OpenEdge® Management and OpenEdge Explorer: Getting Started
# Table of Contents

**Preface**

- Purpose ............................................................................................................. 9
- Audience ............................................................................................................. 9
- Organization ..................................................................................................... 10
- Using this manual ............................................................................................... 10
  - References to ABL compiler and run-time features ........................................... 11
  - References to ABL data types ........................................................................... 11
- Typographical conventions ................................................................................ 11
- Examples of syntax descriptions ......................................................................... 13
  - Long syntax descriptions split across lines ......................................................... 14
  - Complex syntax descriptions with both required and optional elements .......... 15
- OpenEdge messages .......................................................................................... 15
  - Obtaining more information about OpenEdge messages .................................... 16

**Chapter 1: Introducing OpenEdge Management and OpenEdge Explorer**

- OpenEdge Management overview ..................................................................... 18
- OpenEdge Explorer overview ............................................................................ 19
  - OpenEdge Explorer feature availability ............................................................. 20
- Understanding OpenEdge Management architecture and deployment ............... 20
  - OpenEdge Management system architecture .................................................... 20
  - OpenEdge Management deployment ................................................................. 20
    - Deploying OpenEdge Management on a single host ......................................... 21
    - Deploying OpenEdge Management on multiple hosts ...................................... 21
  - Configuring or monitoring resources on a remote AdminServer ....................... 23
    - Configuring remote resources with OpenEdge Explorer .................................. 24
    - Configuring and monitoring remote resources with OpenEdge Management ...... 24
    - Resources that support remote monitoring ...................................................... 24
  - More about monitoring scripted and managed databases .................................. 26
    - Monitoring a scripted database through a remote-enabled AdminServer ........ 27
    - Monitoring a managed database through a remote-enabled AdminServer ......... 27
    - Monitoring scripted databases outside the AdminServer running OpenEdge Management ................................................................. 27
  - Choosing an OpenEdge Management deployment strategy .............................. 28
- OpenEdge Management CPU and memory requirements .................................. 29
  - CPU use ............................................................................................................ 29
  - Memory use ...................................................................................................... 30
- Optionally configuring the OpenEdge Management Trend Database .................. 31
- System requirements .......................................................................................... 31
Chapter 2: Setting Up OpenEdge Management or OpenEdge Explorer for the First Time

Preparing to set up OpenEdge Management or OpenEdge Explorer
Using the management console
Using the Database Administration Console
Completing the initial setup process
Setting up OpenEdge Explorer
Setting up OpenEdge Management
Starting OpenEdge Management or OpenEdge Explorer
Entering the default user name and password
Choosing initial configuration options
Setting initial configurations for OpenEdge Explorer
Setting initial configurations for OpenEdge Management
Specifying the Admin Password
Specifying the AutoStart option
Specifying the location of the OpenEdge Management Trend Database
Specifying the OpenEdge Management e-mail server and default operator
Submitting the OpenEdge Management or OpenEdge Explorer Configuration page
Setting up the Getting Started page for OpenEdge Management
Understanding managed and scripted databases
Defining OpenEdge Management monitors for previously scripted databases
Adding a managed database
Making changes to a managed database configuration
Defining OpenEdge Management monitoring and trending options for file systems and disks
Submitting the Getting Started page for OpenEdge Management

Chapter 3: Using the Console

Starting OpenEdge Management or OpenEdge Explorer
Logging on
Using the management console
Customizing the Resources view
Viewing the contents of a AdminServer
Accessing functions from the menu bar tabs for OpenEdge Management
Accessing functions from the menu bar tabs for OpenEdge Explorer
Navigating the console
Checking resource status and alert severity
Accessing Help
Additional console details
Chapter 4: Setting up Remote Resource Monitoring and Configuration

Remote monitoring and configuration requirements.................................................................59
Preparing to enable remote monitoring and configuration.......................................................60
  Ungluing OpenEdge Management or OpenEdge Explorer from OpenEdge........................61
  Regluing OpenEdge Management or OpenEdge Explorer to OpenEdge............................63
Setting up for remote monitoring or configuration.................................................................64
Setting up a remote AdminServer..........................................................................................64
  Verifying that OpenEdge Management or OpenEdge Explorer can see the remote AdminServer..........................................................................................................................64
  Disabling remote monitoring of a remote AdminServer..........................................................64

