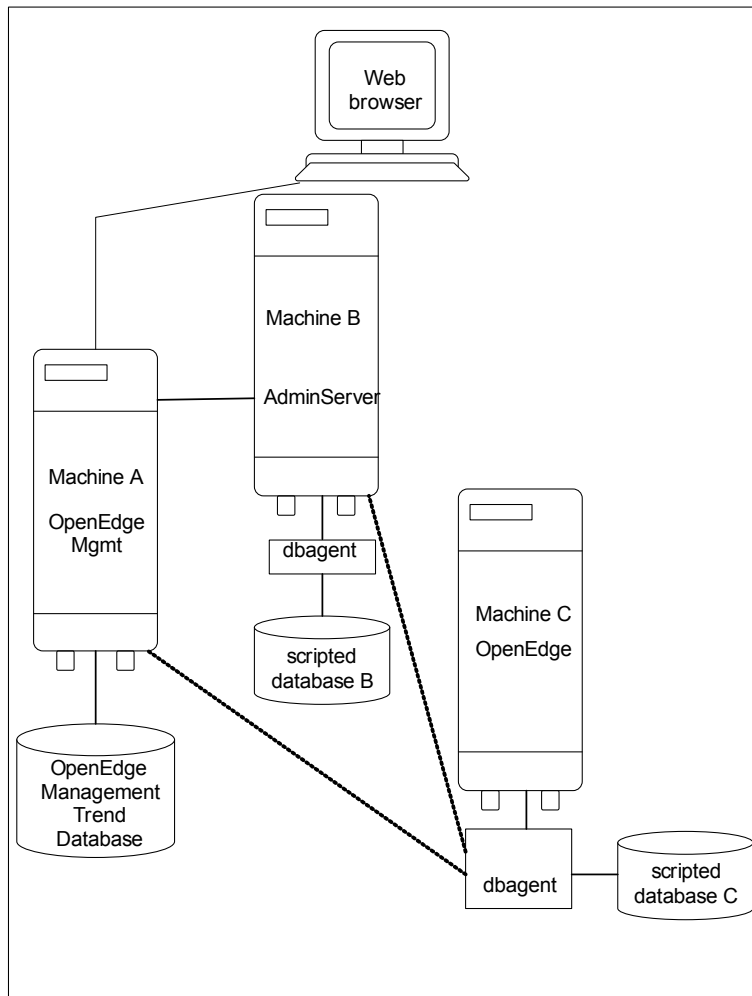


Figure 1–6: Monitoring scripted databases on another machine

Consider you have database B running on Machine B and database C running on Machine C. It would make sense for the dbagent on Machine B to connect to the AdminServer on Machine B, since doing so would provide the most versatility (for the log file viewer and increased performance, for example).

Since there is no AdminServer running on Machine C, the dbagent can decide whether to connect to the AdminServer on Machine A or Machine B.

See *OpenEdge Management: Database Management* for more information.

Choosing an OpenEdge Management deployment strategy

The best strategy for deploying OpenEdge Management depends on your requirements. There is no one strategy that works best for all environments. You may find that a combination of approaches works best for your needs. Some factors to consider when deciding on a deployment strategy include:

- Do you want to minimize the impact of OpenEdge Management on your production machines? If so, you should consider installing OpenEdge Management on a machine dedicated to running OpenEdge Management and use OpenEdge Management remote resource monitoring capabilities.
- Do you want to view the status of all your resources from a single OpenEdge Management console? If so, you should consider using OpenEdge Management's remote resource monitoring capabilities.
- Do you need to run jobs on remote machines? If so, you'll need to install OpenEdge Management on each machine where jobs are to be run. OpenEdge Management does not provide the ability to start a job on a remote machine.
- Will you be monitoring resources outside of your network firewall? If so, you will need to perform the appropriate tunneling to allow OpenEdge Management through the firewall.

The default port for monitoring remote OpenEdge and system resources is 6835.

For more information about using OpenEdge Management with resources being managed by a remote AdminServer, see [Chapter 4, “Setting up remote resource monitoring and configuration.”](#)

Working with OpenEdge Explorer

OpenEdge Explorer provides the functionality currently available in Progress Explorer, but within the OpenEdge Management console running in a Web browser, enabling you to set configuration properties, start or stop, and view the status or log files for various OpenEdge resources.

For more information, see *[OpenEdge Management and OpenEdge Explorer: Configuration](#)*.

Setting Up OpenEdge Management or OpenEdge Explorer for the First Time

This chapter introduces the components of OpenEdge Management and OpenEdge Explorer and describes how to set up each one, as outlined in the following sections:

- [Using the management console](#)
- [Preparing to set up OpenEdge Management or OpenEdge Explorer](#)
- [Completing the initial setup process](#)
- [Starting OpenEdge Management or OpenEdge Explorer](#)
- [Choosing initial configuration options](#)
- [Setting up the Getting Started page for OpenEdge Management](#)

Note that it is not necessary to set up OpenEdge Explorer if you have installed OpenEdge Management. The setup of OpenEdge Management is all that is required.

Using the management console

OpenEdge Explorer uses the same console as OpenEdge Management. The only difference you find when using OpenEdge Explorer is that any OpenEdge Management-specific functionality is disabled in the console when you do not have the required OpenEdge Management license.

For a complete description of the management console, see [Chapter 3, “Using the Console,”](#) which covers the console’s features and functionality in detail.

Preparing to set up OpenEdge Management or OpenEdge Explorer

To ensure that you have the necessary information to perform the setup, consider the following factors before you proceed.

- When you are setting up OpenEdge Management or OpenEdge Explorer:
 - Review the installation and deployment decisions made when you installed OpenEdge Management or OpenEdge Explorer at your site. See [OpenEdge Management and OpenEdge Explorer: Installation](#) for installation considerations.
 - Note that OpenEdge Management runs as a plug-in to the AdminServer; your resources can be administered by OpenEdge Explorer, Progress Explorer, and the command-line utilities, such as dbman or asbman. Therefore, you should be familiar with the AdminServer functionality. For more information, see *OpenEdge Getting Started; Installation and Configuration*.

OpenEdge Explorer and Progress Explorer functionality are essentially the same; you can access online help while working in each interface. For details about the dbman or asbman utility, see *OpenEdge Getting Started: Database Administration*.

- When you are setting up OpenEdge Management or OpenEdge Explorer, note that familiarity with the command-line options (which can be launched from **Start→Programs→OpenEdge Management→Set OpenEdge Management Environment**) is also useful when you are upgrading and you have not preconfigured OpenEdge Management or OpenEdge Explorer to autostart. You can stop and start either one manually, as follows:

```
fathom -start  
fathom -stop
```

You can also start or stop either one from the **OpenEdge Management** menu. To open either one in a browser, click the **Management Console** shortcut on your desktop (if you chose to install the shortcut during OpenEdge Management or OpenEdge Explorer installation).

For details about using command-line options with OpenEdge Management or OpenEdge Explorer, see [Chapter 5, “Administering OpenEdge Management and OpenEdge Explorer.”](#)

Completing the initial setup process

The first time you start OpenEdge Explorer or OpenEdge Management after installation, you must make some initial setup decisions.

Setting up OpenEdge Explorer

If you install only OpenEdge Explorer (and not OpenEdge Management), you are prompted to make initial configuration choices the first time you start it in the browser after installation, when the **OpenEdge Explorer Configuration** page automatically appears. Once you fill in all the fields and click **Submit**, you can begin using OpenEdge Explorer.

Setting up OpenEdge Management

If you install OpenEdge Management, you are prompted to make initial configuration choices the first time you start it in the browser after installation. The OpenEdge Management configuration process involves making choices on these two OpenEdge Management console pages:

- **OpenEdge Management Configuration**
- **Getting Started**

Once you fill in all the fields and click **Submit** on the **OpenEdge Management Configuration** page, OpenEdge Management is partially initialized; and the **Getting Started** page appears. The **Getting Started** page allows you to define monitors for files, disks, and scripted databases.

After you make your initial configuration choices, you can access and change certain configuration options at any time.

Starting OpenEdge Management or OpenEdge Explorer

Whenever you start OpenEdge Management or OpenEdge Explorer in the browser window, you provide the applicable URL in the address or location field and then log on.

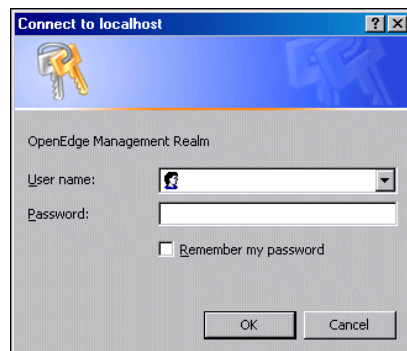
The URL you enter is `http://host:port`, where the *host* is the name of a machine OpenEdge Management or OpenEdge Explorer is installed on, and *port* is the Web server port (by default, this port is 9090).

For details about which browser versions are supported, see [OpenEdge Management and OpenEdge Explorer: Installation](#).



To start OpenEdge Management or OpenEdge Explorer:

1. Be sure that the AdminServer is running on the machine where you want to start OpenEdge Management or OpenEdge Explorer.
2. Choose one:
 - Open a Web browser, and enter the URL `http://host:port` in the address or location field. The logon window appears.
 - From the Windows Desktop on your local host, select **Start**→**Programs**→**OpenEdge Management** or **OpenEdge Explorer**→**Management Console**. Your default browser appears, displaying the logon window.
 - Click the **Management Console** shortcut in your Windows Desktop (if you chose to add the shortcut during OpenEdge Management or Open Edge Explorer installation in a Windows platform). Your default browser appears, displaying the logon window. Note that the specific appearance of this window depends on the browser you are using.



The logon window requires you to enter your user name and password, as described in the [“Entering the default user name and password”](#) section on page 2–6.

Entering the default user name and password

The first time you log on to OpenEdge Management or OpenEdge Explorer, you must use the default user name, which is **admin**, and the default password, which is **admin**.



To enter the default user name and password:

1. Type **admin** in both the **User name** and the **Password** fields.
2. Click **OK**. One of the following occurs:
 - If you are logging on to OpenEdge Management, the **OpenEdge Management Configuration** page opens in the management console, allowing you to set the necessary initial options.
 - If you are logging on to OpenEdge Explorer, the **OpenEdge Explorer Configuration** page opens in the management console, allowing you to set the necessary initial options.

Note that after you make your initial configuration choices, you can access and change certain configuration options at any time.

Keep in mind the following details related to the default password **admin**:

- You use the default password **admin** only once—the first time you log on to OpenEdge Management or Open Edge Explorer. The configuration page that opens at the initial login requires you to change the default password before you can submit your initial setup choices and before you can use OpenEdge Management or OpenEdge Explorer.
- The new password you provide on the configuration page does not take effect until you stop and restart OpenEdge Management or OpenEdge Explorer. You do this by either shutting down and restarting the host machine or using the appropriate command-line interface (CLI) commands. See the [“Using the command-line interface”](#) section on page 5–25 for more information.

You can now make initial configuration choices, as described in the [“Choosing initial configuration options”](#) section on page 2–7.

Choosing initial configuration options

When you log on to OpenEdge Management or OpenEdge Explorer for the first time, you must make some initial configuration choices.

Remember that:

- You can subsequently change these initial configuration decisions.
- As you use the console to establish your configuration, required fields appear in red. Configuration does not proceed if you leave a required field blank.
- OpenEdge Management and OpenEdge Explorer support the implementation of the Secure Sockets Layer (SSL) protocol for HTTP.

When you complete the initial configuration of OpenEdge Explorer, you can further modify your settings by choosing SSL support when setting up the Web server. You have the option of setting up either the HTTP or the HTTPS protocol; you also have the option of setting up both protocols.

When you complete the initial configuration of OpenEdge Management, you can further modify your settings by choosing SSL support when setting up the Web server and when trending to a remote OpenEdge Management Trend Database.

See [Chapter 6, “Setting up Secure Communications,”](#) for more information.

Setting initial configurations for OpenEdge Explorer

When you log on to OpenEdge Explorer the first time, use the **OpenEdge Explorer Configuration** page that appears in the browser to make the following initial choices:

- [Specifying the Admin Password](#)
- [Specifying the AutoStart option](#)
- [Specifying the Web server port](#)

Each of these options is described in following sections.

When you finish setting all the options on the page, click **Submit**.

Setting initial configurations for OpenEdge Management

When you log on to OpenEdge Management for the first time, use the **OpenEdge Management Configuration** page that appears in the browser to make the following initial choices:

- [Specifying the Admin Password](#)
- [Specifying the AutoStart option](#)
- [Specifying the location of the OpenEdge Management Trend Database](#)
- [Specifying the Web server port](#)
- [Specifying the OpenEdge Management e-mail server and default operator](#)

Each of these options is described in following sections of this chapter.

When you finish setting all the options on the page, click **Submit**.

Specifying the Admin Password

OpenEdge Management and OpenEdge Explorer both initialize with a default user name and password for the administrator. The default value for both the user name and the password is **admin**.

You must change the password on the **Configuration** page after you log in for the first time, and you should change it at frequent intervals thereafter. To change the password at any time other than during initial configuration, do so from the **Authorized Users** page. See the [“Adding users as administrators or operators”](#) section on page 5–7 for more information.

The new password you provide on the **Configuration** page does not take effect until you stop and restart OpenEdge Management or OpenEdge Explorer, by either shutting down and restarting the host machine or using the appropriate command-line interface (CLI) commands. See the [“Using the command-line interface”](#) section on page 5–25 for more information.



To change the administrator password:

1. Enter your new administrator password in the **Password** field of the **Admin Password** section:

2. Confirm the new password by typing it in the **Confirm password** field. When you stop and restart OpenEdge Management or OpenEdge Explorer, remember to use the new password.

Note that the default user name of **admin** remains valid.

3. Continue to the next section on the **Configuration** page, where you indicate if you want to start OpenEdge Management or OpenEdge Explorer automatically when the AdminServer starts. (You should delay clicking **Submit** until after reviewing and/or selecting all options on the **Configuration** page.)

Specifying the AutoStart option

If you select the **Autostart OpenEdge Management** or **Autostart OpenEdge Explorer** option, OpenEdge Management or OpenEdge Explorer will start automatically when the AdminServer starts. The **Autostart** check box is selected by default, as shown in the example for OpenEdge Management in Figure 2–1.

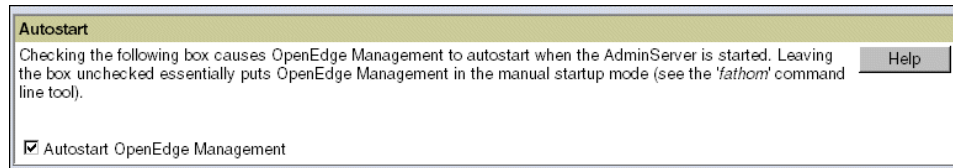


Figure 2–1: Autostart OpenEdge Management option

If you clear this box, you must use the command-line interface to start OpenEdge Management or OpenEdge Explorer. See the “[Using the command-line interface](#)” section on page 5–25 for details.

Specifying the location of the OpenEdge Management Trend Database

OpenEdge Management allows you to store trend data, which is the monitoring information OpenEdge Management maintains, in either a local or remote OpenEdge Management Trend Database. These storage options appear in the **Trend database location** section, shown in Figure 2–2.

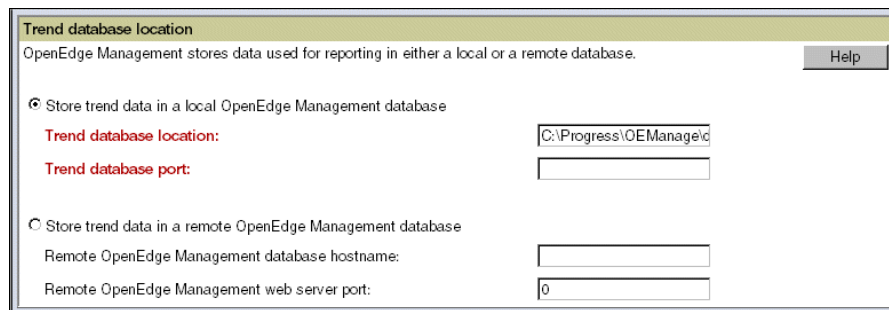


Figure 2–2: Trend database location

If you choose to send trend data to a local database (which is the default), you must specify the trend database location and the port used to connect to that database. If you choose to use a remote database, you must specify the host name and Web server port of the remote OpenEdge Management Web server. The trend database must be locally configured at the remote location. All values you enter for either option are validated.

If you are trending to a remote database and want to establish secure transmission of data, you can choose to use the HTTPS protocol. See [Chapter 6, “Setting up Secure Communications,”](#) for more information.

Note: The configuration option you select for this step must match the installation decisions you implemented during the OpenEdge Management installation process. For example, you can elect to store trend data in a remote OpenEdge Management Trend Database only if you installed OpenEdge Management on both the local machine and the remote machine. For more information, see [OpenEdge Management and OpenEdge Explorer: Installation](#).



To specify the location of the OpenEdge Management Trend Database:

1. Go to the **OpenEdge Management Configuration** page's **Trend database location** section, as shown in [Figure 2–2](#).
2. To store trend data locally, follow these steps:
 - a. Select the **Store trend data in a local OpenEdge Management database** option.
 - b. Specify the **Trend database location**. You can either confirm the explicit path that matches the database location specified during the OpenEdge Management installation process, or you can provide a different path to the OpenEdge Management Trend Database.

If you enter a path location for the OpenEdge Management Trend Database that is different from the one you specified during installation, you must also copy the OpenEdge Management Trend Database from its previously installed location to its new location. You must use either the `procopy` or `prodb` command to preserve the schema integrity.

For more information about either command, see *OpenEdge Data Management: Database Administration*.

The configuration name of the trending database is OpenEdge Management Trend Database. The name of the physical database must be **fathom**.

- c. Enter the port number in the **Trend database port** field.
3. To store trend data remotely, follow these steps:
 - a. Select the **Store trend data in a remote OpenEdge Management database** option.
 - b. Enter the host name of the machine in the **Remote OpenEdge Management database hostname** field. This is the host name where the remote database is installed. The name can be either a valid IP address or a name; it does not have to be fully qualified.
 - c. Enter the HTTP port number in the **Remote OpenEdge Management web server port** field. This is the port number that the OpenEdge Management Web server uses to connect to the remote OpenEdge Management system.

When you choose to store trend data on a remote OpenEdge Management database, the assumption is that you have already configured the OpenEdge Management Trend Database on the remote system. OpenEdge Management displays a warning message if it cannot verify that the remote database is properly configured.

Specifying the Web server port

OpenEdge Management and OpenEdge Explorer contain a Web server. The Web server allows you to connect to either OpenEdge Management or OpenEdge Explorer through the Web-based console. By default, OpenEdge Management and OpenEdge Explorer use port 9090 for this Web server.

If port 9090 is already in use on your system, or if you prefer to use another port, you can change the port used by OpenEdge Management or OpenEdge Explorer by editing the \$FATHOMINSTALLDIR\bin\fathom.properties file. Change the port of the jetty Web server under the [webserver] section. For example:

```
[webserver]
httpport=9099
```

Note: If you change the port number, the Web server immediately stops and restarts on the new port. You must reconnect the console to OpenEdge Management or OpenEdge Explorer on the new port.

Once you set up the Web server port during the initial configuration, you can further modify its settings by choosing to use either the HTTP or the HTTPS protocol; you also have the option of setting up both protocols. See [Chapter 6, “Setting up Secure Communications,”](#) for more information.

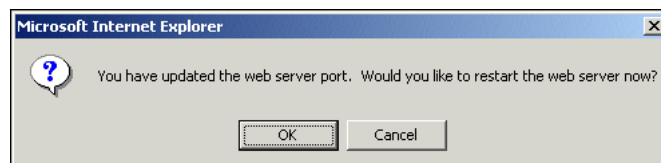


To change the port used by the OpenEdge Management or OpenEdge Explorer server:

1. Scroll to the **Web server port** section of the **Configuration** page, as shown in the following OpenEdge Management example:

2. Accept the default port number 9090, or enter a different port number. Once you finish making configuration choices on this page and click **Submit**, the port number is referenced.

If you change the Web server port, you will see the following message once you finish selecting all the configuration options and click **Submit**:



3. Click **OK** to restart the Web server. You must then reconnect to OpenEdge Management or OpenEdge Explorer, using the new port number in the browser's URL, and refresh the page.

Specifying the OpenEdge Management e-mail server and default operator

OpenEdge Management uses e-mail to send alerts to appropriate personnel. Alerts are messages from OpenEdge Management regarding potential irregularities in the resources you are monitoring.

If your organization has access to a paging service that reports on text-based messages that are sent by e-mail, your organization can use the e-mail action feature to initiate this message. You can determine whether the e-mail alert message is to be sent to an e-mail address or to a pager as a text message. To use alerts, you must specify the Simple Mail Transfer Protocol (SMTP) host and port that OpenEdge Management will use to send e-mail messages.

You should also identify a default user to receive alerts. This user's name will appear as the default recipient of each new alert that you define. You should choose a user who is most likely to receive most, if not all, generated alerts. However, remember that when you set up your monitors with OpenEdge Management, you can choose to override the default user.



To specify the e-mail server and the default operator you want to receive these alerts:

1. Scroll to the **Default alert recipient** section of the **OpenEdge Management Configuration** page:

2. Enter the SMTP host name in the **Mail server (SMTP) host** field. Check with your e-mail administrator if you do not know the e-mail host name.
3. Enter the port used by the SMTP host in the **Mail server (SMTP) port** field. On most systems, this is port 25.
4. Enter the e-mail address of the user you want to be listed as the default recipient of alerts in the **Default e-mail recipient** field.
5. If you want to require the default e-mail recipient to enter a user name and password, select the **Require SMTP user name and password** option. Then provide the user name and the password and confirm the password in the fields provided.

When the default alert recipient information is submitted, OpenEdge Management automatically sets up a Transmission Control Protocol (TCP) network resource monitor, SMTP_MAIL, for the host and port specified using default monitoring values. The SMTP protocol is used for sending e-mail messages between servers.

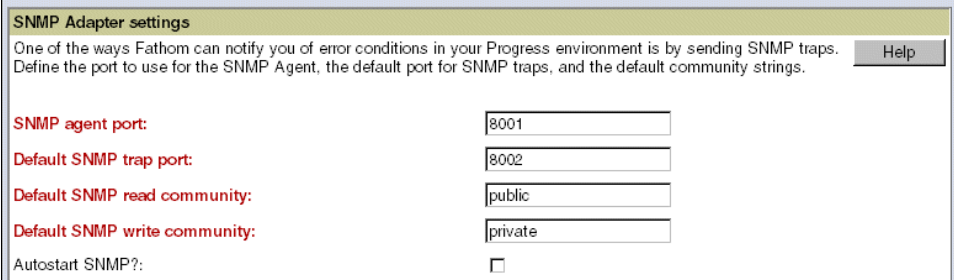
Alerts generated for this resource monitor are based on host and port performance only. For more information about network resource monitors, see [OpenEdge Management: Resource Monitoring](#).

Specifying OpenEdge Management SNMP Adapter settings

The Simple Network Management Protocol (SNMP) Adapter allows you to run the OpenEdge Management SNMP agent and configure it to throw traps to an SNMP management console. *Traps* are OpenEdge Management-resource-related event notifications sent to your SNMP management console. (For more information about the SNMP Trap Action, see [OpenEdge Management: Resource Monitoring](#).)

The SNMP agent is responsible for handling SNMP requests. All OpenEdge Management-specific SNMP variables are contained in the Management Information Base (MIB); the MIB is named `PSC-FM-MIB.txt` and is located in the `<OpenEdgeManagement-install-dir>\config` directory.

If you installed the SNMP Adapter, you see default adapter settings, as shown in [Figure 2–3](#), as you perform the initial OpenEdge Management configuration.



The image shows a dialog box titled "SNMP Adapter settings". It contains a paragraph of text: "One of the ways Fathom can notify you of error conditions in your Progress environment is by sending SNMP traps. Define the port to use for the SNMP Agent, the default port for SNMP traps, and the default community strings." There is a "Help" button in the top right corner. Below the text are four labeled input fields: "SNMP agent port:" with value "8001", "Default SNMP trap port:" with value "8002", "Default SNMP read community:" with value "public", and "Default SNMP write community:" with value "private". At the bottom, there is a checkbox labeled "Autostart SNMP?" which is currently unchecked.

Figure 2–3: SNMP Adapter settings

You can change these SNMP Adapter settings, which are defined as follows:

- **SNMP agent port** — The port number of the host machine on which the SNMP management agent resides. The SNMP agent translates the requests from the SNMP management console and interprets MIB variables. The default port number is 8001.
- **Default SNMP trap port** — The port number to which traps are sent. The default number is 8002.
- **Default SNMP read community** — The community that specifies who has permissions to read which variables.
- **Default write community** — The community that specifies who has permissions to write which variables. (In the case of the OpenEdge Management MIB, the values are read-only.)
- **Autostart SNMP** — The option to autostart the SNMP agent.

Submitting the OpenEdge Management or OpenEdge Explorer Configuration page

Once you make your initial configuration choices, you must save them.



To save your initial configuration options:

1. Click **Submit** at the bottom of the **Configuration** page.

If you entered all required OpenEdge Explorer values and the values are validated, then you are asked if you want to restart the Web server.

If you entered all required OpenEdge Management values and the values are validated, then:

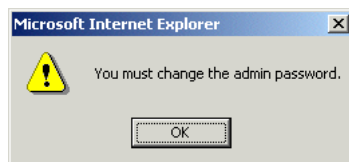
- OpenEdge Management is initialized.
- The creation of SMTP_MAIL is acknowledged.
- A reminder appears about using the new password when restarting OpenEdge Management.

2. Click **OK**.

If you configured the initial OpenEdge Explorer options, you can close the browser and reopen it. Type the user name and the new password you set, and click **OK**. The **OpenEdge Explorer Resources** page appears.

If you configured the initial OpenEdge Management options, the **Getting Started** page automatically appears. Note that this page does not appear if you installed only OpenEdge Explorer.

If all the initial configuration values cannot be validated, warning messages appear. For example, if you have not updated the default password, you receive the following message:



- a. Click **OK** to erase the message, and in this instance change the admin password.
- b. Click **Submit**.

Setting up the Getting Started page for OpenEdge Management

The choices you make on the **Getting Started** page allow you to migrate scripted databases to managed databases recognized by the AdminServer and OpenEdge Management, and define monitoring and trending options for file systems and disks.

Once you establish these initial resource-monitoring options, you can set more specific monitoring criteria for individual resources. Similarly, you can also manually initiate resource discovery of TCP- and UDP-based applications. See [OpenEdge Management: Resource Monitoring](#) for more details.

Understanding managed and scripted databases

You can set up a database resource monitor in OpenEdge Management for a database that the Progress Explorer, the AdminServer, and OpenEdge Management commonly recognize. For example:

- A managed database is a database that the Progress Explorer and the AdminServer recognize and manage. In OpenEdge Management, you can set up resources for file systems and disks associated with managed databases.

When OpenEdge Management starts up, all databases currently managed by Progress Explorer and the AdminServer are automatically discovered (recognized) by OpenEdge Management.

- A scripted database is a database that is not currently listed among the database resources that the AdminServer manages.

If you want to manage a scripted database with the AdminServer, you use the Database Migration utility, which also adds the database to the `conmgr.properties` file.

Defining OpenEdge Management monitors for previously scripted databases

By using the Database Migration Utility, you can add a previously scripted OpenEdge database as a resource to OpenEdge Management. These databases are typically managed outside the AdminServer using parameter files (.pf) and operating system-dependent scripts.

With the Database Migration Utility, you can identify the database as manageable through the Progress Explorer and the AdminServer. After the configuration migration occurs:

- OpenEdge Management creates a resource if one does not already exist.
- You can define trend and monitoring options.

Note: Before you perform the database migration process, you should shut down the database you intend to migrate. This shutdown activity enables the AdminServer to recognize the database as managed when the database is restarted through OpenEdge Management, and to create and enable the database monitor.

Figure 2–4 shows the **Define monitors for external OpenEdge databases** section.

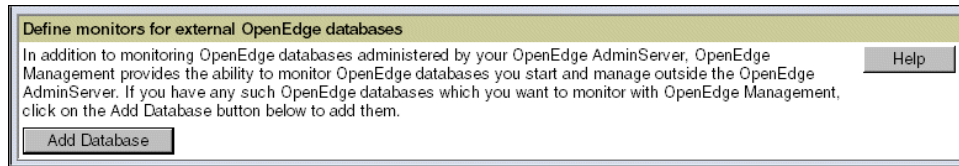


Figure 2–4: Defining monitors for external OpenEdge databases

Note: When you add a managed database using the values you enter on the **Database Migration Utility** page and then submit the **Getting Started** page, a database configuration is created in the `commgr.properties` file, and a database resource is created in the OpenEdge Management configuration data store.

Adding a managed database

Click **Add Database**. The **Database Migration Utility** page appears as shown in Figure 2–5.

Figure 2–5: Database Migration Utility

You enter the database values on this page. Note that any field name in red requires a value; all other fields are optional.

For a description of the fields, click **Help**.

**To add the managed database:**

1. Choose the database container in the **Container** field.
2. Enter the database display name in the **Database Display Name** field.
3. Enter the database path and filename associated with the physical database in the **Database Path and Filename** field.
4. Optionally provide values to add database arguments, using either or both of these methods:
 - In the **Parameter File Name** field, enter the name of the parameter file (.pf) that contains database argument values if you have overriding arguments defined for database brokers.
 - Enter the database argument values explicitly in the **Other Database Broker Arguments** field. If you want to specify a port for the database, type **-S** and then the port number.

If the port specified for the database is **0**, then the database is considered non-networked. It will not be monitored by OpenEdge Management.

Note that you can enter any miscellaneous, non-AdminServer-recognized arguments using either of the previous methods.

Values set using the parameter file method can be overridden by the values specified in the **Other Database Broker Arguments** field. Processing difficulties related to these values are handled as follows:

- If an argument cannot be mapped to a unique property in the `conmgr.properties` file, it is appended to the **Other Args** property. (If you are working with OpenEdge Management, any unmapped arguments are displayed in an alert box when you submit the **Getting Started** page.)
 - If an error occurs either when the database configuration is created or when the database resource is created, the configuration is not added to the database properties file (`conmgr.properties`), and the resource is not created.
5. Select one of the **Database Broker Type** options to indicate the type of client that is allowed to connect to the broker: **4GL** brokers allow only ABL client connections and **SQL** brokers allow SQL Explorer or other SQL client connections. The default option, **Both**, allows ABL and SQL clients.

Remember that the client type choice you make here is honored only when you have installed the proper licenses for that client.

6. Select **AutoStart Database Broker** to start the database broker automatically when the AdminServer is started.
7. Select **Watch Dog Process (WDOG)** to start a watchdog process for the database.

The following are Enterprise-only options that are automatically started only if the database broker is also automatically started:

- Select **After Image Process (AIW)** to start an after-image writer for the database.
- Select **Before Image Process (BIW)** to start a before-image writer for the database.
- Enter a numeric value in the **Asynchronous Page Writers (APW)** field to define the number of asynchronous page writers to start. The default value is 1.

Note: If you are running the Workgroup database, the default value for each of the writers is zero, and you cannot change it.

Making changes to a managed database configuration

You can view, modify, or delete a managed database configuration.

Note: From within OpenEdge Management or OpenEdge Explorer, you can use the **Control** page to start and stop a database configuration. For more information about starting and stopping the database, see [OpenEdge Management and OpenEdge Explorer: Configuration](#).

Defining OpenEdge Management monitoring and trending options for file systems and disks

OpenEdge Management can create resource monitor and trending options for all file systems and disks on a system where OpenEdge Management is installed.

As shown in [Figure 2–6](#), you can specify whether you want OpenEdge Management to monitor only those file systems and disks used by OpenEdge databases, or all file systems and disks.

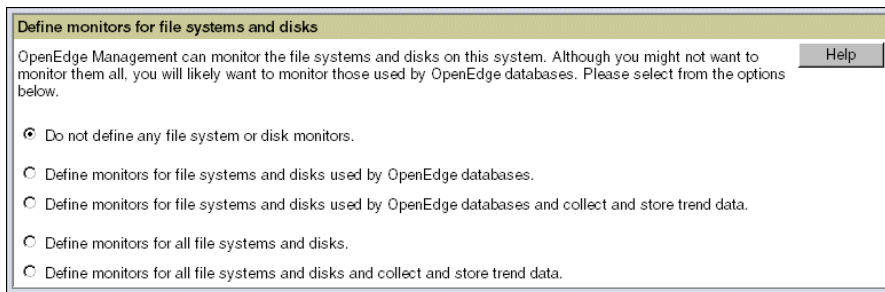


Figure 2–6: Defining monitors for file systems and disks

You can also choose whether or not OpenEdge Management should collect and store trend data on the file systems and disks. If you prefer, you can opt not to set up monitors for file systems and disks at all. These file system and disk resource monitors are created with default settings, helping you to expedite the resource monitoring setup activities.

Monitoring and trending considerations

Consider the following before you add monitors for file systems and disks in OpenEdge Management for your OpenEdge databases:

- If a file system monitor or resource does not already exist, a new file system resource or monitor is configured. The monitor or trend process is enabled for each file system that is accessed by a managed database or any of its extents.
- If a disk monitor or resource does not exist, a new disk resource or monitor is added. The monitor or trend process is enabled for each disk on the system that is accessed by a managed database or any of its extents.

Choose one of the following options to define monitors for file systems and disks:

- Select **Do not define any file system or disk monitors** to bypass any monitoring and trending options.
- Select **Define monitors for file systems and disks used by OpenEdge databases** to add only monitors for file systems and disks.
- Select **Define monitors for file systems and disks used by OpenEdge databases and collect and store trend data** to add monitoring and trending activities for file systems and disks used by your OpenEdge databases.
- Select **Define monitors for all file systems and disks** to define monitors for all file systems and disks, not just those used by OpenEdge databases.
- Select **Define monitors for all file systems and disks and collect and store trend data** to add monitoring and trending activities for all file systems and disks, not just those used by your OpenEdge databases.

Submitting the Getting Started page for OpenEdge Management

When you finish making your selections on the **Getting Started** page, click **Submit**. OpenEdge Management starts the monitoring database agent for each managed database for which you selected the monitoring option. CPU and memory resources are created as well.

The OpenEdge Management console appears with a confirmation that OpenEdge Management is ready to use, as shown in [Figure 2–7](#).

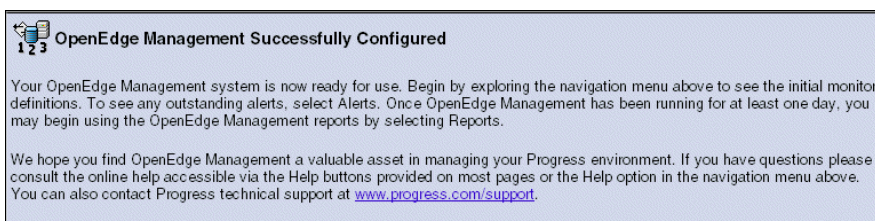


Figure 2–7: OpenEdge Management Configuration success

Using the Console

The browser-based management console is the graphical user interface for OpenEdge Management and OpenEdge Explorer.

This chapter provides an introduction to the console, as outlined in the following sections:

- [Starting OpenEdge Management or OpenEdge Explorer](#)
- [Using the management console](#)
- [Navigating the console](#)
- [Changing the console display](#)
- [Additional console details](#)

Starting OpenEdge Management or OpenEdge Explorer

The management console is the Web-based graphical user interface that you use to work with OpenEdge Management or OpenEdge Explorer. You access this console from any browser that OpenEdge Management and OpenEdge Explorer support. (See *OpenEdge Management and OpenEdge Explorer: Installation* for specifics about which browsers are supported.)

You use the management console to access all of OpenEdge Management's and OpenEdge Explorer's functionality.

Logging on

After you log on to OpenEdge Management or OpenEdge Explorer for the first time, you must establish some initial configuration settings before you can use it.



To access the logon window and open the management console:

1. Depending on whether you are accessing the management console from a Web browser or locally, choose one of the following methods:
 - To access OpenEdge Management or OpenEdge Explorer from a Web browser, enter the URL `http://host:port` in the **Address** or **Location** field. The *host* is the name of a machine on which OpenEdge Management or OpenEdge Explorer is installed, and the *port* is the Web server port (by default, this port is 9090). A logon window appears.
 - To access OpenEdge Management or OpenEdge Explorer locally from the Windows Desktop, choose **Start**→**Programs**→**OpenEdge Management/OpenEdge Management and Explorer/OpenEdge Explorer**→**Management Console**. The default browser appears in the background. The logon window appears in the foreground, as shown:

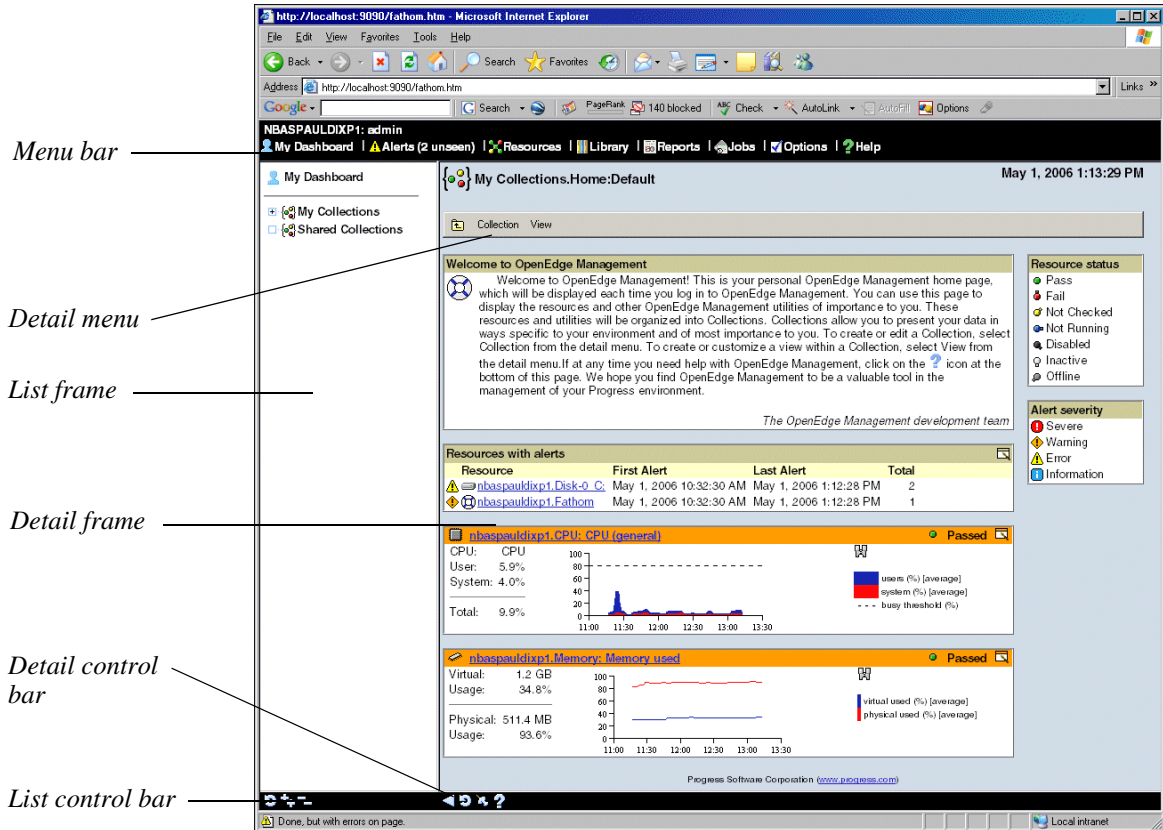


Note: If you installed OpenEdge Management or OpenEdge Explorer in Windows and chose to install the shortcut icon, you can click the **Management Console** shortcut icon to display this window.