Chapter 5: Administering OpenEdge Management and OpenEdge Explorer

  Updating configuration options........................................................................................................68
  Adding users as administrators or operators............................................................................70
    Managing the authorized users list..............................................................................................70
    Adding a new user....................................................................................................................70
    Changing passwords and descriptions....................................................................................72
    Changing the Admin password ................................................................................................72
    Deleting users............................................................................................................................72
  Customizing the operator role......................................................................................................73
    Managing access to the Database Administration Console..................................................74
  Setting OpenEdge Management user preferences.................................................................75
  Setting up a remote AdminServer.............................................................................................75
    Viewing a remote AdminServer................................................................................................76
    Deleting a remote AdminServer...............................................................................................76
    Setting up secure communication-related security for a remote AdminServer.....................77
  Changing general configuration settings..................................................................................79
  Changing OpenEdge Management e-mail alerts settings.........................................................80
  Changing OpenEdge Management resource monitoring settings...........................................81
  Setting the OpenEdge Management graph cache....................................................................82
  Configuring process pooling......................................................................................................83
    Process pooling modes..............................................................................................................83
    Setting process pooling options...............................................................................................84
    Creating a new process pooling configuration.........................................................................84
    Deleting a custom process pooling configuration....................................................................85
  Setting OpenEdge Management resource monitor defaults..................................................85
  Setting OpenEdge Management distribute resource properties............................................86
  Changing the OpenEdge Management SNMP Adapter settings.............................................87
  Using the command-line interface............................................................................................89
  Using the OpenEdge environment window Proenv.................................................................90
    Starting, querying, and stopping from the command line..........................................................90
Examples of starting, querying, and stopping from the command line.................................91
Dumping, backing up, and restoring the configuration database......................................92
Dumping the configuration database................................................................................92
Restoring the configuration database from a backup file...............................................93
Accessing command-line help.........................................................................................93
Setting the log level for the AdminServer log file ..........................................................94

Chapter 6: Setting Up Secure Communications.........................................................95
Transferring data securely with the HTTPS protocol......................................................96
Using the demo certificate or your own certificate........................................................96
Understanding common secure communication-related terminology.............................96
Getting started: using the demo certificate.......................................................................97
Configuration update errors or warnings..........................................................................98
Identifying trusted clients...............................................................................................98
Reconnecting after updates............................................................................................98
Changing Web server settings.........................................................................................99
Using advanced HTTP and HTTPS options with the Web server..................................100
Changing OpenEdge Management Trend Database settings.......................................102
Using advanced HTTPS options when trending remotely.........................................103
Using the procertm utility...............................................................................................104
Managing the trust keystore with procertm.................................................................104
Converting digital certificates with procertm.............................................................106
Using Secure Communication.......................................................................................106
Detecting a certificate from an unknown Certificate Authority.......................................107
When browsing in Internet Explorer...............................................................................107
Installing certificate in Internet Explorer..........................................................................108
Using your own certificate.............................................................................................109
Using the keytool utility..................................................................................................110
Step 1: Creating a keystore repository............................................................................110
Step 2: Generating a certificate request..........................................................................112
Step 3: Importing the CA Certificate...............................................................................113
Step 4: Importing the signed certificate to the store......................................................114

Index.............................................................................................................................115
Preface

For details, see the following topics:

- 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

Introducing OpenEdge Management and OpenEdge Explorer on page 17
Provides an introduction to working with OpenEdge Management 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.

Setting Up OpenEdge Management or OpenEdge Explorer for the First Time on page 37
Describes how to select initial configuration options and how to start OpenEdge Management or OpenEdge Explorer.

Using the Console on page 51
Describes the management console, which is common to both OpenEdge Management and OpenEdge Explorer. The chapter also describes the Database Administration Console, which you use to work with databases enabled for multi-tenancy.

Setting up Remote Resource Monitoring and Configuration on page 59
Provides information about how to set up resources for remote monitoring by OpenEdge Management and remote configuration by OpenEdge Explorer.