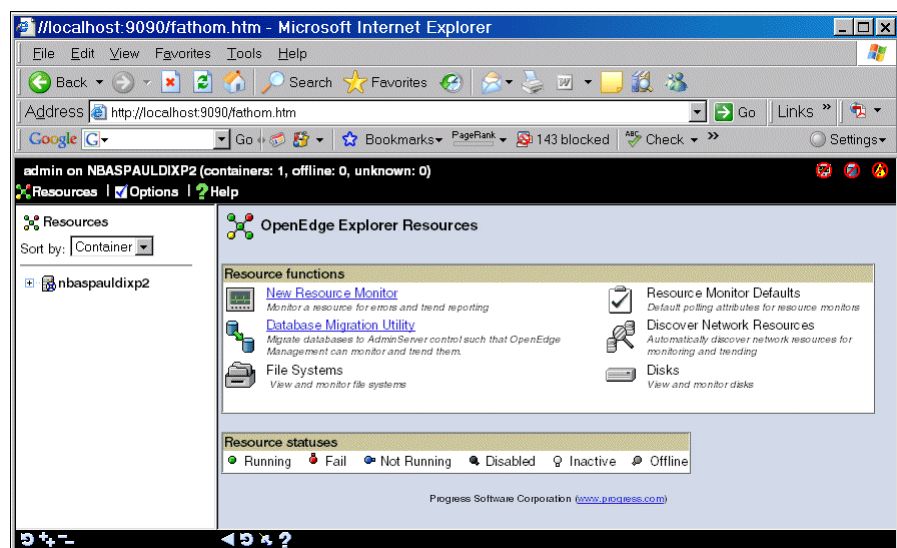
The specific appearance of the logon window depends on the browser you are using.

- If you are logging on for the first time, type the user name **admin** and the password **admin** in the appropriate fields, and click **OK**. The **OpenEdge Management Configuration** or **OpenEdge Explorer Configuration** page appears when the console opens.

When you log on after the first time, you use a new password you have created. For OpenEdge Management, the console opens to **My Dashboard**, as shown:



For OpenEdge Explorer, the console opens to the **OpenEdge Explorer Resources** page:



The overall layout of the console is the same in OpenEdge Explorer as it is in OpenEdge Management.

Using the management console

The management console consists of the following components:

- **Menu bar** — Identifies the host OpenEdge Management or OpenEdge Explorer is running on.

For OpenEdge Management, the menu bar provides access to these features:

- **My Dashboard**
- **Alerts**
- **Resources**
- **Library**
- **Reports**
- **Jobs**
- **Options**
- **Help**

For OpenEdge Explorer, the menu bar provides access to these features:

- **Resources**
- **Options**
- **Help**

- **Detail menu** — A dynamic HTML menu available on each detail page in the management console. The content of the menu varies depending on where it appears and whether you are working with OpenEdge Management or OpenEdge Explorer. The detail menu commands enable you to perform a number of common tasks.
- **List frame** — The left pane in the console. The list frame provides access to different areas within OpenEdge Management or OpenEdge Explorer by presenting a collapsible and expandable tree-like structure and a sort feature.
- **Detail frame** — The right pane in the console. The detail frame displays the OpenEdge Management or OpenEdge Explorer component you select in the list frame.
- **Detail control bar** — Allows you to work with the contents of the detail frame by returning to the previous OpenEdge Management or OpenEdge Explorer page, refreshing the page, displaying the page in a new window, or accessing online help.
- **List control bar** — Allows you to work with the contents of the list frame by refreshing the list frame display, expanding the list frame categories, or collapsing the list frame categories.

Figure 3–1 shows how the management console for OpenEdge Management appears if you select **Resources** in the menu bar, and then click the plus sign preceding the **Container** name in the list frame. The list frame displays existing resource-related information (in this case, for the container **nbaspauldixp1**), with a **Sort by** option, and the detail frame displays the **OpenEdge Management Resources** page.

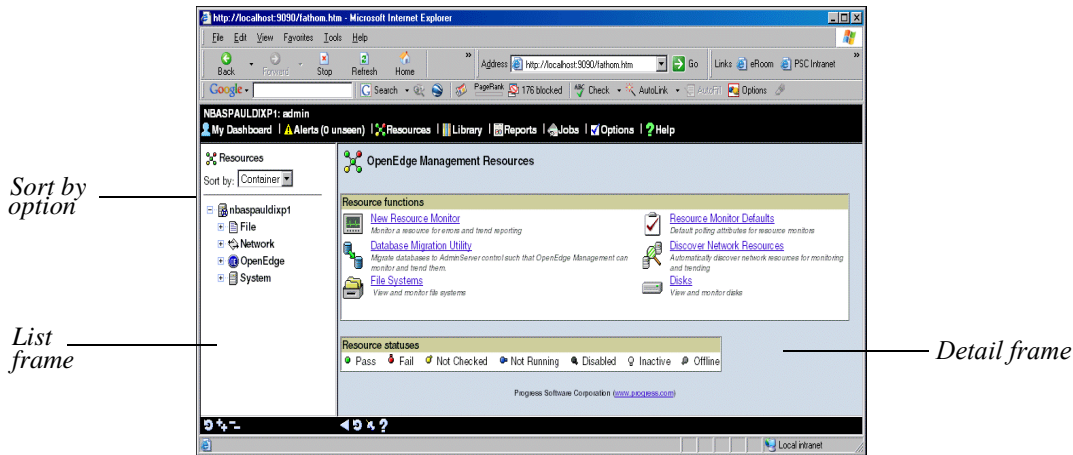


Figure 3–1: OpenEdge Management Resources page

Viewing the contents of a container

When you click the container name in the list frame, the **Container** page appears in the detail frame, as shown in the OpenEdge Management example in Figure 3–2.

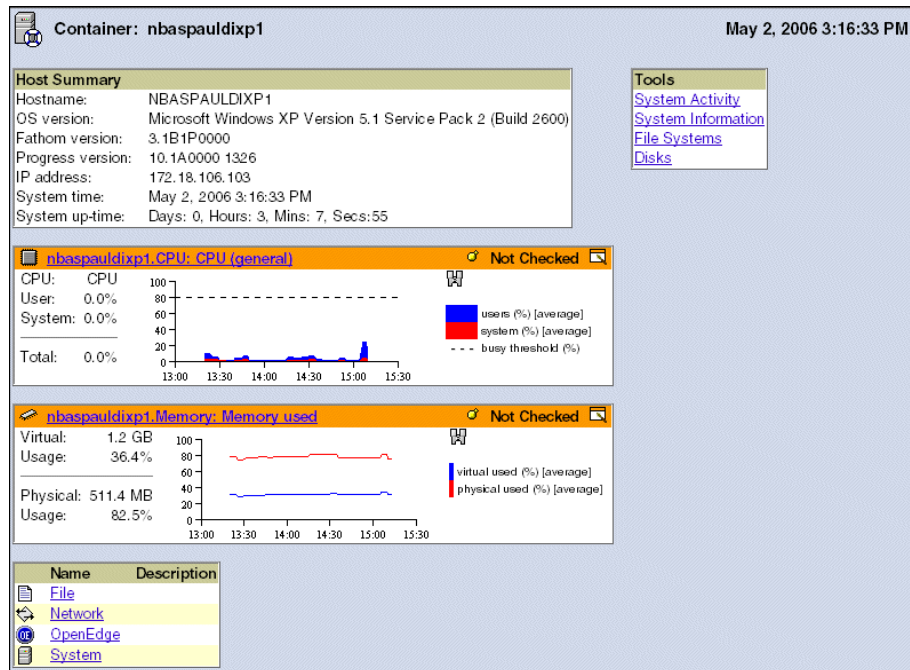


Figure 3–2: Container view in the detail frame

The OpenEdge Management **Container** page includes summary information about the host machine, viewlets that illustrate CPU and memory performance details, and access to the different resource categories, such as **File** and **Network**.

The OpenEdge Management **Container** page also provides access to the following details:

- **System Activity** — The System Activity report, which identifies host information, CPU utilization, and memory utilization
- **System Information** — The System Information report, which provides details about the host, the operating system, the OpenEdge Management installation, the OpenEdge installation, and startup information (such as Java classpath setting, the library path setting, and system path setting)
- **File Systems** — Tabular and graphical details about the container's file systems, including the systems' overall capacity, free space, current usage, and other statistics
- **Disks** — A list of the container's disks and access to details about each one

Accessing functions from the menu bar

You can access OpenEdge Management or OpenEdge Explorer functions from the management console menu bar.

OpenEdge Management

You can access the following OpenEdge Management functions from the menu bar:

- **My Dashboard** — Customizable private or shared collections of resources that include views of OpenEdge Management components.
- **Alerts** — Open alerts.
- **Resources** — Resources being monitored by OpenEdge Management. These include database, file, network, OpenEdge server, and system.
- **Library** — Functions you use to centrally define components for sharing and reuse among resources. Library functions include actions, search criteria, rule sets, schedules, and templates.

You can also perform various export and import activities related to resource distribution and management from the Library.

- **Reports** — Reporting functions, such as creating, scheduling, and running reports.
- **Jobs** — Job functions, such as creating, scheduling, and running jobs.
- **Options** — Administrative and user management functions.
- **Help** — Various help resources, such as OpenEdge Management and OpenEdge Explorer documentation, support, and Knowledge Base access.

OpenEdge Explorer functions

You can access the following OpenEdge Explorer functions from the menu bar:

- **Resources** — Resources whose configuration you can set or modify in OpenEdge Explorer. These include AppServer Internet Adapters, AppServers, Databases, DataServers (ODBC, Oracle, or MS SQL Server), Messengers, NameServers, SonicMQ Adapters, WebSpeed Transaction Servers, and Web Services Adapters.
- **Options** — Administrative and user management functions.
- **Help** — Various help resources, such as OpenEdge Management and OpenEdge Explorer documentation, support, and Knowledge Base access.

Viewing additional details

Your user name and the name of the machine that is hosting OpenEdge Management or OpenEdge Explorer also appear in the menu bar. In the OpenEdge Management example shown in [Figure 3–3](#), the user name is **admin** and the machine name is **nbaspauldixp2**. When you click the user name, you see details about the user, such as the user name, a description of the user (if available), and the user's role (either Administrator or Operator).

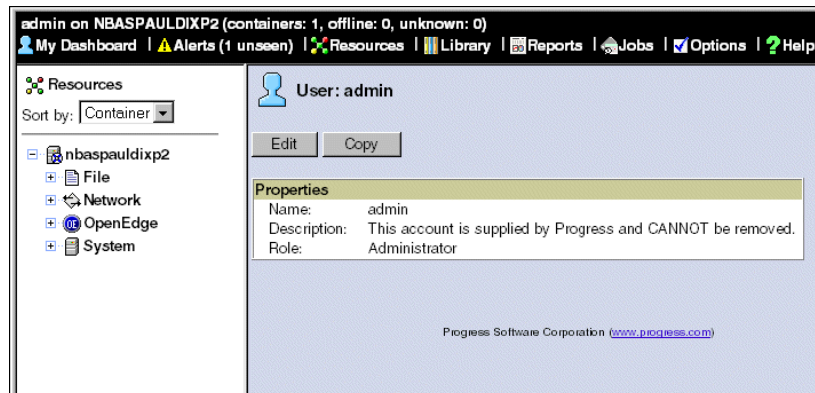


Figure 3–3: OpenEdge Management user name details

Navigating the console

When you are working with OpenEdge Management or OpenEdge Explorer and you open the management console, you see a list of items in the list frame. As you select different features in the menu bar, the contents of the list frame and detail frame change.

For example, if you are working with OpenEdge Management and you click **Library** in the menu bar, you see the library-related components in the list frame, as shown in [Figure 3–4](#).

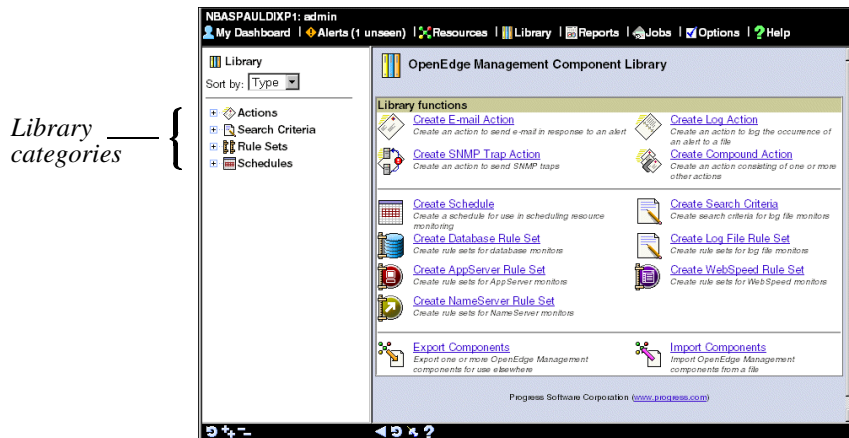


Figure 3–4: Collapsed Library categories in OpenEdge Management list frame

If a plus sign (+) precedes a category in the console list frame, as shown in [Figure 3–4](#), you can click the plus sign to expand the collapsed category and see its contents. If a minus sign (-) precedes a category, the category has been fully expanded and all its contents are in view. If an empty box precedes a category, the category has no contents.

If you click the plus sign preceding each of the collapsed main **Library** categories shown in Figure 3–4, the expanded view looks like that shown in Figure 3–5.

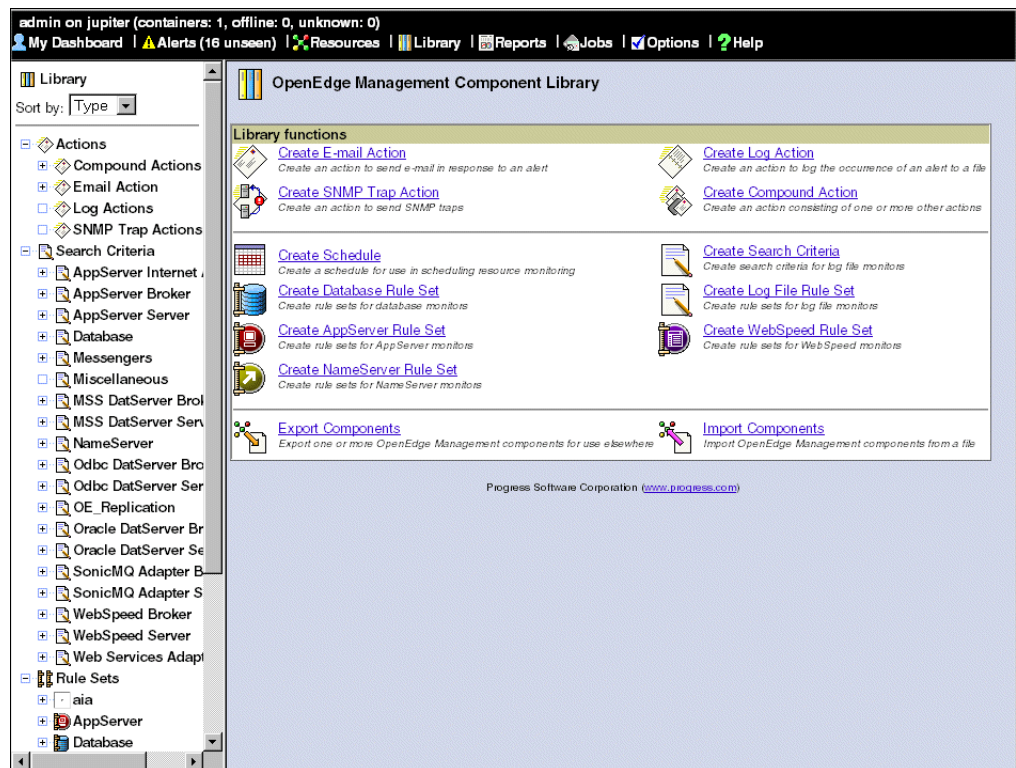


Figure 3–5: Expanded Library categories in OpenEdge Management list frame

When you click a category in the list frame, a list of items in that category appears in the detail frame. For example, if you click **Email Action** under the **Actions** category in the OpenEdge Management list frame, a list of email actions you can choose from appears, as shown in Figure 3–6.

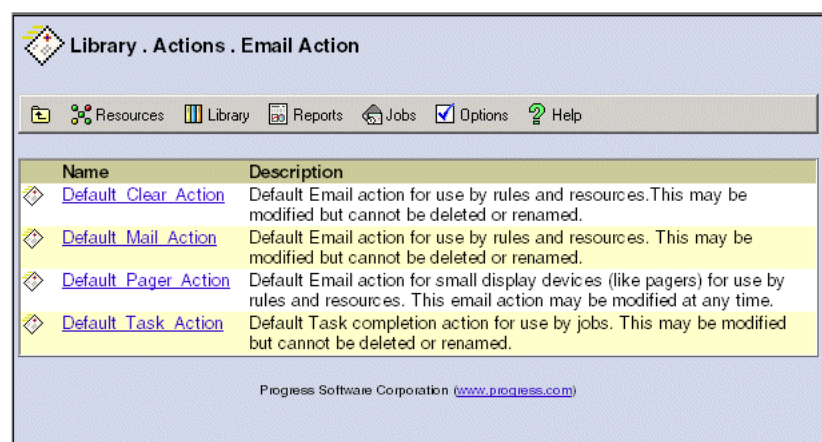



Figure 3–6: Email actions in OpenEdge Management Library→ Actions

A dynamic HTML menu bar listing **Resources**, **Library**, **Reports**, **Jobs**, **Options**, and **Help** categories appears in Figure 3–6. This menu bar is known as the *detail menu bar*. As you navigate throughout the console, you will notice that options available on the menu of certain OpenEdge Management and OpenEdge Explorer pages differ, depending on where you are in the application.