Administering OpenEdge Management and OpenEdge Explorer on page 67
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.

Setting Up Secure Communications on page 95
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.

For the latest documentation updates see the OpenEdge Product Documentation Overview page on Progress Communities:
References to ABL compiler and run-time features

ABL is both a compiled and an interpreted language that executes in a run-time engine. The documentation refers to this run-time engine as the **ABL Virtual Machine (AVM)**. When the 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 the 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, built-in 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 *character* appears, this is a reference to the **CHARACTER**, **LONGCHAR**, or **CLOB** 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 built-in 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 and syntax conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Bold typeface indicates commands or characters the user types, provides emphasis, or the names of user interface elements.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic typeface indicates the title of a document, or signifies new terms.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SMALL, BOLD CAPITAL LETTERS</td>
<td>Small, bold capital letters indicate OpenEdge key functions and generic keyboard keys; for example, GET and CTRL.</td>
</tr>
<tr>
<td>KEY1+KEY2</td>
<td>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.</td>
</tr>
<tr>
<td>KEY1 KEY2</td>
<td>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.</td>
</tr>
<tr>
<td>Syntax:</td>
<td></td>
</tr>
<tr>
<td>Fixed width</td>
<td>A fixed-width font is used in syntax, code examples, system output, and file names.</td>
</tr>
<tr>
<td>Fixed-width italics</td>
<td>Fixed-width italics indicate variables in syntax.</td>
</tr>
<tr>
<td>Fixed-width bold</td>
<td>Fixed-width bold italic indicates variables in syntax with special emphasis.</td>
</tr>
<tr>
<td>UPPERCASE fixed width</td>
<td>ABL keywords in syntax and code examples are almost always shown in upper case. Although shown in uppercase, you can type ABL keywords in either uppercase or lowercase in a procedure or class.</td>
</tr>
<tr>
<td>Period (.) or colon (:)</td>
<td>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.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Large brackets indicate the items within them are optional.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Small brackets are part of ABL.</td>
</tr>
<tr>
<td>{ }</td>
<td>Large braces indicate the items within them are required. They are used to simplify complex syntax diagrams.</td>
</tr>
<tr>
<td>{}</td>
<td>Small braces are part of ABL. For example, a called external procedure must use braces when referencing arguments passed by a calling procedure.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate repetition: you can choose one or more of the preceding items.</td>
</tr>
</tbody>
</table>
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 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 runs within the OpenEdge Management console, which runs in a Web browser. Using OpenEdge Explorer, 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 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.

For details, see the following topics:

• OpenEdge Management overview
• OpenEdge Explorer overview
• Understanding OpenEdge Management architecture and deployment
• Configuring or monitoring resources on a remote AdminServer
• Choosing an OpenEdge Management deployment strategy
• OpenEdge Management CPU and memory requirements
• Optionally configuring the OpenEdge Management Trend Database
• System requirements
OpenEdge Management includes the following key features and benefits:

- Provides centralized monitoring of the OpenEdge environment to present a comprehensive picture of the health and performance of your OpenEdge application.

- Can be used immediately to monitor local log files and resources running on a local machine. You can also use OpenEdge Management to monitor resources running under an AdminServer on a remote machine.

- Allows you to make configuration changes to resource instances. These changes are then automatically reflected in the corresponding property file—`conmgr.properties` for a database and `ubroker.properties` for the remaining resources.

- Allows you to create collections and custom views from the Dashboard page. You can create and use a collection to better organize and operate on resources. You can also optionally create one or more custom views in OpenEdge Management and specify exactly what types of information you want to see. The information provides, sometimes in a graphical format, a customized view of your various resources' status.

- Offers a graphical display of database views, which allows you to see at a glance what is happening in the database. The graphics appear in several different, easy-to-understand charts whose display you can open as a separate window and customize in style and size.

A graphical representation of data also appears in the summary information for other resources—such as OpenEdge server resources, or memory, CPU, disk, file, or file system resource—and for several AppServer- and WebSpeed-related performance views.