The **Parent Folder** icon  is included in the detail menu bar. Click the **Parent Folder** icon to navigate up a level from the page being shown in the console. In the OpenEdge Management example shown in Figure 3–6, the parent folder is **Actions**, so the detail frame would change to display the **Actions** category's contents, as shown in Figure 3–7.

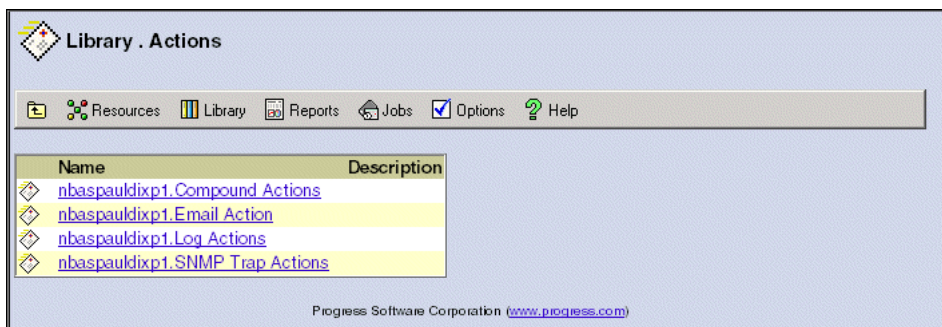


Figure 3–7: OpenEdge Management Actions category

Sorting in the console list frame

By using the **Sort by** feature, you can sort items in the list frame. The sorting options differ, depending on the component.

If you are working with OpenEdge Management, you can sort alerts, library components, and resource categories in one or more of the following ways (depending on the component):

- **Container** — In alphanumeric order by container name
- **Resource Name** — In alphanumeric order by *<container name> .<resource name>*
- **Alert Name** — In alphanumeric order by alert name
- **Last Date** — By date in descending date, from most recent to least recent
- **Severity** — By severity: **Severe**, **Error**, **Warning**, or **Information**
- **Type** — By type, such as actions or rule sets in the **Library**
- **Name** — In alphanumeric order by name
- **Status** — By the following statuses: **Pass**, **Fail**, **Not Checked**, **Not Running**, **Disabled**, **Inactive**, and **Offline**, as shown in Figure 3–8.

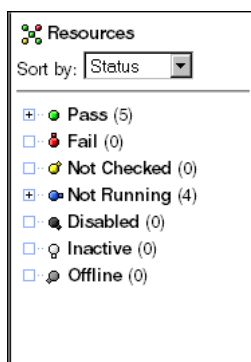


Figure 3–8: Resources sorted by status

If you are working with OpenEdge Explorer, you can sort by:

- **Type** — By type, such as actions or rule sets in the **Library**
- **Name** — In alphanumeric order by name
- **Status** — By the following statuses: **Pass**, **Fail**, **Not Checked**, **Not Running**, **Disabled**, **Inactive**, and **Offline**, as shown in [Figure 3–8](#).
- **Container** — In alphanumeric order by container name

The number in parentheses that follows each status category indicates how many resources the category currently includes.

See the “[Checking resource status](#)” section on page 3–11 for details about the significance of the colored bullet that precedes each category.



To sort resources in the list frame, choose the **Sort by** category in the drop-down list.

Checking resource status

Once you set up resources, OpenEdge Management and OpenEdge Explorer give you a visual indication in the detail frame as to the general status of each resource monitor by using one of the small, colored icons. Each of the icons in the **OpenEdge Management Resource statuses** legend, shown in [Figure 3–9](#), corresponds to a particular status.

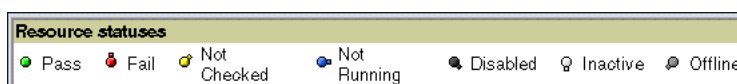


Figure 3–9: OpenEdge Management Resource statuses

The icons shown in [Figure 3–10](#) represent the statuses available in OpenEdge Explorer.



Figure 3–10: OpenEdge Explorer Resource statuses

[Table 3–1](#) briefly describes what each status/color combination represents.

Table 3–1: Resource status legend

(1 of 2)

Status	Color	Description
Pass	Green	The resource monitor is currently working.
Fail	Red	The most recent test involving the resource failed. This includes statuses such as tardy, timeout, and unreachable. Check the Alert Summary page or the specific monitor for possible alert details. This status can also identify an internal error that prevents the resource from being monitored.
Running	Green	The resource is currently running.

Table 3–1: Resource status legend

(2 of 2)

Status	Color	Description
Not Running	Blue	The resource is currently not running. This status is particularly informative as it applies to resources such as databases that must be operating before you can monitor them. Since databases have operational dependencies, the state of the AdminServer, database broker, or agent can cause a Not Running status to be generated for a database or off-line container.
Not Checked	Yellow	The resource monitor's status is currently unknown. For example, at system startup, it is possible that the resource has not yet been polled.
Disabled	Black	The resource monitor has been disabled and is not currently monitoring a resource.
Inactive	White	There is no active monitoring plan at this time.
Offline	Gray	The resource is currently offline.

How outstanding OpenEdge Management alerts can affect resource statuses

If you are working with OpenEdge Management and there are outstanding alerts on a resource, the icon that indicates the most severe alert status displays to the left of the status icon. If there are no alerts on the resource, only the status icon appears. The presence of the alert icon helps you to easily see if there are any outstanding alerts on a resource.







Note that it is possible for a resource to have a **Pass** status when the resource still has open alerts, as indicated by a green status icon. This status indicates that the resource passed on the last poll but failed at some point in the past.

Changing the console display

You can use the management console control bars to change or update the console display. The two adjoining control bars appear horizontally across the bottom of the management console. The list control bar appears across the bottom of the list frame, and the detail control bar appears across the bottom of the detail frame.


Each control bar contains a set of icons that you can use to perform a particular task on the information within the frame, as shown in [Table 3–2](#).

Table 3–2: Console control bar icons

Icon	Description
	Refresh
	Expand all
	Collapse all
	View previous page
	Display page in new window
	Access context-sensitive help



Refreshing the console

As you work with OpenEdge Management or OpenEdge Explorer, be sure to frequently refresh or reload (depending on the browser) the management console so that the console display is the most current. To refresh or reload all or part of the console, perform one of the following tasks:

- Select **View→Refresh** or **View→Reload** from the browser tool bar to refresh the entire console.
- Click the **Refresh** icon  in the list frame control bar or the detail frame control bar to refresh either the list frame or the detail frame.

Expanding or collapsing resource categories

The ability to expand categories can be very useful when you have a large number of categories and subcategories in the list frame you are reviewing.

- To expand all existing categories and subcategories in the list frame, click the **Expand All** icon .
- To collapse all categories to a more condensed view, click the **Collapse All** icon .


Returning to the previous page in the console

You might want to go back to the console page you just viewed.

- ▶ To return to the most recent console page reviewed, click the **Previous Page** icon  in the detail control bar.


Displaying a page in a new window

You can display a page in a new window in the management console. This provides an easy way for you to view different components simultaneously.

- ▶ To open the current detail frame in a new window, click the **Display Page in New Window** icon  in the detail control bar.

Accessing Help

You can access Help in two different ways:

- From the detail control bar, click the **Help** icon  to see context-sensitive help directly related to the active console page.
- From the management console menu bar, choose **Help**→**Documentation** for an online version of the OpenEdge Management and OpenEdge Explorer guides.

Additional console details

As you work with the management console, keep the following details in mind:

- By default all required fields in the management console appear in red. If you are reading this document in .pdf file format through a browser, notice that the required fields shown in the screen captures also display in red. Depending on your printer and printer options, it is possible that the required fields will not print in red if you print the .pdf file.
- The management console presents some initial default values. You can either use the defaults to get OpenEdge Management or OpenEdge Explorer up and running quickly or you can change them to suit your own particular needs.
- When you are working with OpenEdge Management and you select a resource, the management console provides summary information at the top of the detail frame. This information helps you assess—at a glance—name, polling, and status information such as last poll, last failure, and percent of failure.
- The management console includes ToolTips that save you from clicking on each OpenEdge Management alert to see the contents of the alert message. ToolTip information that summarizes alert details for a resource can be displayed on alert icons in the list frame and on the specific alert as it appears on the resource monitor summary page. To display a ToolTip, place your cursor over either of these alert icons. The summarized alert message appears after a few moments.

In addition, ToolTips for unavailable console links identify if the feature or function is available only to OpenEdge Management users. The ToolTip appears when you place your cursor over the unavailable link icon.

- OpenEdge Management and OpenEdge Explorer do not asynchronously update pages, except when you are starting or stopping OpenEdge servers or databases. Therefore, periodically refresh the management console to be sure that you are looking at the most recent data.

If you are working with OpenEdge Management, you can also set the pages to refresh automatically. (By default, this option is disabled.) Click **Options** on the console menu bar, and then select **User Preferences**. You can then choose how often you want OpenEdge Management to automatically refresh the pages.

- To display session context data in more than one browser, you should launch a separate browser. Creating a new browser window simply using the browser's functionality can lead to an unreliable display of information.

Setting up remote resource monitoring and configuration

Any resource type that you can monitor locally you can also monitor remotely, as long as there is an AdminServer on the remote machine. The only exceptions to this are network resources or jobs, which can be monitored only locally.

This chapter describes how to set up OpenEdge Management and OpenEdge Explorer for remote monitoring and configuration, as outlined in the following sections:

- [Remote monitoring and configuration requirements](#)
- [Setting up for remote monitoring or configuration](#)
- [Remote monitoring configuration utility command-line options](#)
- [Disabling remote monitoring](#)
- [Uninstalling if remote monitoring is configured](#)

Remote monitoring and configuration requirements

Remote monitoring and configuration require that you have:

- One OpenEdge and OpenEdge Management/OpenEdge Explorer installation.
- One supported standalone installation of Progress (Release 9.1E04 or later, with the most recent Hotfix) or OpenEdge (Release 10.0B, 10.1x, or 10.2x).

Note: To monitor or configure a remote AppServer Internet Adapter, DataServer, SonicMQ Adapter, or Web Services Adapter, you must be running OpenEdge Release 10.1C03 or 10.2A01.

- You can monitor up to 40 remote containers (AdminServers and/or standalone OpenEdge installations).
- You must also have root permissions on each machine.

When OpenEdge Management is configured for remote monitoring, messages are exchanged between the OpenEdge Management machine and the remote machines. These messages are time stamped, and the time information is used in the communication protocol used between the machines. It is, therefore, important that the machines involved have their universal time setting coordinated. This can be accomplished by ensuring that the machines subscribe to an NTP time service.

Setting up for remote monitoring or configuration

The order in which you set up the machines is important: You must have the machine with the OpenEdge Management/OpenEdge Explorer installation up and running with remote monitoring/configuration in place **before** you establish the required settings on any remote machine.

Setting up the first machine

You must first set up resource monitoring/configuration on the machine that has both OpenEdge Management/OpenEdge Explorer and OpenEdge installed before setting up a second machine.



To set up the first machine:

1. Install OpenEdge.
2. Install OpenEdge Management or OpenEdge Explorer.
3. When the installation completes, start OpenEdge Management or OpenEdge Explorer. The **Configuration** page opens.
4. Fill in the configuration settings, and then click **Submit**. If you are working with OpenEdge Management, the **Getting Started** page appears.
5. Fill in the **Getting Started** page settings, and then click **Submit**.
6. From the Windows **Start** menu, choose **Programs**→**OpenEdge**→**Proenv**. The **Proenv** window opens.
7. Run the following command in the **Proenv** window:

```
fmconfig -enable
```

8. Steps in the setup process are listed (as they occur) in the **Proenv** window, until the setup is complete, as shown:

```

OpenEdge Release 10.2A as of Mon Nov  3 22:05:01 EST 2008
proenv>fmconfig -enable
OpenEdge Release 10.2A as of Mon Nov  3 22:05:01 EST 2008

Unpacking files ... Done
Invoking 2nd phase of setup.
Determining configuration type ... Fathom detected.
Running remote monitoring configuration for Fathom adminserver.
Enabling support in Fathom for remote monitoring
Begin install of SonicMQ (this may take a few minutes).
Install of SonicMQ complete.
Begin tailoring SonicMQ for Fathom.
Creating DS directory /fathom.
Creating DS directory /fathom/fathomgmt...
Creating DS directory /fathom/adminserver...
Creating DS directory /fathom/system...
Creating DS directory /fathom/appserver...
Creating DS directory /fathom/database...
Creating DS directory /fathom/nameserver...
Creating DS directory /fathom/smdatabase...
Creating DS directory /fathom/webspeed...
Creating DS directory /fathom/aia...
Creating DS directory /fathom/odbc...
Creating DS directory /fathom/oracle...
Creating DS directory /fathom/mss...
Creating DS directory /fathom/messengers...
Creating DS directory /fathom/mqadapter...
Creating DS directory /fathom/usa...
Setting storage hints for /fathom/fathomgmt...
Setting storage hints for /fathom/adminserver...
Setting storage hints for /fathom/system...
Setting storage hints for /fathom/appserver...
Setting storage hints for /fathom/database...
Setting storage hints for /fathom/nameserver...
Setting storage hints for /fathom/smdatabase...
Setting storage hints for /fathom/webspeed...
Setting storage hints for /fathom/aia...
Setting storage hints for /fathom/odbc...
Setting storage hints for /fathom/oracle...
Setting storage hints for /fathom/mss...
Setting storage hints for /fathom/messengers...
Setting storage hints for /fathom/mqadapter...
Setting storage hints for /fathom/usa...
Creating DS component Fathom...
Creating DS component ManagementPlugin...
Creating DS component osmetrics...
Creating DS component AppServer...
Creating DS component Database...
Creating DS component NameServer...
Creating DS component SMDatabase...
Creating DS component WebSpeed...
Creating DS component AppServer Internet Adapter...
Creating DS component ODBC DataServer...
Creating DS component Oracle DataServer...
Creating DS component MSS DataServer...
Creating DS component Messengers...
Creating DS component SonicMQ Adapter...
Creating DS component Web Services Adapter...
Creating attribute set for Fathom...
Creating attribute set for ManagementPlugin...
Creating attribute set for osmetrics...
Creating attribute set for AppServer...
Creating attribute set for Database...
Creating attribute set for NameServer...
Creating attribute set for SMDatabase...
Creating attribute set for WebSpeed...
Creating attribute set for AppServer Internet Adapter...
Creating attribute set for ODBC DataServer...
Creating attribute set for Oracle DataServer...
Creating attribute set for MSS DataServer...
Creating attribute set for Messengers...
Creating attribute set for SonicMQ Adapter...
Creating attribute set for Web Services Adapter...
The directory store for C:\Progress\OEManage\MQ6.1\ has been successfully updated.
Tailoring of SonicMQ complete.
Remote monitoring in Fathom is now ENABLED.

Settings take effect the next time the adminserver is started.

```

Additionally, the following new directory is installed: *<install-dir>*\MQ6.1, in which *install-dir* is the directory where OpenEdge Management or OpenEdge Explorer is installed.

Note: If you see the error message “DISPLAY variable must be set” while you are running fmconfig, you must set your \$DISPLAY value to a machine running an X-Windows server.

9. To verify that remote monitoring has been set up properly, run the following command in the **Proenv** window:

```
fmconfig -query
```

The remote monitoring properties appear:

```
proenv>fmconfig -query
OpenEdge Release 10.2A as of Mon Nov  3 22:05:01 EST 2008

=====
Fathom remote monitoring properties.
=====
Type:      Fathom
Status:    Enabled
Domain:    Fathom1
Container: FathomAdminServer1
Host:      MBASPAULDIXP2
Port:      6835
=====
```

10. Restart the AdminServer.

Note: All fmconfig command actions take effect only **after** the AdminServer has been restarted.

The following actions occur:

- The Fathom1.FathomAdminServer1.log file is created in the same directory as the AdminServer log file (admserv.log).
- The last line of the Fathom1.FathomAdminServer1.log file includes the following text:

```
(info) ...reconciling complete
```

- The admserv.log completes as usual, with the starting of the OpenEdge Management probe.

OpenEdge Management is now ready to monitor and configure remote systems, and OpenEdge Explorer is now ready to configure remote resources.

Setting up the second machine

Once you set up the machine that has both OpenEdge and OpenEdge Management/OpenEdge Explorer installed, you can set up the machine you want to monitor remotely. This second machine must have a supported version of OpenEdge or Progress installed.

Before you begin setting up the second machine, make sure the AdminServer is running on the first machine you set up.



To set up the second machine:

1. Stop the AdminServer.
2. Run the following command in the **Proenv** window:

```
fmconfig -host <machine-hostname> -enable
```

Where *<machine-hostname>* is the name of the host where OpenEdge Management or OpenEdge Explorer is running.

3. Press ENTER. Steps in the setup process are listed as they occur in the **Proenv** window, until the setup is complete. (Be sure to use the **Proenv** window and not the **Set OpenEdge Management Environment** window.)

For example:

```
Proenv
DLC: C:\Progress\OPENED~3
Inserting C:\Progress\OPENED~3\bin to beginning of path and
the current directory is
C:\OpenEdge\WRK
OpenEdge Release 10.2A as of Mon Nov 3 22:05:01 EST 2008
proenv>fmconfig -host nbaspauldixp2 -enable
OpenEdge Release 10.2A as of Mon Nov 3 22:05:01 EST 2008
Created property file C:\Progress\OPENED~3\properties\management.properties with
defaults
Unpacking files ... Done
Invoking 2nd phase of setup.
Determining configuration type ... Fathom NOT detected.
Configuring for remote monitoring by Fathom.
Enabling support for remote monitoring.
Connecting to Fathom JMS broker: nbaspauldixp2:6835
Connecting to Fathom directory services ... Done
Creating new container for host: NBDCKP5 ... Done
New container created: NBDCKP51
Adding components to container: NBDCKP51
Creating CONNECTION attribute set...
Creating COMPONENT attribute set for ManagementPlugin...
Creating COMPONENT attribute set for osmetrics...
Creating COMPONENT attribute set for AppServer...
Creating COMPONENT attribute set for Database...
Creating COMPONENT attribute set for NameServer...
Creating COMPONENT attribute set for SMDatabase...
Creating COMPONENT attribute set for WebSpeed...
Creating boot file: container.xml ... Done
Copying file to work directory: MFConfigurationElements.xsd C:\OpenEdge\WRK\
Remote monitoring of the adminserver is now ENABLED.

Settings take effect the next time the adminserver is started.

proenv>
```

Additionally, required files are created in the \$DLC/java/ext directory.