- Enables you to configure alerts to notify appropriate IT personnel of problems with your OpenEdge applications. For example, you can configure alerts to send e-mail notifications to IT personnel and to execute scripts.

- Allows you to view, print, and save reports showing historical and trend data related to all of the monitored resources. Each report instance that you create and run is based on a report template, either one of the over 20 provided by OpenEdge Management, or one of your own creation. You can also write custom reports with ABL or use other reporting tools, such as Crystal Reports. Use this feature to help with capacity planning and forecasting.

OpenEdge-related reports include a graphical and an HTML display of information.

- Is easy to deploy, configure, and use. A multi-platform user interface allows you to configure and use OpenEdge Management through any compatible Web browser.

- Allows you to define batch-style application programs using your existing scripts as OpenEdge Management jobs, both locally and remotely. You can schedule the jobs for execution at regular intervals. OpenEdge Management also provides historical reports of the jobs.

- Is non-intrusive. You are not required to make any changes to the network applications you choose to monitor.

- Allows you to use cryptographic protocols when you are setting up:
  - Remote trending of data to the OpenEdge Management Trend Database
• The OpenEdge Management Web server
• Remote AdminServer
• OpenEdge Management email alerts
• Pacific Application Server for OpenEdge (PAS for OpenEdge)

• Allows you to query a running AppServer to see a list of client systems to which the AppServer is currently connected. This information may be helpful in identifying application components that may have malfunctioned.
• Supports TCP/IP versions 4 and 6.
• Includes the Database Administration Console, which allows you to manage and work with databases enabled for multi-tenancy.

OpenEdge Explorer overview

You can use OpenEdge Explorer within the graphical user interface console also used by OpenEdge Management. The console runs in a browser, making it accessible in Windows and on supported UNIX platforms.

OpenEdge Explorer allows you to:
• Create and delete new instances of licensed resources
• Set or modify properties for these instances
• Start or stop the instances (where applicable)
• View a real-time status of the instances
• View an instance’s log file
• Work with databases enabled for multi-tenancy

OpenEdge Explorer is installed with OpenEdge for the following products:

<table>
<thead>
<tr>
<th>4GL Development System</th>
<th>OpenEdge Enterprise, Workgroup, or Personal database</th>
</tr>
</thead>
<tbody>
<tr>
<td>NameServer</td>
<td>OpenEdge DataServer for ODBC, Oracle, or MS SQL Server</td>
</tr>
<tr>
<td>WebSpeed Workshop</td>
<td>OpenEdge Development Server</td>
</tr>
<tr>
<td>Progress Developer Studio for OpenEdge</td>
<td>OpenEdge Application Server Basic</td>
</tr>
<tr>
<td>OpenEdge Studio</td>
<td>OpenEdge Application Server Enterprise</td>
</tr>
</tbody>
</table>
OpenEdge Explorer feature availability

As you work with OpenEdge Explorer within the console, you might see that certain links and functionality are not available. In general, the settings you can establish and the options you can access when using OpenEdge Explorer (and OpenEdge Management) are determined both by the platform you are using and the products that you are licensed to use. If you notice that a particular property setting is dimmed in the OpenEdge Explorer console and not available for modification, it is because that property has no meaning within your operating environment or your licensed configuration.

Understanding OpenEdge Management architecture and deployment

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

- OpenEdge Management system architecture on page 20
- OpenEdge Management deployment on page 20

OpenEdge Management system architecture

OpenEdge Management consists of the following:

- 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.
- The Database Administration Console, which allows you to manage and work with databases enabled for multi-tenancy.
- 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 AdminServer is a background process that provides a common point of management for the resources managed by OpenEdge Management or OpenEdge Explorer. (For more information about the AdminServer, see OpenEdge® Management and OpenEdge Explorer: Getting Started.)
- The Orient DB 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 Management deployment

You can deploy OpenEdge Management by installing it on:

- A single host
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 below, all components of OpenEdge Management exist on the same host, Machine A.

**Figure 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 monitors 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 below.
The above figure 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 this deployment 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 below.
The above figure 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 2 on page 22 and Figure 3 on page 23, 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 or monitoring resources on a remote AdminServer**

If you have OpenEdge Management installed, you can monitor and configure resources running on a remote AdminServer. You can use OpenEdge Explorer to set configuration properties for (but not monitor) remote resources.