4. To verify that remote monitoring has been set up properly, run the following command in the **Proenv** window:

```
fmconfig -query
```

The remote monitoring properties appear:

```
proenv>fmconfig -query
OpenEdge Release 10.2R as of Mon Nov 3 22:05:01 EST 2008

=====
Fathom remote monitoring properties.
=====
Type:      Remote
Status:    Enabled
Domain:    Fathom1
Container: NBDCKP51
Host:      nbaspauldixp2
Port:      6835
=====
```

5. Restart the AdminServer.

Note: All `fmconfig` command actions take effect only **after** the AdminServer has been restarted.

The following events occur:

- The `Fathom1.<container-name>.log` file is created. The container name is generated by the Remote Monitoring Configuration Utility; the format of the name is *hostname+number*—for example, `PCTEST1`.
- The last line of the log file confirms that startup is complete. For example:

```
(info) Startup complete
```

- The `admserv.log` completes as usual.

Verifying that OpenEdge Management or OpenEdge Explorer can see the remote container

After you run the Remote Monitoring Configuration Utility on the OpenEdge Management/OpenEdge Explorer machine and the remote machine, you see the remote container in the OpenEdge Management/OpenEdge Explorer machine's console list frame.



To verify that the remote container is visible:

1. From the management console, select **Resources**.
2. In the list frame, sort the resources by **Container**. The newly added remote container is listed in the tree view in the list frame.

Remote monitoring configuration utility command-line options

The command-line options described in [Table 4-1](#) are available for use with the Remote Monitoring Configuration Utility. You run each command-line option in the **Proenv** window.

Table 4-1: Remote Monitoring Configuration Utility options

Command-line option	Description
-enable	Runs the configuration process and updates the following line in the <i>OpenEdge-install-dir/properties/management.properties</i> file: <code>isMonitored=true</code>
-disable	Updates the following line in the <i>OpenEdge-install-dir/properties/management.properties</i> file: <code>isMonitored=false</code>
-query	Reports the current settings for remote monitoring and configuration
-update	Reruns the configuration process and allows you to change the host your client connects to
-debug	Provides detailed information

The command-line options listed in [Table 4-2](#) are also available for use. Use caution, however, when running either option to ensure that remote monitoring continues to operate properly.

Table 4-2: Additional Remote Monitoring Configuration Utility options

Command-line option	Description
-port	Allows you to change the default listening port, which is 6835.
-name	Allows you to specify the container name. The default container name is <code><hostname>+1</code> .
-host	Identifies the remote host where OpenEdge Management/OpenEdge Explorer is running.

Disabling remote monitoring

If you want to stop remote monitoring, you can disable it by entering the following command from the **Proenv** window:

```
fmconfig -disable
```

Uninstalling if remote monitoring is configured

If you want to uninstall OpenEdge Management/OpenEdge Explorer from a UNIX platform and you configured remote monitoring or configuration, see the section about uninstalling OpenEdge Management/OpenEdge Explorer in *OpenEdge Management and OpenEdge Explorer: Installation* for details about how to complete the uninstall correctly.

If you are uninstalling OpenEdge Management/OpenEdge Explorer from a Windows platform and you configured remote monitoring, you need not take any steps other than those described in *OpenEdge Management and OpenEdge Explorer: Installation*. The uninstall process removes the remote monitoring settings along with the OpenEdge Management/OpenEdge Explorer installation.

Administering OpenEdge Management and OpenEdge Explorer

You can fine-tune the initial OpenEdge Management or OpenEdge Explorer configuration and licensing decisions you made, as described in the following sections:

- [Reviewing the configuration](#)
- [Updating licensing information](#)
- [Updating configuration options](#)
- [Adding users as administrators or operators](#)
- [Changing configuration settings](#)
- [Setting OpenEdge Management user preferences](#)
- [Changing the OpenEdge Management SNMP Adapter settings](#)
- [Setting OpenEdge Management user preferences](#)
- [Using the command-line interface](#)
- [Using the OpenEdge Management environment window](#)
- [Setting the log level for the AdminServer log file](#)

Reviewing the configuration

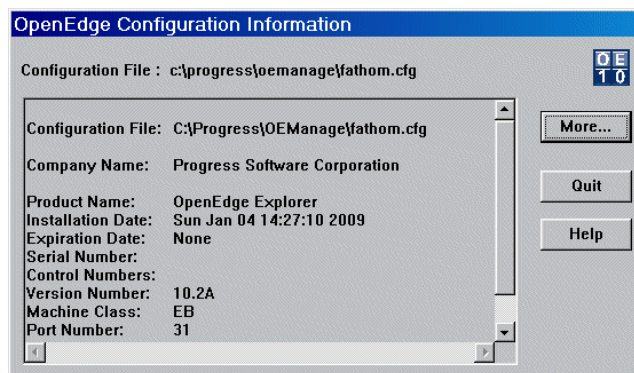
When you installed OpenEdge Management or OpenEdge Explorer, the installation program prompted you to enter serial and control numbers, which you found on the ESD site or, for OpenEdge Management, in the License Addendum that was included in your software package. The installation program recorded the license information in the configuration file, `fathom.cfg`.

Later, you can review the product installation and configuration information. This is helpful when you are considering whether adding other licensed products to your installation.



To review the current OpenEdge Management or OpenEdge Explorer product configuration:

1. Choose **Start**→**Programs**→**OpenEdge Management** or **OpenEdge Explorer**→**Config**. The **OpenEdge Configuration Information** dialog box appears and identifies the configuration information stored in `fathom.cfg`, as shown:



2. Review the configuration details provided, and scroll down to see configuration details for additional products that are installed (if applicable).

The display contains the following configuration details:

- **Configuration File** — The location of the `fathom.cfg` file
- **Company Name** — The name you entered during the installation

The display also provides the following information:

- **Product Name** — What you installed
 - **Installation Date** — When you installed it
 - **Expiration Date** — When the license expires
 - **Serial Number** — The number associated with the license agreement
 - **Control Numbers** — The numbers used by the installation software
 - **Version Number** — The software product version
 - **Machine Class** — The tier code associated with the license agreement
 - **Port Number** — The platform on which the software product is installed
3. To view and load another .cfg file, click **More**. Locate the file, and then click **Save**.
 4. Click **Quit** to close the dialog box.

Updating licensing information

You can update the OpenEdge Management or OpenEdge Explorer licensing information that you provided during the initial installation.



To update the OpenEdge Management or OpenEdge Explorer licensing information:

1. Choose **Start → Programs → OpenEdge Management or OpenEdge Explorer → License Update**.
2. Click **Yes**. The **OpenEdge Management Installed Versions** dialog box appears.
3. Select one of the installed versions, and click **Next**. The **Welcome** dialog box appears.
4. Click **Next**. The **Serial & Control Numbers** dialog box appears.
5. Enter the serial and control numbers for the product you want to install, and click **Accept**. Repeat this step for each product you are installing.
6. When you finish, click **Done**.

Updating configuration options

As you use OpenEdge Management or OpenEdge Explorer, you can update configuration options. You can update the initial options you established, and you can continue to make subsequent updates as you use and develop a better understanding of which settings work best for your environment.

From the management console, select **Options**. If you have OpenEdge Management installed, the list frame shown in [Figure 5–1](#) opens.

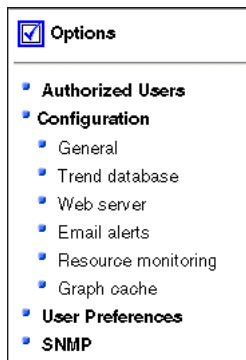


Figure 5–1: Options in OpenEdge Management list frame

If you have OpenEdge Explorer installed, the list frame shown in [Figure 5–2](#) appears.

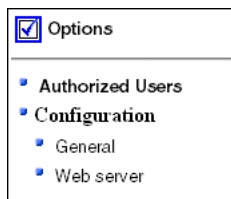


Figure 5–2: Options in OpenEdge Explorer list frame

Depending on whether you are working with OpenEdge Management, OpenEdge Explorer, or both, you can make modifications in one or more of the areas described in [Table 5–1](#).

Table 5–1: Configuration option availability

(1 of 2)

Option	Description	Applicable in OpenEdge Management	Applicable in OpenEdge Explorer
Authorized Users	Allows you to add or remove users; customize the operator role	Yes	Yes
Configuration			
General	Starts OpenEdge Management automatically when the AdminServer starts	Yes	Yes

Table 5–1: Configuration option availability*(2 of 2)*

Option	Description	Applicable in OpenEdge Management	Applicable in OpenEdge Explorer
Email alerts	Provides the e-mail address of the default recipient for e-mail notification when an alert is generated; also provides the SMTP mail server host name and port	Yes	No
Resource monitoring	Determines whether to automatically poll resources, generate alerts, collect trend data, and include status changes	Yes	No
Graph cache	Chooses the graph cache time period setting for resources and containers	Yes	No
User preferences	Selects the rate (if any) at which OpenEdge Management automatically refreshes; changes the default polling attributes for resource monitors	Yes	No
SNMP	(If installed) Starts or stops the SNMP Agent; changes one or more of the following values: SNMP agent port, default SNMP trap port, default SNMP read community, default SNMP write community, and autostarting of SNMP	Yes	No

By choosing to use the HTTPS protocol for secure browser-to-instance or instance-to-instance communications, you can further qualify current settings for:

- The Web server for OpenEdge Explorer and OpenEdge Management
- The OpenEdge Management Trend Database

See [Chapter 6, “Setting up Secure Communications,”](#) for details about using the secure protocol.

Adding users as administrators or operators

OpenEdge Management and OpenEdge Explorer provide two different user roles: administrator and operator. One predefined user with an administrator role is provided and is named **admin**.

An *administrator user* can add other users and specify their role. The administrator user has access to all OpenEdge Management or OpenEdge Explorer functionality. In OpenEdge Management, an administrator user can, for example, read all OpenEdge Management information, modify settings and configurations, set operations into action (such as starting or stopping the database), and delete resources and users. In OpenEdge Explorer, an administrator user can access and control certain database and OpenEdge server operations.

At a minimum, *operator users* can view configurations and configure their own views. Operators can also change their own passwords and descriptions. The operator role can be configured by administrators to give operator users access to more functionality.

If a user's role changes from administrator to operator and the user is logged on at the time, any operator restrictions become effective for that user immediately. In other words, the links or buttons, for example, that operators no longer have access to become disabled immediately for the affected user.

User accounts are defined solely within OpenEdge Management or OpenEdge Explorer. They define who can log in using a Web browser.

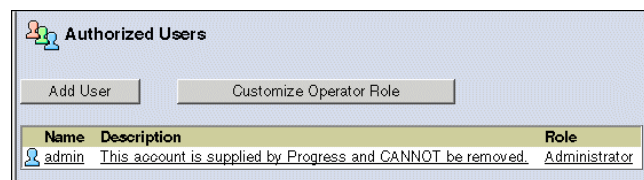
Managing the authorized users list

The authorized users list provides information about users authorized to access OpenEdge Management or OpenEdge Explorer.



To view the list of authorized users:

1. From the management console menu bar, select **Options**.
2. Select **Authorized Users** in the list frame. The **Authorized Users** page appears:



The **Authorized Users** page shows the one predefined admin user. The list of users on the page is dynamic; the name and description details are added and removed from this list as you add and delete users.

Note that you cannot delete the predefined admin user, although you can modify its password.

Customizing the operator role

As an administrator, you can determine which functionality operators can access. If you make no changes to the default permissions OpenEdge Management or OpenEdge Explorer assigns to operators, the operators are restricted to read-only permissions.

Note that the permissions you define affect all operators equally.



To set up operator role customization:

1. From the **Authorized Users** page, click **Customize Operator Role**. The **Operator Role Customization** page appears.

Within OpenEdge Management, the page consists of the following areas of operator permission: **Database operations**, **OpenEdge operations**, **Resource and monitor operations**, and **Task operations**, as shown:

Database operations:	
Alerts	
Clear Alerts	<input type="checkbox"/>
Database	
Start/Stop Database	<input type="checkbox"/>
Start/Stop Agent	<input type="checkbox"/>
Scripted Database	
Stop Agent	<input type="checkbox"/>

OpenEdge operations:	
AppServer	
Start/Stop AppServer Broker	<input type="checkbox"/>
Add/Trim AppServer Server Pool	<input type="checkbox"/>
Kill AppServer Server Process	<input type="checkbox"/>
MSS DataServer	
Start/Stop MSS DataServer	<input type="checkbox"/>
NameServer	
Start/Stop NameServer	<input type="checkbox"/>
ODBC DataServer	
Start/Stop ODBC DataServer	<input type="checkbox"/>
Oracle DataServer	
Start/Stop Oracle DataServer	<input type="checkbox"/>
SonicMQ Adapter	
Start/Stop SonicMQ Adapter	<input type="checkbox"/>
Web Services Adapter	
Web Services Operations	<input type="checkbox"/>
Deployed Web Services Operations	<input type="checkbox"/>
WebSpeed	
Start/Stop WebSpeed Broker	<input type="checkbox"/>
Add/Trim WebSpeed Agent Pool	<input type="checkbox"/>
Kill WebSpeed Agent Process	<input type="checkbox"/>

Resource and monitor operations:			
	Create & Edit	Delete	
Database			
Database	<input type="checkbox"/>	<input type="checkbox"/>	
OpenEdge			
AppServer	<input type="checkbox"/>	<input type="checkbox"/>	
AppServer Internet Adapter	<input type="checkbox"/>	<input type="checkbox"/>	
Messengers	<input type="checkbox"/>	<input type="checkbox"/>	
MSS DataServer	<input type="checkbox"/>	<input type="checkbox"/>	
NameServer	<input type="checkbox"/>	<input type="checkbox"/>	
ODBC DataServer	<input type="checkbox"/>	<input type="checkbox"/>	
Oracle DataServer	<input type="checkbox"/>	<input type="checkbox"/>	
SonicMQ Adapter	<input type="checkbox"/>	<input type="checkbox"/>	
Web Services Adapter	<input type="checkbox"/>	<input type="checkbox"/>	
WebSpeed	<input type="checkbox"/>	<input type="checkbox"/>	
System			
File	<input type="checkbox"/>	<input type="checkbox"/>	
Network	<input type="checkbox"/>	<input type="checkbox"/>	
System	<input type="checkbox"/>	<input type="checkbox"/>	
Library			
Actions	<input type="checkbox"/>	<input type="checkbox"/>	
Search Criteria	<input type="checkbox"/>	<input type="checkbox"/>	
Rule Sets	<input type="checkbox"/>	<input type="checkbox"/>	
Schedules	<input type="checkbox"/>	<input type="checkbox"/>	

Task operations:			
	Create & Edit	Delete	Run
Reports			
Report Templates	<input type="checkbox"/>	<input type="checkbox"/>	
Reports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jobs			
Job Templates	<input type="checkbox"/>	<input type="checkbox"/>	
Jobs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

With OpenEdge Explorer, the areas of operator permission are **Database operations** and **OpenEdge operations**.

2. Choose one of the following methods to define operator functionality:
 - Select each individual option that you want to make available to operators.
 - Click **Select All** to choose all options.
 - Click **Select None** to clear all options.

Note: If you select the **Start/Stop Database** check box under **Database**, the **Start/Stop Agent** check box is automatically selected. You can, however, select **Start/Stop Agent** without selecting **Start/Stop Database**.

The only option under **Scripted Database** that is available to operators is to stop the remote database agent.

3. When you finish, click **Submit**.

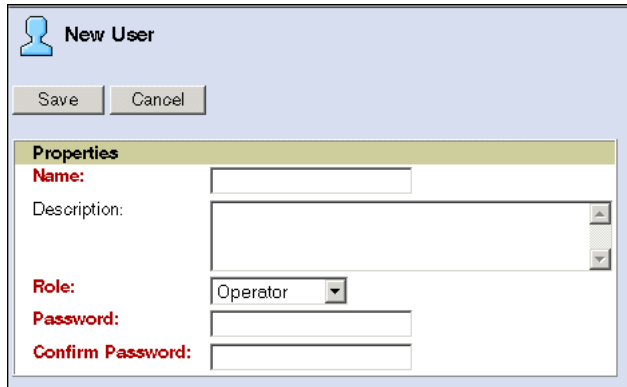
Adding a new user

If you are logged in as an administrator in OpenEdge Management or OpenEdge Explorer, you can add new users.



To add a new user:

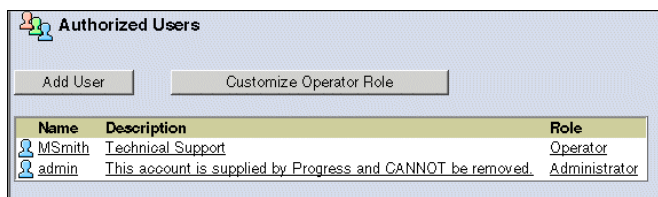
1. From the **Authorized Users** page, click **Add User**. The **New User** window appears:



The **New User** dialog box contains the following fields and controls:

- Buttons:** **Save** and **Cancel**
- Properties Section:**
 - Name:** Text input field
 - Description:** Text input field with a vertical scrollbar
 - Role:** Dropdown menu with **Operator** selected
 - Password:** Text input field
 - Confirm Password:** Text input field

2. Enter a unique user name in the **Name** field. The name can contain up to 32 alphanumeric characters. (Spaces are not allowed.)
3. Enter an optional description of the user.
4. Choose a role for the user: **Administrator** or **Operator**.
5. Enter a password for this user in the **Password** field. The password must be between 4 and 16 characters in length.
6. Re-enter the same password in the **Confirm password** field.
7. Click **Save**. The user name and description you added appear on the list of authorized users on the **Authorized Users** page, as shown:



The **Authorized Users** dialog box shows a list of users with the following structure:

Name	Description	Role
MSmith	Technical Support	Operator
admin	This account is supplied by Progress and CANNOT be removed.	Administrator

Buttons: **Add User**, **Customize Operator Role**

Changing passwords and descriptions

Whether you are an administrator or an operator, you can change your own unique password and/or your description from the **Authorized Users** page at any time. Administrators can edit anyone's password or description, but operators are restricted to editing only their own password and description.

If an administrator changes a user's password, that user is presented with a login screen when next accessing OpenEdge Management or OpenEdge Explorer. When the user provides the correct password, the user can resume working. If, however, the user does not enter the correct password, the user's login fails and access is denied.



To change the password and/or description:

1. From the users listed on the **Authorized Users** page, click the name of the user whose properties you want to change. The **User** page appears:

User: MSmith	
Edit	Copy
Delete	
Properties	
Name:	MSmith
Description:	Technical Support
Role:	Operator

2. Click **Edit** or **Copy** to either edit the user details or copy them as the basis for another user. If you copy the details, you must change the user name, since duplicate user names are not allowed.

Note: If you change the password by entering the new password once in the **Password** field, you must also enter it again in the **Confirm Password** field.

3. Click **Save**. The **User** page redisplay, showing any changes that you might have made to the user name or description details.

Changing the Admin password

During the initial access of OpenEdge Management or OpenEdge Explorer, you reset the default admin user's password on the **Configuration** page. Each subsequent update you make to the admin password must be done by using the **Authorized Users** page. See the steps in the [“Changing passwords and descriptions”](#) section on page 5–11 for more information.

Deleting users

To delete users from the **Authorized Users** list, you must be logged on as an administrator. You cannot delete the admin user.