To configure or monitor a remote resource, you identify the resource's AdminServer. An AdminServer represents a named instance of an AdminServer that is running OpenEdge Management or OpenEdge Explorer. A remote AdminServer can be one of the following:

- An AdminServer that you set up to be configured or monitored remotely by OpenEdge Management
• An AdminServer that you have set up to be configured remotely by OpenEdge Explorer

There is typically a one-to-one relationship between the host name and the AdminServer name, unless there are multiple AdminServers running OpenEdge Management or OpenEdge Explorer on the same host.

For details about setting up remote AdminServers, see Setting up Remote Resource Monitoring and Configuration on page 59

Configuring remote resources with OpenEdge Explorer

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

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 disabled OpenEdge Explorer on the remote resource’s host machine. This is not a mandatory step, but we highly recommend that you have the Explorer disabled.

See Setting up for remote monitoring or configuration on page 64.

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 provided that:

• An AdminServer is available and running on the remote resource’s host machine.

• You have disabled OpenEdge Management (and OpenEdge Explorer) on the remote resource’s host machine. This is not a mandatory step, but we highly recommend that you have the Explorer disabled.

See Setting up for remote monitoring or configuration on page 64 for details.

Remote configuration and monitoring provide 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 remote monitoring framework, which is a very fast and reliable messaging system.

Resources that support remote monitoring

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

• Databases — OpenEdge Releases 11.3 and greater.

• OpenEdge servers — AppServer, WebSpeed, OE Web Server and NameServer.

• System resources — CPU, memory, disk, and file system.
The following figure shows a deployment in which OpenEdge Management is monitoring resources on a remote machine.

**Figure 4: Remote monitoring of resources on one machine**

![Diagram showing the deployment model](image)

The illustration shown in Figure 4 on page 25 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 4 on page 25 to multiple hosts, as shown in Figure 5 on page 26.
The illustration shown in Figure 5 on page 26 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 remote monitoring framework 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 Setting up Remote Resource Monitoring and Configuration on page 59.

**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 below.
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 bests 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:
OpenEdge Management and OpenEdge Explorer: Getting Started

OpenEdge Management CPU and memory requirements

OpenEdge Management consumes both CPU and memory on the system where it is running. The amount consumed varies based on the number and types of resources being monitored, the frequency with which they are polled, and the processing power of the host system.

CPU use

OpenEdge Management CPU utilization should typically be in the range of 1-5% (with possible spikes as noted below). Factors that might result in greater levels of CPU utilization include:

- **A very high number of monitored resources relative to the processing power of the host system** — The number of resources you can monitor with OpenEdge Management before it introduces an unacceptable CPU load is very dependent upon the processing power of the host system.

  On most systems monitoring a moderate number of resources such as 10 databases, 20 system resource monitors, and 20 network resource monitors, the CPU load of OpenEdge Management should be minimal. Host systems with greater processing power will be able to support greater resource counts.

- **A very short polling interval on monitored resources** — Each poll of a resource requires a small measure of CPU utilization. Polling a lot of resources with very short polling intervals will increase OpenEdge Management load on the CPU. Using the default OpenEdge Management polling interval should minimize this problem.

  If OpenEdge Management CPU utilization becomes a problem, you can reduce it by increasing the polling interval of monitored resources. For example, rather than polling databases every 5 minutes, you can set them to poll every 15 minutes.

- **A very high level of user interaction with OpenEdge Management through the management console** — Each page displayed in the console needs to be produced by OpenEdge Management, and, therefore, requires a small measure of CPU utilization. A very high level of
user interaction with the console will increase OpenEdge Management load on the CPU. This is especially true of any page that displays graphical data.

One feature to be particularly conscious of is the OpenEdge Management Auto Refresh capability. This feature allows you to configure the OpenEdge Management console such that the displayed pages are automatically refreshed at a specified rate. Automatically refreshing pages with lots of graphical data at a high frequency will increase OpenEdge Management load on the CPU. For details about the Auto Refresh feature, see Setting OpenEdge Management user preferences on page 75.