To delete users:

1. Select the user whom you want to delete from the **Authorized Users** list.
2. Click **Delete** at the top of the page. A confirmation window appears before the user's privileges are deleted.
3. Click **OK**. The deleted user's access to functionality is denied immediately.

Changing configuration settings

You can modify the initial configuration settings you established for OpenEdge Explorer or OpenEdge Management.

For OpenEdge Explorer, you can change the General and Web server protocol settings. See [Chapter 6, “Setting up Secure Communications,”](#) for protocol setting details.

For OpenEdge Management, you can change the following configuration settings by choosing **Options** from the menu bar:

- **General**
- **Email alerts**
- **Resource monitoring**

From the **Options** menu in OpenEdge Management, you can also:

- Set the graph cache.
- Change OpenEdge Management Web server and OpenEdge Management Trend Database protocol settings. See [Chapter 6, “Setting up Secure Communications,”](#) for details.

Changing general configuration settings

You can change the following current general configuration settings:

- The automatic starting of OpenEdge Management or OpenEdge Explorer when the AdminServer starts.
- The action OpenEdge Management or OpenEdge Explorer should perform, if any, when an internal alert is triggered. Set up the **On internal OpenEdge Management alerts perform action** panel to set an action for internal alerts, such as notification in OpenEdge Management that the OpenEdge Management Trend Database is down.

You can execute any action when an internal alert is triggered. For example, you can set an alert to trigger the **Default_Action**, which is a process that occurs in response to the status, availability, or performance of a monitored resource. For example, in this situation you can choose to associate the **Default_Action** to OpenEdge Management Trend Database operations, or select **None** to indicate that no alert triggers.



To change the general settings:

1. From the management console menu bar, select **Options**→**Configuration**→**General**. The **General Configuration** page appears in the detail frame and displays the current values, as shown:

2. Change one or both of the settings for the following options, as needed:
 - Select the **Start OpenEdge Management automatically** check box to start OpenEdge Management or OpenEdge Explorer automatically when the AdminServer starts.
 - (OpenEdge Management only) Click the **Action to perform on internal OpenEdge Management alerts** option to specify an action that OpenEdge Management performs when an internal alert is triggered.
3. Click **Submit**. The **General Configuration** page refreshes to reflect the changes you have made.

Changing OpenEdge Management e-mail alerts settings

You can change the current OpenEdge Management e-mail alerts configuration settings.



To change the e-mail alerts settings:

1. From the management console menu bar, select **Options**→**Configuration**→**Email alerts**. The **OpenEdge Management Email Alerts Configuration** page appears in the detail frame and displays the current e-mail alert settings, as shown:

2. Change one or more of the settings.
3. Click **Submit**.

Changing OpenEdge Management resource monitoring settings

You can either enable or disable the following current OpenEdge Management resource monitoring settings:

- Polling for all resources
- Generating alerts
- Collecting of resource trend data
- Including resource status changes in the trending

Each option is set independently of the others, with the exception of **Include status changes**. If you do not select the **Collect trend data** option, the **Include status changes** option is disabled.

These resource monitor options allow you to disable specific OpenEdge Management functionality. For example, if you know that your OpenEdge Management Trend Database is going to be taken down for maintenance, you could elect to turn off trending, but let the rest of the OpenEdge Management functionality continue to run.



To change the OpenEdge Management resource monitoring settings:

1. From the management console menu bar, select **Options**→**Configuration**→**Resource monitoring**. The **OpenEdge Management Resource Monitoring Configuration** page appears in the detail frame, as shown:

OpenEdge Management Resource Monitoring Configuration

Submit Cancel

Current resource monitoring settings

☒ Poll resources? Help

☒ Generate alerts?

Trending

☒ Collect trend data?

☒ Include status changes?

2. Select or clear each option.
3. Click **Submit**.

Setting the OpenEdge Management graph cache

OpenEdge Management graphing includes a persistent data cache. You determine how long you want to keep graph data cache persisted on a per resource instance basis. The default graph cache setting is 48 hours; however, you can change the setting to whatever value you want. Keep in mind that if you change the setting to a longer period of time, more disk space is used to store the growing cache. Additionally, the more data that has been stored, the more data there is to be represented in a graph, and the higher the CPU use will be at the time a graph using the data is created.

It is recommended that you start with the 48-hour default graph cache setting. You can then increase the value if you want, perhaps by small increments to see what the impact is to the disk space and CPU activity. You might consider setting certain resource types to the 48-hour default, and set others to a different time period, such as twelve hours, to save memory and CPU.

You select the graph cache settings for resources by choosing **Options** in the management console menu bar.



To set the OpenEdge Management graph cache:

1. From the management console menu bar, choose **Options**→ **Configuration**→ **Graph cache**. The **Graph Cache Database Configure** page appears:

Graph Cache Database Configure
Oct 17, 2006 5:45:37 PM

Time period setting to apply to selected resources

Sample time period to collect: ☒ hours ☐ days

Resources to operate on

Available Filter	Available	Selected
List resource of type: <input type="text" value="*"/>		
for container: <input type="text" value="*"/>		
<input type="button" value="Apply Filter"/>		
	<input type="button" value="Select All"/>	<input type="button" value="Select All"/>

Warning

Use this functionality with care. Substantial increases in the time period of retention of graph cache samples will result in large increases in disk space consumed by the graph cache samples (especially with regards to Database resources). Larger graph caches may also noticeably slow creation of graphs due to more substantial paging requirements to access the data.

2. In the **Sample time period to collect** field, type the graph cache time period you want to apply to the resources you plan to select. Then choose **hours** or **days**. The default time period is **48 hours**.

3. Select the resources to which you want the graph cache time period to apply to by following these steps:
 - a. In the **List resource of type** field, optionally select resource types either by choosing from the available resources or by choosing the wildcard (*).
 - b. In the **for container** field, optionally select the containers either by choosing from those available or by choosing the wildcard.

Note: When you use the wildcard, OpenEdge Management includes all *current* resources of the type or all container(s) you select. The wildcard does not apply, however, to any resources or containers you subsequently create. If you create a new resource, resource type, or container, you must set its graph cache time period.

4. Click **Apply Filter**. The resource types that match the filter specifications appear in the **Available** list, as shown in the following example:

Graph Cache Database Configure
Oct 17, 2006 5:54:56 PM

Time period setting to apply to selected resources

Sample time period to collect: ☒ hours ☐ days

Resources to operate on

Available Filter	Available	Selected
List resource of type: *	nbaspauldixp2.AppServer.asbroker1 <2 days> nbaspauldixp2.AppServer.esbbroker1 <2 days> nbaspauldixp2.AppServer.icfrepo <2 days> nbaspauldixp2.CPU.CPU <2 days> nbaspauldixp2.Database.Backorders <2 days> nbaspauldixp2.Database.FathomTrendDatabase <2 days> nbaspauldixp2.Disk.Disk-0_C_ <2 days> nbaspauldixp2.FileSystem.FileSys-C_ <2 days> nbaspauldixp2.Memory.Memory <2 days> nbaspauldixp2.WebSpeed.wsbroker1 <2 days> nbaspauldixp2.WebSpeed.wsdynamics1 <2 days>	

Warning

Use this functionality with care. Substantial increases in the time period of retention of graph cache samples will result in large increases in disk space consumed by the graph cache samples (especially with regards to Database resources). Larger graph caches may also noticeably slow creation of graphs due to more substantial paging requirements to access the data.

5. Select the resources:
 - To select all the resources in the **Available** list, click **Select All**. Then click the right arrow.
 - To choose one or more individual resources, highlight and click each resource you want to include; then click the right arrow.

The resources appear in the **Selected** list. The information in angle brackets to the right of each resource name is the current graph cache setting for that resource.

6. Review the **Selected** list. When you finish, click **Apply to selected**, as shown:

Apply to selected →

Graph Cache Database Configure
Oct 17, 2006 5:54:56 PM

Time period setting to apply to selected resources

Sample time period to collect: 24 ☒ hours ☐ days **Apply to selected**

Resources to operate on

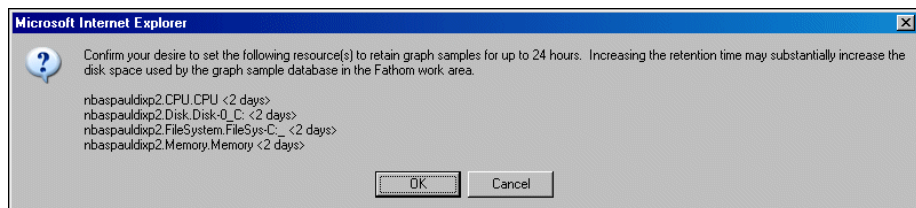
Available Filter	Available	Selected
List resource of type: * for container: * Apply Filter	* nbaspauldixp2.AppServer.asbroker1 <2 days> nbaspauldixp2.AppServer.esbbroker1 <2 days> nbaspauldixp2.AppServer.icrepos <2 days> nbaspauldixp2.Database.Backorders <2 days> nbaspauldixp2.Database.FathomTrendDatabase <2 days> nbaspauldixp2.WebSpeed.wsbroker1 <2 days> nbaspauldixp2.WebSpeed.wsdynamics1 <2 days>	nbaspauldixp2.CPU.CPU <2 days> nbaspauldixp2.Disk.Disk-0_C <2 days> nbaspauldixp2.FileSystem.FileSys-C_ <2 days> nbaspauldixp2.Memory.Memory <2 days>

Select All **Select All**

Warning


Use this functionality with care. Substantial increases in the time period of retention of graph cache samples will result in large increases in disk space consumed by the graph cache samples (especially with regards to Database resources). Larger graph caches may also noticeably slow creation of graphs due to more substantial paging requirements to access the data.

A message appears similar to the following (depending on which resources you select) confirming the resources you are about to affect:



7. Click **OK** to confirm. The **Graph Cached Database Configure** page appears.

8. To verify that the time period was changed correctly for the resources you selected, choose the resources and containers, and click **Apply Filter**. The **Available** list shows the resources whose graph cache time period is still set to the 48-hour default as well as those whose time period you have changed (perhaps to 24 hours), as shown in the following example:


Graph Cache Database Configure
 Oct 17, 2006 6:00:16 PM

Time period setting to apply to selected resources
 Sample time period to collect: ☒ hours ☐ days

Resources to operate on

Available Filter	Available	Selected
List resource of type: <input type="text" value="*"/>	nbaspauldixp2.AppServer.asbroker1 <2 days> nbaspauldixp2.AppServer.esbbroker1 <2 days> nbaspauldixp2.AppServer.icrepos <2 days> nbaspauldixp2.CPU.CPU <1 day> nbaspauldixp2.Database.Backorders <2 days> nbaspauldixp2.Database.FathomTrendDatabase <2 days> nbaspauldixp2.Disk.Disk-f0_C: <1 day> nbaspauldixp2.FileSystem.FileSys-C:_ <1 day> nbaspauldixp2.Memory.Memory <1 day> nbaspauldixp2.WebSpeed.wsbroker1 <2 days> nbaspauldixp2.WebSpeed.wsdynamics1 <2 days>	<input type="button" value="Select All"/>

Warning
 Use this functionality with care. Substantial increases in the time period of retention of graph cache samples will result in large increases in disk space consumed by the graph cache samples (especially with regards to Database resources). Larger graph caches may also noticeably slow creation of graphs due to more substantial paging requirements to access the data.

Setting OpenEdge Management user preferences

You can establish your own preferences for the following OpenEdge Management features:

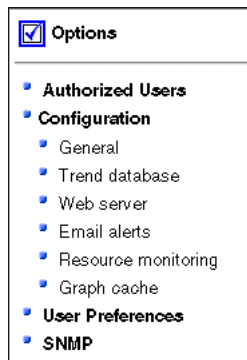
- The OpenEdge Management console page refresh rate
- The default polling and trending attributes for your OpenEdge Management resources: database, file, network, OpenEdge server, and system

You make these selections on the **User Preferences** page.



To set OpenEdge Management user preferences for page refresh and for default polling and trending:

1. Select **Options** from the management console menu bar. A list of options appears in the list frame, as shown:



2. Select **User Preferences**. The **User Preferences** page appears.
3. Continue with the [“Setting the OpenEdge Management page refresh option”](#) section on page 5–20.

Setting the OpenEdge Management page refresh option

From the **User Preferences** page, you can choose if and when you want the OpenEdge Management pages to refresh.

Consider your page refresh needs closely before establishing a setting. Frequent refreshing of menu, list, and detail frames adds to the processing time used by OpenEdge Management.

The current setting appears in the **Currently** field, as shown in [Figure 5–3](#).

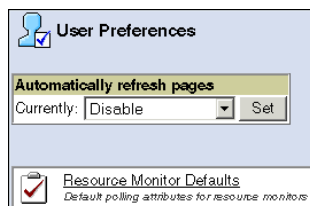


Figure 5–3: Refresh Pages page

The following refresh options are available:

- **Disable**
- **Every 30 seconds**
- **Every 45 seconds**
- **Every minute**
- **Every 2 minutes**
- **Every 5 minutes**
- **Every 10 minutes**
- **Every 30 minutes**



To change the refresh setting:

1. From the **Currently** drop-down list, select a new option.
2. Click **Set**. The following events occur:
 - The menu and detail frames are immediately refreshed.
 - The objects in the menu frame refresh according to your new setting.
 - Any time the list frame displays the **Alert List** page or the **Resources** page, these objects will be refreshed according to the new setting selected.

Remember that you can always click the **Refresh** icon, shown below, in the list control bar in the lower-left corner of the console:



Changing the OpenEdge Management SNMP Adapter settings

If you have installed the SNMP Adapter, you can change the current SNMP Adapter settings.



To change the SNMP Adapter settings:

1. Select **Options**→**Configuration**→**SNMP**. The **SNMP Adapter** page appears in the detail frame and displays the **SNMP agent status** and current settings:



You can also start or stop the SNMP agent from the **SNMP Adapter** page.

2. Click **Edit**. Change one or more of the following settings:
 - **Snmp agent port** — The port number of the host machine on which the SNMP management agent resides. The SNMP agent translates the requests from the SNMP management console and interprets MIB variables. The default port number is 8001.
 - **Default SNMP trap port** — The default port number to which traps are sent. The number is 8002.
 - **Default SNMP read community** — The community that specifies who has permissions to read which variables.
 - **Default write community** — The community that specifies who has permissions to write which variables. (In the case of the OpenEdge Management MIB, the values are read-only.)
 - **Autostart SNMP** — The option to autostart the SNMP agent.
3. Click **Submit**.

Setting OpenEdge Management resource monitor defaults

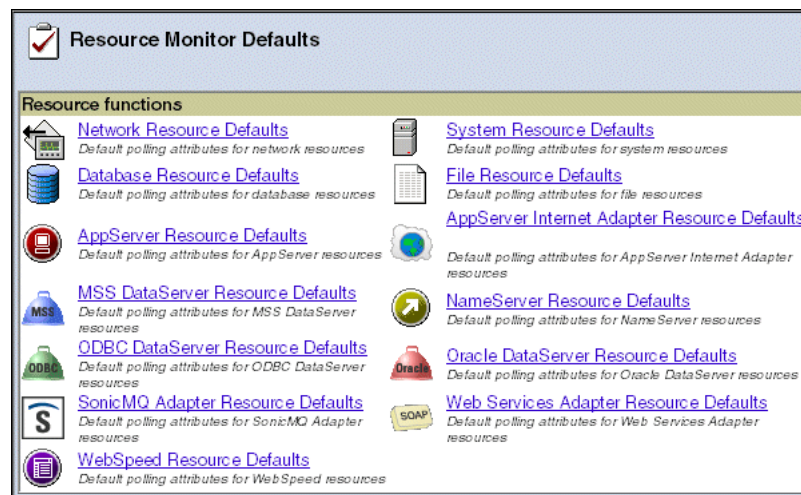
From the OpenEdge Management **User Preferences** page, you can set either default polling or default polling and trending attributes for the following resources:

- Network
- Database
- AppServer
- MSS DataServer
- ODBC DataServer
- SonicMQ Adapter
- WebSpeed
- System
- File
- AppServer Internet Adapter
- NameServer
- Oracle DataServer
- Web Services Adapter



To choose the default options:

1. Click **Resource Monitor Defaults**. The **Resource Monitor Defaults** page appears:



2. Click a resource category. The defaults page for that category appears.

3. Select the defaults.
4. When you finish setting the defaults, click **Submit**. A message appears confirming that the defaults have been successfully updated.



To return to the original OpenEdge Management defaults for a category, click **Restore Defaults** on the category's defaults page.

For more information about selecting resource monitor defaults for system, network, and file resources, see the relevant sections in *OpenEdge Management: Resource Monitoring*. For more information about selecting resource monitor defaults for databases, see the relevant section in *OpenEdge Management: Database Management*. For more information about selecting resource monitor defaults for OpenEdge server components, see the relevant section in *OpenEdge Management: Servers, DataServers, Messengers, and Adapters*.

Using the command-line interface

OpenEdge Management and OpenEdge Explorer provide a command-line interface that performs functions without the use of the graphical user interface.

Note: To use the command-line interface, HTTP must be enabled with **localhost** defined as a trusted client. See [Chapter 6, “Setting up Secure Communications,”](#) for details.

Specifically, the command-line interface allows you to:

- Start, query, and stop OpenEdge Management or OpenEdge Explorer.
- Dump the contents of the OpenEdge Management or OpenEdge Explorer configuration database to a readable form (an XML file) and, in the event of a catastrophic failure, use the backup dump file to restore the database.
- Access command-line help.

You can also use the command-line interface to work with alerts in the following ways:

- Clear an alert
- Enable and disable polling
- Work with alert commands

For details about working with alerts in the command line, see [OpenEdge Management: Alerts Guide and Reference](#).

Using the OpenEdge Management environment window

As a convenience, you can execute both OpenEdge Management and OpenEdge command-line utilities from an OpenEdge Management environment window. Access this window by choosing **Start**→**Programs**→**OpenEdge Management**→**Set OpenEdge Management Environment**. The environment window sets the shell environment variables needed for executing both OpenEdge Management and OpenEdge commands, as shown in [Figure 5-4](#).



Figure 5-4: Set OpenEdge Management Environment window

Starting, querying, and stopping from the command line

Use the following syntax to start, query, or stop OpenEdge Management or OpenEdge Explorer from the command line:

Syntax

```
fathom [-start | -query | -stop] <option>
```

[Table 5-2](#) describes the options you can use when starting or stopping from the command line.

Table 5-2: Command-line options for starting and stopping

Option syntax	Description
-host	Host where the AdminServer process resides.
-port	Port where the AdminServer runs. Default is 20931.
-timeout <time>	Time, in seconds, for OpenEdge Management or OpenEdge Explorer to wait for a response. The default is 240 seconds.
-user <user-name>	Username on machine where the AdminServer resides. The default is current user.
-password <user-password>	Password associated with the specified username. This is not needed for local connection. Note: Use of the -password parameter might allow others to see your password in clear text.