- **Very high levels of report execution** — OpenEdge Management uses an OpenEdge database for storing trend information and ABL for running reports. This combination makes OpenEdge Management historical reports very efficient; however, running reports very frequently or against a large volume of historical data will increase OpenEdge Management load on the CPU.

You should use the OpenEdge Management scheduling facility to schedule reports to run at off-peak hours. You can also install a copy of OpenEdge Management on a nonproduction host and use it as the trend database for the OpenEdge Management install on your production hosts. Doing this will allow you to offload the management of trend data and run historical reports from your production host.

- **A large number of jobs** — Like reports, jobs can put a heavy load on the CPU. The scheduling algorithm of your operating system might give all available CPU time to execute jobs or reports, which can cause a spike in CPU utilization while the job or report is running. You should schedule CPU-intensive jobs, such as database backups, to run at off-peak hours to minimize the chances of introducing too much overhead during peak system times. Offloading jobs to nonproduction systems is another option.

### Memory use

OpenEdge Management memory utilization is directly related to the number and types of resources being monitored. The AdminServer with OpenEdge Management loaded but no resources defined requires 25MB to 35MB of RAM memory. This requirement can vary based upon the platform and the number of other OpenEdge products installed.

As you add resources to OpenEdge Management, the memory requirements increase. Each monitored database requires about 2MB of memory. Other monitored resource types require much less, typically in the range of 10KB to 100KB per resource.

OpenEdge Management allows you to store the data being used for graphs. This increased storage can cause a significant increase in memory usage.

Factors you can control to manage OpenEdge Management memory utilization include:

- **The number of monitored resources** — If OpenEdge Management is consuming an unacceptable amount of memory, you can reduce the number of monitored resources. You can also choose to install an instance of OpenEdge Management on a nonproduction host and use that host to monitor network and log file resources. This would remove the load from your production hosts, leaving on them only the monitoring of local system resources and databases.

- **Use of the OpenEdge Management remote database monitoring agent** — Using an instance of OpenEdge Management on a nonproduction host in conjunction with the remote database monitoring agent will allow you to greatly minimize overhead on your production systems. In this configuration, the majority of OpenEdge Management activity is off-loaded to a nonproduction host. Only the overhead of the remote database agent will be incurred on your production systems. This overhead is minimal.
• **Adding remote monitoring on the OpenEdge Management machine** — The addition of remote monitoring will substantially increase memory use.

• **Working with the Database Administration Console** — When you are working with the Database Administration Console (and depending on how it is configured), there may be one or more copies of `_progress.exe` actively running. These copies of `_progress` may connect and disconnect from any monitored databases to perform tasks needed for the Database Administration Console.

### Optionally configuring the OpenEdge Management Trend Database

After you install OpenEdge Management and before you begin the configuration in the OpenEdge Management console (as described in Setting Up OpenEdge Management or OpenEdge Explorer for the First Time on page 37), you can preallocate file system space in the OpenEdge Management Trend Database. This preallocation step is optional; however, it will make the database run more efficiently if you create fixed length extents before the database is created.

To preallocate file system space:

1. Copy the OpenEdge Management Trend Database structure file (`fathom.st`) that exists in `<OpenEdgeManagement-install-dir>\db` to the directory where the database will reside. (The default OpenEdge Management install directory is `Progress\oemgmt`.)
2. Edit the file, and add fixed length data extents to area 7.
3. Continue with the configuration as described in Setting Up OpenEdge Management or OpenEdge Explorer for the First Time on page 37. When the OpenEdge Management Trend Database is created, the database uses the structure file that exists in the directory where the database is being created.

For more information about editing `.st` files, see *OpenEdge Data Management: Database Administration*.

### System requirements

Most of the system requirements for OpenEdge Management or OpenEdge Explorer are the same as those for OpenEdge. For more information, see *OpenEdge Getting Started: Installation and Configuration*.

### Browser support

A Web browser is required to run the OpenEdge Management or OpenEdge Explorer graphical user interface known as the management console.