Examples

You want to connect to your AdminServer but you do not want to wait more than five minutes for the connection to be made. Enter the following syntax to start OpenEdge Management for OpenEdge Explorer from the command line (and assume that the AdminServer port is the default of 20931):

Syntax

```
fathom -start -timeout 30
```

Enter the following syntax to stop OpenEdge Management or OpenEdge Explorer from the command line and specify that the command-line interface tool wait five minutes before reporting an error (and assume that the AdminServer port is the default of 20931):

Syntax

```
fathom -stop -timeout 300
```

To learn the execution status of OpenEdge Management or OpenEdge Explorer with an AdminServer port number of 1905, enter the following syntax:

Syntax

```
fathom -query -port 1905
```

Dumping, backing up, and restoring the configuration database

Using the command-line interface, you can dump the OpenEdge Management or OpenEdge Explorer configuration database (fathom.odb), even while either one is running, to a readable XML file. You can use the dump file as a backup of the configuration database; in the event of a catastrophic failure, you can use the backup dump file to restore the configuration database. Because the dump file is readable, you can also use the file in OpenEdge Management when you are performing diagnostics.

You can also perform a dump and load to reduce the disk space that the configuration database is using.

Dumping the configuration database

You can dump the configuration database to a file whose name you specify by typing the following command:

```
fathom -dump <filename>
```

The resulting file will be in XML format and will contain an XML representation of all definitions in the configuration database. You can use this resulting file in OpenEdge Management, for example, either as a potential single-file backup of the database or to assist with diagnostics regarding database performance.

Note that you can run the dump command when both the AdminServer and OpenEdge Management/OpenEdge Explorer are running, or when they are both not running. You cannot dump the configuration if OpenEdge Management or OpenEdge Explorer is a plugin of the AdminServer but has been stopped.

You can also use the `-httpport` argument, as follows, to identify the port of the OpenEdge Management or OpenEdge Explorer Web server:

```
fathom -httpport <port-number> -dump <filename>
```

Restoring the configuration database from a backup file

You can load a dump file you created from the configuration database. To run the load command, be sure that OpenEdge Management or OpenEdge Explorer is offline; if either is running, you must stop the AdminServer before you run the command.

To load the file, type the following command:

```
fathom -load <filename>
```

The `-load` command recreates the configuration database and populates it with definitions in the file whose name you specify.

Reducing configuration database disk space usage

You can perform both the `-dump` and `-load` commands to reduce the amount of disk space consumed by the configuration database. You might want to perform this reduction in space if OpenEdge Management or OpenEdge Explorer has been performing a lot of resource modifications over an extended period of time, in which case some database fragmentation might have occurred causing more disk space to be consumed than is actually required.

Note that OpenEdge Management or OpenEdge Explorer must be offline when you run the `-load` command. If either is online, be sure to stop the AdminServer.



To dump the data, do the following:

1. Select **Start→Programs→OpenEdge Management** or **OpenEdge Explorer→Set OpenEdge Management Environment**.
2. Dump the `fathom.o*` files by using either of the following commands:

```
fathom -dump <filename>
```

```
fathom -dump <filename> [-httpport<portNumber>]
```

where `<filename>` is the name of the xml file created that contains the dumped contents of the `fathom.odt` database and `<portNumber>` is the port that OpenEdge Management/OpenEdge Explorer is running on. The default port number is 9090.

3. Load the dumped file using the following command:

```
fathom -load <filename>
```

Accessing command-line help


To access help about any command-line option, use the following:

```
fathom -help -command
```

To access help for the `-stop` command, enter the following:

```
fathom -help -stop
```

The help information shown in [Figure 5–5](#) appears.



```
Set OpenEdge Management Environment
proenv>fathom -help -stop
Fathom Version 10.2A as of Mon Jan 19 04:12:48 EST 2009
Usage: fathom -stop [options]

options:
  -help                Print this message.
  -port <port>         Port where AdminServer Process resides.
                        Default is 20931.
  -timeout <time in sec> Time <in seconds> for fathom to wait for a response.
  -host <hostname>      Host name where the Adminserver process resides.
  -user <username>      Username on machine where the AdminServer process
                        resides.
  -password <password> *The password associated with the username specified.

* Note: use of this parameter may allow others to see your password in clear
text.
proenv>_
```

Figure 5–5: Command-line help for `-stop`

Setting the log level for the AdminServer log file

The AdminServer log (`admserv.log`) records AdminServer activity. The log is located in the OpenEdge Work directory. You can determine how much information is written to the log file by setting the log level.



To set the log level in Windows or on UNIX:

1. Open the following file in a text editor:

```
OpenEdge-install-dir\properties\AdminServerPlugins.properties
```

2. Locate the `[PluginPolicy.Progress.AdminServer]` section.
3. Add the following to the `jvmargs` line:

```
-DLogLevel=n
```

In which *n* is a number from 1 to 5. The default is 3. Log level 5 provides the highest level of verbose information.

4. Save the file.

Setting up Secure Communications

As you monitor resources and trend data using OpenEdge Management, one of your primary considerations will be the security of the data as it is transferred over the Internet.

This chapter describes how to use the HTTPS protocol with the Web server for OpenEdge Management or OpenEdge Explorer and with OpenEdge Management for the OpenEdge Management Trend Database, as outlined in the following sections:

- [Transferring data securely with the HTTPS protocol](#)
- [Understanding common SSL terminology](#)
- [Getting started: using the demo certificate](#)
- [Changing Web server settings](#)
- [Changing OpenEdge Management Trend Database settings](#)
- [Using SSL](#)
- [Using your own certificate](#)
- [Using the keytool utility](#)

Transferring data securely with the HTTPS protocol

As you work with OpenEdge Management and OpenEdge Explorer, you want to ensure that data being transferred between the Web browser and the Web server is secure. With OpenEdge Management, you might also require the same level of security when you trend performance data if the trend database is located on a remote machine. In cases in which you are sending or receiving sensitive data, the security of the communications is essential.

You can use the HTTPS protocol for communications between the Web browser and the OpenEdge Management or OpenEdge Explorer Web server, as well as between an OpenEdge Management instance and a remote trending database. The HTTPS protocol with Secure Sockets Layer (SSL) encrypts data through the use of a public/private key pair and a signed certificate, thereby making sure that both the client and the server (or, as in the case of OpenEdge Management and OpenEdge Explorer, a Web browser and the Web server) can authenticate each other's identity. If you are trending data to a remote database, you can ensure that communication between the two machines is secure.

Using the demo certificate or your own certificate

To help you get started using the SSL protocol, OpenEdge Management and OpenEdge Explorer include a demo keystore and certificate, valid for approximately one year, that you can set up on a nonproduction system. If you prefer (or if you want to set up SSL on a production system), you can generate your own certificate or use one that you acquire from a certificate authority.

Instructions for setting up SSL by either method are provided here.

Understanding common SSL terminology

As you prepare to establish secure communications of OpenEdge Management and OpenEdge Explorer data, there are several terms with which you should be familiar.

Data encryption

A method of translating data into a code that is indecipherable without a special key or password. The sender of the data encrypts it, and the receiver of the data decrypts it.

Encrypted data is also known as *cipher text*.

SSL handshake

A communication that allows the server to identify (authenticate) itself to the client by sending a certificate. The client uses the certificate to verify that the sender is who it claims to be.

Public and private key pair

The combination of a sender's *public key*, which is common knowledge, and a *private key*, which is known only by the recipient of an Internet communication. For example, if a server wants to send a secure communication to a client, the server uses the private key to encrypt the contents of the message. The client then uses its public key to decrypt the encrypted message.

Keystore

A database that functions as a repository for the certificates and keys.

Keytool

A key and certificate management utility, developed by Sun Microsystems, that allows you to administer your own private/public key pairs and associated certificates. You then use these keys and certificates for self-authentication (in which you authenticate yourself to other users or services) using digital signatures.

X.509

A commonly used standard for defining digital certificates.

Certificate

An attachment included in a network communication for the purposes of security. A certificate allows the recipient of the communication to verify that the sender is as claimed and allows the recipient to return to the sender an encrypted response.

A certificate is issued by a Certificate Authority (CA).

Each certificate is a dated entity that has a limited lifespan. A typical certificate is issued for a year; however, a trial certificate will likely be valid for a shorter period of time, perhaps for fourteen days.

You can typically obtain a 14-day trial certificate from a certificate/security company such as Verisign (<http://www.verisign.com>).

Certificate Authority

A provider of encrypted digital certificates. The CA signs the certificate request and chains it to its root certificate.

Root certificate

A certificate that identifies the Certificate Authority. A root certificate is self-signed, meaning it does not chain to another certificate to establish trust. If a certificate user, such as a browser, does not recognize a particular certificate, it walks the chain for a parent that it does know, until it reaches the root.

Digital signature

A signature on a certificate from a trusted Certificate Authority.

procertm utility

A utility you can use to add any Certificate Authority's root certificate to the trend trust keystore, if the root certificate is not already there. You can also use the procertm utility to convert digital certificates between certificate file types (.der and .pem).

Getting started: using the demo certificate

If you want to get up and running with SSL quickly, you can use the demo certificate that OpenEdge Management and OpenEdge Explorer provide and set up the HTTPS protocol for communication with the Web server.

If you are using OpenEdge Management, you can also set up secure communication with a remote OpenEdge Management Trend Database.

Caution: This demo certificate is not intended for use in a production environment.

Configuration update errors or warnings

In the event that you make an update to the Web server or OpenEdge Management Trend Database configuration and the update is not successful, an error message appears, describing the issue. Additionally, a red letter X appears next to the field that prompted the generation of the error. The presence of one or more errors stops the update; click **OK** to close the error message.

If you make an update to the configuration and a warning is generated, an alert box appears and describes the particular warning. Additionally, a blue question mark appears next to the field that prompted the warning. Unlike what happens when an error is detected during a configuration update, the warning does not stop the update from proceeding; it is simply an informational reminder to you that you might want to reconsider implementing the configuration update.

If you make a change in configuration and the change does not appear to have taken effect, consult the AdminServer log (`admserv.log`), which is located in your OpenEdge Work directory, for details.

Identifying trusted clients

As you update the configuration of either the Web server (or the OpenEdge Management Trend Database, if available in your configuration), you can optionally identify one or more trusted clients who are allowed to connect to the OpenEdge Management or OpenEdge Explorer instance using the designated protocol. If you want to list more than one trusted client, separate each entry by a comma.

You can use the trusted clients feature to allow a few well-known clients (or even an entire subnet) to connect unsecured to OpenEdge Management for convenience and possible performance reasons, while requiring all other clients to use a secured connection. For example, you might want to establish that you use the HTTP protocol for intranet connections and the HTTPS protocol for any Internet connections (for example, coming through a firewall).

You can identify a trusted client by using any of the following formats:

- DNS name (for example, **pcjoe**)
- A dot-formatted address string (for example, **123.123.123.123**)
- A wildcard dot-formatted address string (for example, **123.123.123.***)

Independent of how you configure trusted clients, you are always able to connect from the local host. If you leave the trusted clients list empty, any client can connect.

Reconnecting after updates

Note that changes you make to the configuration might require that you reconnect (log in again) to OpenEdge Management or OpenEdge Explorer. If logging in again is necessary, you are prompted to do so.

Changing Web server settings

When you perform the initial OpenEdge Management or OpenEdge Explorer configuration, you identify the Web server port you plan to use. Although you cannot choose to use the HTTPS protocol when you are making your initial configuration decisions regarding the Web server (as described in [Chapter 2, “Setting Up OpenEdge Management or OpenEdge Explorer for the First Time”](#)), you can make that choice later by updating the configuration options. You can change the port number, and you can also decide whether to use HTTP only, HTTPS (SSL) only, or both HTTP and HTTPS (SSL). If you choose to use both the HTTP and HTTPS protocols, you can define for both protocols a list of trusted clients.

For example, you might prefer to restrict the clients you want to talk to OpenEdge Management without SSL. For HTTP, you might put the local host (or create a subnet of local users to use HTTP) as the trusted client. For HTTPS, you can open data transfer to anyone, keeping in mind that it might add some overhead to communications.

Note: To use the existing command-line interface, HTTP must be enabled with **localhost** defined as a trusted client.



To change the Web server settings:

1. Select **Options**→ **Configuration**→ **Web server**. The **Web Server Configuration** page appears in the detail frame and displays the current Web server settings.
2. Choose from the following protocol options:
 - If you want to allow HTTP connections, select the **Enable HTTP protocol** option. Type the port number in the **HTTP port** field.
 - If you want to allow HTTPS connections, select the **Enable HTTPS protocol** option. Type the port number in the **HTTPS port** field.
 - If you want to allow both HTTP and HTTPS connections, select both the **Enable HTTP protocol** option and the **Enable HTTPS (SSL) protocol** option. Then type the port numbers in the **HTTP port** field and the **HTTPS port** field.
3. Choose one of the following options:
 - If you want to work with the demo keystore, click **Submit**. See the [“Using SSL”](#) section on page 6–16 for details about using an HTTPS connection.
 - If you are an advanced user and you want to change keystore information, continue with the [“Using advanced HTTP and HTTPS options with the Web server”](#) section on page 6–8.

Using advanced HTTP and HTTPS options with the Web server

You can use the following advanced options when configuring the use of HTTP or HTTPS:

- Use a Trust Keystore other than the demo provided by OpenEdge Management or OpenEdge Explorer.
- Identify trusted clients for HTTP and/or HTTPS.



To use the advanced options:

1. From the **Web Server Configuration** page, click **Advanced Options**. The expanded **Web Server Configuration** page appears:

2. Under **HTTP Configuration**, type the name of one or more trusted clients in the **Trusted clients** field. If you type more than one trusted client, use a comma-delimited list.

You can identify trusted clients by machine name, subnet, or IP address.

Under **HTTPS Configuration**, notice that the following fields are prefilled with data taken from the demo keystore, which is `demoWebServerIdentityKeystore.jks`:

- **Keystore path name**
- **Keystore pass phrase**
- **Alias**
- **Alias pass phrase**

The **Keystore pass phrase**, **Alias**, and **Alias pass phrase** are all case-sensitive.

The following details relate to the demo certificate information:

- **Owner** — The Common (CN) and Organization (O) name components of the Distinguished Name (DN), whose public key the certificate identifies. For the demo, the owner is Demo or localhost, Progress Software Corp.

Note that most popular browsers expect the common name portion of the owner name to be the DNS host name of the machine that is using the certificate for SSL. If a certificate has a different common name, as does the demo certificate, the browser notifies you of the difference when you connect to a Web server using this certificate.

- **Issuer** — The Common (CN) and Organization name components of the Distinguished Name (DN), the organization that signed the certificate.
 - **Type** — The type of certificate. X.509 is the most widely accepted format and is currently the only format supported by the JDK keytool. This is also the default format used by SSL.
 - **Public key** — The algorithm used to generate the public/private key pair. This should always be RSA, which is the only algorithm that some browsers recognize.
 - **Signature algorithm** — The algorithm used by the CA to sign the certificate.
 - **Version** — The version of the X.509 standard that applies to this certificate. There are currently three certificate versions: V1, V2, and V3.
 - **Valid from** — The dates for which the certificate is valid.
3. Type the name of one or more trusted clients in the **Trusted clients** field. If you type more than one trusted client, use a comma-delimited list.
 4. Click **Submit**. A message appears confirming that the configuration has been successfully updated.
 5. Click **OK**.

Changes you make to the configuration might require you to reconnect (log in again) to OpenEdge Management or OpenEdge Explorer.

Changing OpenEdge Management Trend Database settings

You determine whether the OpenEdge Management Trend Database stores trend data in a local or remote OpenEdge Management database. For trending to a local database, you specify the local database path name and the local database port when you initially configure OpenEdge Management. For trending to a remote OpenEdge Management instance, you specify the remote OpenEdge Management host name and the OpenEdge Management Web server port. (These initial configuration steps are described in [Chapter 2, “Setting Up OpenEdge Management or OpenEdge Explorer for the First Time.”](#))

Although you cannot choose to use the HTTPS protocol when you are making your initial configuration decisions regarding the location of the OpenEdge Management Trend Database, you can make that choice afterwards by updating the configuration options. If you have a client that needs to get through a firewall, you can also configure trending to use a proxy server instead of connecting directly to the Internet.

For HTTPS, you can open data transfer to anyone, keeping in mind that it might add some overhead to communications.

If you choose to trend to a scripted database and use the HTTPS protocol, the machine on which the database resides must have HTTPS enabled in the Web server configuration.



To store trend data in a managed OpenEdge Management database:

1. Select **Trend database** in the list frame. The **OpenEdge Management Trend Database Configuration** page appears in the detail frame and displays the current trend database settings.
2. Select **Store trend data in a local OpenEdge Management database**.
3. Type the database path name (for example, **C:\Progress\OEManage\db\Fathom.db**). (Note that the inclusion of the **.db** extension is optional when you provide the path name.)
4. Type the database port number (for example, **1234**).
5. Click **Submit**.

**To store trend data in a remote OpenEdge Management instance:**

1. Select **Trend database** in the list frame. The **OpenEdge Management Trend Database Configuration** page appears in the detail frame and displays the current trend database settings.
2. Select **Store trend data in a remote OpenEdge Management instance**.
3. Type the host name in the **OpenEdge Management host name** field.
4. Type the remote OpenEdge Management Web server port number in the **OpenEdge Management port** field. Typically, the number is **9090** for HTTP or **9443** for HTTPS.
5. To use HTTPS, select the **Use HTTPS (SSL) protocol** option.
6. Choose one:
 - If you want to work with the demo keystore and are not using a proxy server, click **Submit**. See the [“Using SSL”](#) section on page 6–16 for details about using an HTTPS connection.
 - If you are an advanced user and you want to change keystore information or use a proxy server, continue with the [“Using advanced HTTPS options when trending remotely”](#) section on page 6–11.

Using advanced HTTPS options when trending remotely

If you want to use HTTPS for communications with a remote OpenEdge Management Trend Database, you can also use the following advanced options:

- A Trust Keystore other than the demo provided by OpenEdge Management
- A proxy server



To use the advanced options:

1. From the **OpenEdge Management Trend Database Configuration** page, click **Advanced Options**. The expanded **OpenEdge Management Trend Database Configuration** page appears:

Under HTTPS Configuration, the full path name to the demo keystore (demoTrendTrustKeystore.zip) appears in the **Keystore path name** field.

Note: Although the demo keystore is a .zip file, the .zip file format is not a requirement for a keystore. You can also use a .cer file or a .pem file as the keystore.

2. To use a keystore other than the demo, type the keystore name in the **Keystore path name** field.
3. If you want to use a proxy server, do the following:
 - a. Select the **Use a Proxy server** check box.
 - b. Type the host name in the **Proxy host name** field.
 - c. Type the server port number in the **Proxy server port** field.
4. Click **Submit**. A message appears confirming that the configuration has been successfully updated.
5. Click **OK**.

Note that changes you make to the configuration might require you to reconnect (log in again) to OpenEdge Management.

Using the procertm utility

If you are using HTTPS for communications with a remote OpenEdge Management Trend Database, you use the demo keystore — `demoTrendTrustKeystore.zip` — to validate the SSL connection from the OpenEdge Management installations that are trending to a remote management console (the location of the OpenEdge Management Trend Database). The Digital Certificate that identifies the Certificate Authority who issued the remote management console's digital certificate must be in the `demoTrendTrustKeystore.zip` for the validation to succeed.

The `demoTrendTrustKeystore.zip` file contains a number of trusted root digital certificates for an OpenEdge Management demo and common, public Certificate Authorities. It is not typically necessary for you to modify the file; however, the `demoTrendTrustKeystore.zip` file contains neither the digital certificate for every public Certificate Authority nor certificates for any privately run company Certificate Authority.

You can obtain the distributed list of certificates by running the `procertm` utility and listing the contents of the `demoTrendTrustKeystore.zip` file certificate store. You can also use the `procertm` utility to add any Certificate Authority's root certificate to the `demoTrendTrustKeystore.zip`, if not already there.

If the remote management console's issuing Certificate Authority is not already present, you must first follow these steps:

1. Contact the CA who issued the management console's digital certificate and obtain the CA's trusted Root Digital Certificate. This may be returned in either PEM (`.0`, `.txt`, or `.pem`) or DER (`.cer` or `.crt`) format.
2. If the CA root digital certificate is in a PEM format (with a file extension of `.0`, `.txt`, or `.pem`), use the `procertm` tool to convert it to DER format (identified with a `.cer` file extension).
3. Use the `procertm` tool to import the DER-formatted CA digital certificate into the `demoTrendTrustKeystore.zip` certificate store.

Managing the trust keystore with procertm

You run the `procertm` utility from a command line using the following syntax:

Syntax

```
procertm [options] cert_store
```

Where:

- `cert`

The path to the digital certificate you want to import, export, or remove. This is used with the `-i`, `-e`, and `-r` options. When importing, the path is relative to the working directory. When exporting or removing digital certificates from `cert_store`, the path is the full digital certificate path specified in `cert_store`. Subdirectories should be specified with a forward slash (`/`). You can use multicharacter (`*`) and single-character (`?`) wildcards in the `cert` filename and file extension.

- `cert_store`

The path to the zip or jar certificate store file. If the certificate store file does not exist, and you are importing digital certificates, a new file is created.

When you run `procertm`, it performs the options in the following order:

1. Imports any certificates specified with the `-i` option from the working directory into `cert_store`. If a certificate is not found, a warning message displays.
2. Exports any certificates specified with the `-e` option from `cert_store` to the working directory. If a certificate is not found, a warning message displays.
3. Removes any certificates specified with the `-r` option from `cert_store`. If a certificate is not found, a warning message displays.
4. Shows the resulting `cert_store` file contents, if the `-l` option is specified.
5. Prints any digital certificate list information, if the `-p` option is specified.

You can provide the following options in any combination and in any order:

- `-v`

Prints verbose information about the progress of the digital certificate's import and export. When used with `-l`, additional digital certificate field information is printed.

- `-l`

Lists the contents of the `cert_store` file after all import, export, and remove operations are completed.

- `-p`

Prints the digital certificate list the `cert_store` contents to the file `cert_store.dcl`, after all import, export and remove operations are completed.

- `-i cert`

Imports certificate file(s) matching `cert` to `cert_store` from the working directory. The `cert_store` file is created as required. You can specify this option multiple times. See the definition of `cert`.

- `-e cert`

Exports the certificate file(s) matching `cert` from `cert_store` to the working directory. Any subdirectories are created if required. You can specify this option multiple times. See the definition of `cert`.

- `-r cert`

Removes the certificate file(s) matching `cert` from `cert_store`. You can specify this option multiple times. See the definition of `cert`.

- `-d`

Sets the working directory path where certificates are imported from or exported to. The default is the current working directory.

Converting digital certificates with procertm

You can use the `procertm` utility to convert digital certificates between `.DER` and `.PEM` file formats. To convert files from one file format to the other, use the following command line syntax:

Syntax

```
procertm -c in_cert out_cert
```

Where:

- `in_cert`

The digital certificate whose file format you want to convert.

- `out_cert`

The file format to which you want to convert the digital certificate. `Procertm` performs the conversion based on the file-extension type. For example, if `in_cert` has a file extension type of `.crt` and `out_cert` has a file extension type of `.pem`, `in_cert` is converted from `.der` to `.pem` format and written to the file `out_cert`.

Using SSL

Once you configure the Web server to use SSL, enable the HTTPS protocol on a port, and identify a valid identity keystore and certificate, you can connect to OpenEdge Management or OpenEdge Explorer by using the HTTPS protocol.

In the browser's **Address** field, type the following command:

```
https://<host-name>:<port-number>
```

Where:

- *host-name*

Either the DNS name or the dot-formatted address where OpenEdge Management or OpenEdge Explorer is running.

- *port-number*

The port on which HTTPS is listening for SSL connections.

The login window appears.

Detecting a certificate from an unknown Certificate Authority

If the browser determines that the certificate uses an unknown CA (as is the case with the demo certificate), a message appears informing you of this fact. Depending on the version of the browser, the content of the message varies.

When browsing in Internet Explorer

If you are using the Internet Explorer browser and attempt to connect to a Web site whose certificate uses an unknown CA, you see the message shown in [Figure 6-1](#).

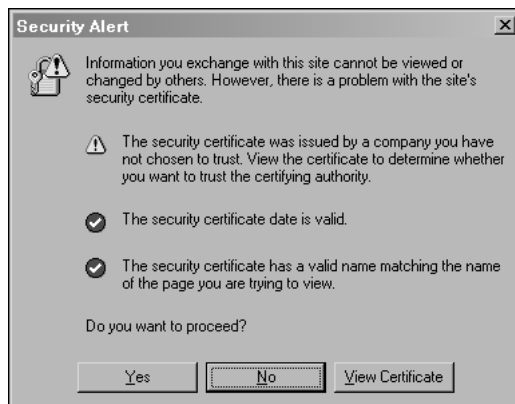


Figure 6-1: Security Alert dialog in Internet Explorer

You have the following choices:

- Click **Yes** to accept the certificate for the current session only.
- Click **No** to terminate the session.
- Click **View Certificate**.

The certificate appears, as shown in [Figure 6-2](#).



Figure 6-2: Certificate details

The certificate contains three tabs of information: **General**, **Details**, and **Certification Path**.



To install the certificate:

1. Click **Install Certificate**. The **Certificate Import Wizard** launches:



2. Click **Next**. The Wizard continues:



3. Accept the defaults, and click **Next**. The Wizard completes:



4. Click **Finish**. A message appears informing you that the import was successful.

Note: If you are using the certificate for testing purposes only, you can remove the certificate from the browser at any time.

Using your own certificate

If you want to use a certificate other than the demo included with OpenEdge Management or OpenEdge Explorer, you can do either of the following:

- Generate your own certificate (to be placed in a JSEE-compatible keystore) by using the keytool utility. See the [“Using the keytool utility”](#) section on page 6–20 for details.
- Use an existing certificate that you have already acquired from a third-party CA. To use the existing certificate, follow the [“Step 3: Importing the CA Certificate”](#) section on page 6–24 and the [“Step 4: Importing the signed certificate to the store”](#) section on page 6–25.

Using the keytool utility

You can use a valid certificate that you have already acquired from a CA, or you can use the keytool utility to take you through the following four steps to obtain and import your own certificate:

1. Creating a keystore repository and generating a key
2. Generating a certificate request
3. Importing the CA's root certificate
4. Importing the signed identity certificate to the store

Step 1: Creating a keystore repository

Before you obtain a digital certificate, you must create a keystore repository to hold the identity and CA certificates. Creating a keystore repository will also put a self-signed certificate and key pair into the store.

Note: For improved readability of the command-line samples in this document, each command-line option appears in its own line. However, you must actually type the command as one continuous string, without including any return characters.

To create the repository, type the following command **all on one line**:

```
Keytool
-genkey
-dname "CN=<myPC>, OU=<dept.> O=<company>, L=<city>, S=<state>, C=<country>"
-alias <alias>
-keypass <alias-passphrase>
-keystore <OpenEdgeManagement-install>/config/myIdentityKeystore.jks
-storepass <keystore passphrase>
-validity <days>
-keyalg rsa
-keysize 1024
```

Where:

- **-genkey**

Creates the public/private key pair and wraps the public key into a self-signed certificate.

- **-dname**

Defines the distinguished name string that identifies your site, as described in [Table 6–1](#).

Table 6–1: Distinguished name string components

Component	Description
CN	The common name, which is typically the host name for the system. (If you do not type the host name, you will get an alert from the browser.)
OU	The name of your organization or department.
O	The name of your company.
L	The name of your city.
S	The name of your state.
C	The name of your country.

- **-alias**

A value that identifies a specific certificate/key pair. You must provide a unique alias for each certificate/key pair in a keystore. In the example shown here, the alias is **Acme**.

- **-keypass**

A password that you will use to access a specific certificate/key pair. In the example shown here, the keypass is **coyote**.

- **-keystore**

The full path (relative to the OpenEdge Management or OpenEdge Explorer install directory) and the name of the keystore file you want to create.

In the example shown here, `myIdentityKeystore.jks` is the repository name, and it is stored in the `<OpenEdgeManagement-install or OpenEdge Explorer-install>\config` directory, which is the default location.

- **-storepass**

A password for the keystore file. In the example shown here, the storepass is **roadrunner**.

- **-validity**

The length of time, in days, that the certificate can be used. The default is 90 days.

- `-keyalg`

The algorithm being used to create the certificate signature.

Use this option to override the default value of **dsa** by specifying **rsa**, which is the default used by the Jetty Web server and required by Internet Explorer and Netscape.

- `-keysize`

The default key size of 1024; other values include 512 and 2048.

A sample of creating a keystore appears in [Figure 6–3](#).

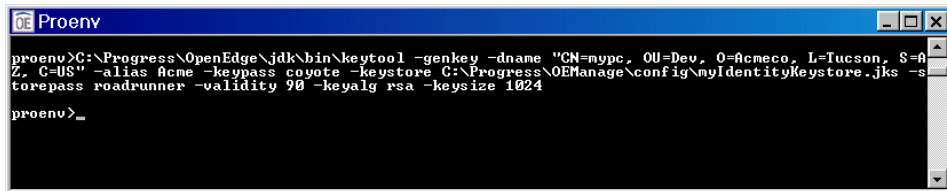


Figure 6–3: Creating a keystore

The command shown in [Figure 6–3](#) accomplishes the following:

- Generates a public/private key pair for the entity whose distinguished name (DN) has a common name (CN) of **mypc**, the organizational unit (OU) **Dev**, the company (O) **AcmeCo**, the city (L) **Tucson**, the state (S) **AZ**, and the country (C) **US**.
- Establishes that the certificate is valid for **90** days and is associated with the private key in a keystore entry referred to by the alias **Acme**.
- Assigns to the private key the keypass (password) **coyote**.
- Creates the keystore named **myIdentityKeystore** in the `<OpenEdgeManagement-install-dir>\config` directory.
- Assigns to the keystore the storepass (password) **roadrunner**.
- Uses the **rsa** key-generation algorithm to create the keys.
- Establishes the size for each key as **1024**.
- Creates a self-signed certificate that includes the public key and the distinguished name details.

Note that if you choose not to type the entire command, you can begin by typing only the `-genkey` command. The utility then prompts you for each of the subsequent pieces of information.

Step 2: Generating a certificate request

Now that you have created a self-signed certificate, you want to request a signed certificate from a Certificate Authority, so that the certificate is more apt to be trusted by others.



To request the certificate:

1. Execute the following command, typing it as **one continuous string** without including any return characters:

```
Keytool -certreq  
-alias acme  
-file d:\work\acme.csr  
-keypass coyote  
-keystore d:\work\fathomstore  
-storepass roadrunner
```

Where:

- `-certreq`

Generates a Certificate Signing Request (CSR).

- `-file d:\work\acme.csr`

Specifies the path to and name of the file that is generated to hold the certificate request information. Generally, the naming convention used to identify a CSR is to add `.csr` to the end of the file name. In the example shown here, the file is `d:\work\acme.csr`.

2. Submit the certificate request to a Certificate Authority (or to your own company's certificate authority, such as Microsoft's Certificate Authority). The submittal of the request is usually done by copying the contents of the file into the appropriate field into a Web page generated by your chosen certificate authority's Web site; however, the process for submitting the CSR is dependent upon the certificate authority.

The CA will typically authenticate you as the requestor and return a certificate, signed by the CA, authenticating your public key.

3. When you receive the reply (usually sent by e-mail), copy the contents starting with **---Begin Certificate** and ending with **---End Certificate** into a file with a `.cer` extension.

In this case, the CA will actually return a chain of certificates; each certificate authenticates the public key of the signer of the previous certificate in the chain.

4. Download the CA's root certificate for use in the Web server identity keystore.

If necessary, obtain the CA's root certificate from your certificate authority to use in your browser and for remote trending. This certificate is used on the client side (browser) to authenticate the root signer and also needs to be added to the certificate keystore file. If the CA certificate is from a well-known authority such as Verisign, then it may not be necessary to install the CA certificate into the client-side browser as most browsers already include support for well-known certificate authorities.

If the CA is not one that is included in the `trendtrustkeystore.zip`, you must get the CA's certificate and add it.

You must now update the keystore file (created in the [“Step 1: Creating a keystore repository”](#) section on page 6–20) by importing the CA certificate and your new site certificate.

Step 3: Importing the CA Certificate

Once you receive the signed certificate from the CA, you must import it.

To import the certificate, execute the following command, typing it as one continuous string without including any return characters:

```
keytool -import
-alias ca
-file d:\work\ca.cer
-keypass ca
-keystore d:\work\fathomstore
-storepass roadrunner
```

Where:

- `-import`

Causes the certificate to be imported into the keystore file.

- `-alias`

Refers to the new CA certificate.

- `-file`

Refers to the path to and name of the file that contains the CA certificate.

Step 4: Importing the signed certificate to the store

To add the signed certificate to the store, execute the following command, typing it as **one continuous string** without including any return characters:

```
Keytool -import  
-alias acme  
-file d:\work\acme.cer  
-keypass coyote  
-keystore d:\work\fathomstore  
-storepass roadrunner
```

The CA needs to be distributed to the clients. You can do this either by loading the CA certificate file manually into the browser, or, upon connecting to the OpenEdge Management Web server the first time, choosing to download and install the CA certificate.

Index

A

Accessing help in the management console
3–14

Adding a new user 5–10

Admin password
entering 2–8
updating 2–8, 5–11

Administrator users 5–7

Alerts
option in the OpenEdge Management
menu bar 3–6

AutoStart option 2–9

C

Collapsing resource categories 3–13
Collapse all icon 3–13

Command-line interface 5–25
and setting environment 5–26
help 5–29
using to start and stop 5–26

Commands
remote configuration 4–8

Configuration process
establishing values
on the Getting Started page 2–15
on the OpenEdge Explorer
Configuration page 2–7
on the OpenEdge Management
Configuration page 2–8

initial configuration options 2–4, 2–7
specifying and initially changing the
admin password 2–8

Configuring

OpenEdge Explorer 2–4
OpenEdge Explorer for remote
configuring 4–1
OpenEdge Management
completing 2–4
OpenEdge Management for remote
monitoring and configuring 4–1
OpenEdge Management or OpenEdge
Explorer
before you begin 2–3
initial options for 2–7

Container

viewing the contents of 3–5, 3–6

Control bar

icons 3–13

D

Database Migration Utility

adding a managed database page by using
2–16

Databases

managed 2–15
scripted 2–15

Deleting users 5–12

Deploying OpenEdge Management 1–3

on a single host 1–3
on multiple hosts 1–4, 1–5
strategy for 1–12

Detail control bar 3–3, 3–4

Detail frame 3–4

Detail menu 3–3, 3–4

Detail menu bar 3–10

Disabled status 3–11

Displaying a page in a new window in the console
icon 3–13

E

E-mail server 2–12

Expanding resource categories
Expand all icon 3–13

F

Fail status 3–11

G

Getting Started page
defining options for file systems and disks 2–18
managed and unmanaged databases 2–15

H

Help
command line 5–29
option in the OpenEdge Explorer menu bar 3–7
option in the OpenEdge Management menu bar 3–6

Help icon 3–13

HTTPS protocol
using with OpenEdge Management 6–1, 6–25

I

Inactive status 3–11

J

Jobs
option in the OpenEdge Management menu bar 3–6

L

Library
option in the OpenEdge Management menu bar 3–6

List control bar 3–3, 3–4

List frame 3–3, 3–4
expanding and collapsing contents 3–8, 3–9
sorting 3–10, 3–11

M

Managed and scripted databases
adding 2–15
defined 2–15

Managed databases 1–8
monitoring 1–10

Management console
accessing 3–2
accessing help in 3–14
and logging on to OpenEdge Management or OpenEdge Explorer 3–2
changing the display of 3–13
detail control bar 3–3, 3–4
detail frame 3–3, 3–4
detail menu 3–3, 3–4
displaying a page in a new window in 3–14
expanding or collapsing list frame categories in 3–13
list control bar 3–3, 3–4
list frame 3–3, 3–4
menu bar 3–3, 3–4
navigating 3–8
refreshing 3–13
resource statuses in 3–11
returning to the previous page in 3–14
using 3–1, 3–15
using to start OpenEdge Management or OpenEdge Explorer 3–2
viewing host machine name in 3–7

Menu bar 3–3, 3–4

Monitoring remote OpenEdge Management resources 1–6

My Dashboard page 3–3
option in the OpenEdge Management menu bar 3–6

N

Not Checked status 3–11

Not Running status 3–11

O

Offline status 3–11

OpenEdge
configuration
reviewing 5–2

OpenEdge Management
configuration
reviewing 5–3
configuration file 5–2
configuring
before you begin 2–3
deployment 1–3, 1–5
environment window 5–26
logging on 2–5

OpenEdge Management Configuration page
accessing during the configuration
process 2–6
admin password 2–8
AutoStart option 2–9
SNMP Adapter settings 2–13
submitting 2–14

Operator users 5–7

Options
in the OpenEdge Explorer menu bar 3–7
in the OpenEdge Management menu bar
3–6, 3–7

P

Parent folder 3–10

Pass status 3–11

Password
when logging on 2–6

R

Refreshing the console 3–13
Refresh icon 3–13

Remote monitoring
command-line options 4–8
configuring 4–1, 4–10
disabling 4–9

Reports

option in the OpenEdge Management
menu bar 3–6

Resource statuses 3–11

Resources
option in the OpenEdge Explorer menu
bar 3–7
option in the OpenEdge Management
menu bar 3–6

Returning to the previous page in the
console 3–14

S

Scripted databases 1–8
monitoring 1–10, 1–11

SMTP_MAIL network resource monitor
2–12

SNMP Adapter settings 2–13

Sort by option in the list frame 3–10

Startup options
default alert operator 2–12
e-mail server 2–12

Status indicators 3–11
and alerts 3–12

System
architecture 1–2
agents 1–2
console 1–2
database 1–2

System Activity report 3–6

System information report 3–6

U

Uninstalling
in Windows systems
if remote monitoring is configured
4–10
on UNIX systems
if remote monitoring is configured
4–10

User information
adding 5–10
changing password 5–11
changing the admin password 5–11
deleting 5–12
establishing 5–7
maintaining 5–7

User name
when logging on 2–6

Users
adding 5–10
administrators 5–7
deleting 5–12
operators 5–7

V

View previous page icon 3–13

Viewing the previous page 3–14
icon 3–13, 3–14

W

Web server port 2–11
identifying in the command-line interface
5–26