The following browsers are supported in Windows platforms:

- Firefox (minimum Version 3.6 required)
- Google Chrome
• Internet Explorer (minimum Version 8 required)
• Opera
• Safari

On UNIX platforms, the following browsers are supported:
• Firefox (minimum Version 3.6 required)
• Google Chrome
• Opera

On the Macintosh platform:
• Firefox
• Google Chrome
• Opera
• Safari

Although you may find either other browsers or earlier versions of the browsers listed here that you can use with OpenEdge Management or OpenEdge Explorer, those versions/browsers may present limited functionality or rendering problems.

Accessing OpenEdge Management and OpenEdge Explorer documentation

OpenEdge Management and OpenEdge Explorer documentation is available as follows:

• From the management console footer bar, select Help Me to see context-sensitive help related to the active console page directly, and find OpenEdge Management and OpenEdge Explorer guides.

  If no context-sensitive help exists for a particular page, the OpenEdge Management and OpenEdge Explorer: Getting Started topic appears. From there, you can select Search in the left pane of the management console to search for the specific details you want.

• In the Documentation and Samples (doc_samples) directory of the OpenEdge Product ESD.
• In PDF and HTML format from Progress Communities:


For best results when using the PDF files, install the Acrobat Reader. You can download the Reader from the following location on the Adobe Web site:

In addition to this manual, the following documents comprise the OpenEdge Management and OpenEdge Explorer document set:

- **OpenEdge Management and OpenEdge Explorer: Configuration**
  Describes how to establish property and configuration settings for OpenEdge databases, DataServers (for ODBC, Oracle, and MS SQL Server), NameServers, AppServers, AppServer Internet Adapters, Web Services Adapters, WebSpeed® Transaction Servers, WebSpeed Messengers, OE Web Server, and ActiveMQ® Adapters in OpenEdge Management and OpenEdge Explorer. In addition, this manual also includes details about viewing status and log files.

- **OpenEdge Management: Resource Monitoring**
  Provides detailed information about the management console; the procedures to set up and run resource monitors, jobs, job templates; and the procedures to perform OpenEdge Management-based import and export activities.

- **OpenEdge Management: Database Management**
  Describes how to use OpenEdge Management to monitor and manage OpenEdge database resources.

- **OpenEdge Management: Alerts Guide and Reference**
  Presents alert concepts and procedures and provides a comprehensive reference section to assist you in working with the OpenEdge Management alerts feature.

- **OpenEdge Management: Servers, DataServers, Messengers, and Adapters**
  Describes how OpenEdge Management supports monitoring and managing specific resources associated with the OpenEdge server products (AppServer, WebSpeed Transaction Server, and NameServer), DataServers (ODBC, Oracle, and MS SQL Server), WebSpeed Messengers, and Adapters (AppServer Internet Adapter, SonicMQ Adapter, OE Web Server, and Web Services Adapter).

- **OpenEdge Management: Reporting**
  Provides detailed information about creating and working with report instances and templates.

- **OpenEdge Management: Trend Database Guide and Reference**
  Describes how to manage the OpenEdge Management Trend Database by compacting and purging data. This book also provides a detailed look at the Trend Database schema.

- **OpenEdge Management and OpenEdge Explorer: Configuring Multi-tenancy**
  Describes how to manage and work with databases enabled for multi-tenancy. From the management console, you can perform a variety of different tasks, such as adding a local or remote database connection definition; creating new tenants and viewing their areas, domains, partitions, and schemas; uploading and previewing schema updates; making storage area and allocation decisions; filtering views; and creating and working with tenant templates and tenant groups.
  You can also enable local and remote databases for multi-tenancy, convert tables to multi-tenancy, and establish and manage user and table security settings. Support for viewing, exporting, and editing values for sequences is also available.

- **OpenEdge Management and OpenEdge Explorer: Getting Started with Multi-tenancy**
  Describes how to get started using multi-tenancy in the Database Administration Console.
Getting started with OpenEdge Management tasks

To help you get started with OpenEdge Management, the following figure illustrates the major OpenEdge Management tasks in the order they are typically performed. This diagram is not intended to depict all of the features or functionality in OpenEdge Management, but rather to provide a high-level view. Use the information in the following table to locate information on performing each task.

**Figure 7: OpenEdge Management workflow overview**

Table 1: Documentation for major OpenEdge Management tasks (1 of 2)

<table>
<thead>
<tr>
<th>For information on this task . . .</th>
<th>See . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing a deployment plan before you install OpenEdge Management</td>
<td>This guide</td>
</tr>
<tr>
<td>For information on this task . . .</td>
<td>See . . .</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Setting up OpenEdge Management or OpenEdge Explorer, which includes logging on and defining initial settings</td>
<td>This guide</td>
</tr>
<tr>
<td>Setting up OpenEdge Management for remote monitoring and configuration, and OpenEdge Explorer for remote configuration; and setting up users.</td>
<td>This guide</td>
</tr>
<tr>
<td>Updating initial OpenEdge Management settings related to authorized users, user preferences, the SNMP Adapter, and other configuration settings in the following categories: general, OpenEdge Management Trend Database, Web server, e-mail alerts, and resource monitoring</td>
<td>This guide</td>
</tr>
<tr>
<td>Using the HTTPS (TLS) protocol for trending to a remote database or for communication between an OpenEdge Management Web server and client</td>
<td>This guide</td>
</tr>
<tr>
<td>Creating new instances of resources, and setting or modifying their configuration properties</td>
<td>This guide</td>
</tr>
<tr>
<td>Creating monitoring plans for and managing system, network, file, and OpenEdge resources in OpenEdge Management</td>
<td>OpenEdge Management: Resource Monitoring</td>
</tr>
<tr>
<td>Creating collections and custom views (Dashboard) in OpenEdge Management</td>
<td>OpenEdge Management: Resource Monitoring</td>
</tr>
<tr>
<td>Creating and scheduling jobs in OpenEdge Management</td>
<td>OpenEdge Management: Resource Monitoring</td>
</tr>
<tr>
<td>Importing and exporting configurations in OpenEdge Management</td>
<td>OpenEdge Management: Resource Monitoring</td>
</tr>
<tr>
<td>Creating and running reports in OpenEdge Management</td>
<td>OpenEdge Management: Reporting</td>
</tr>
<tr>
<td>Creating monitoring plans for and managing database resources in OpenEdge Management</td>
<td>OpenEdge Management: Database Management</td>
</tr>
<tr>
<td>Creating monitoring plans for and managing OpenEdge server, DataServer, Messenger, and Adapter resources</td>
<td>OpenEdge Management: Servers, DataServers, Messengers, and Adapters</td>
</tr>
<tr>
<td>Understanding and working with OpenEdge Management alerts</td>
<td>OpenEdge Management: Alerts Guide and Reference</td>
</tr>
<tr>
<td>Managing your OpenEdge Management Trend Database by compacting and purging data, and understanding the trend database schema</td>
<td>OpenEdge Management: Trend Database Guide and Reference</td>
</tr>
<tr>
<td>For information on this task . . .</td>
<td>See . . .</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Managing and working with databases enabled for multi-tenancy</td>
<td><em>OpenEdge Management and OpenEdge Explorer: Configuring Multi-tenancy</em></td>
</tr>
<tr>
<td>Getting started with multi-tenancy in the Database Administration Console</td>
<td><em>OpenEdge Management and OpenEdge Explorer: Getting Started with Multi-tenancy</em></td>
</tr>
</tbody>
</table>
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.

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.

For details, see the following topics:

• 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
• Understanding managed and scripted databases
• Defining OpenEdge Management monitors for previously scripted databases
• Defining OpenEdge Management monitoring and trending options for file systems and disks
• Submitting the Getting Started page for OpenEdge Management
Preparing to set up OpenEdge Management or OpenEdge Explorer

Consider the following factors before you set up OpenEdge Management or OpenEdge Explorer for the first time:

• Determine the names and locations of the resources that you need to monitor and the properties you want to configure. You can configure properties for resources associated with local and remote AdminServers. With OpenEdge Management, you can also monitor certain resources running under a local or remote AdminServer.

• (In OpenEdge Management only) Determine whether to save monitoring information to the OpenEdge Management Trend Database and, if saving the monitoring information, decide where to locate the database.

The OpenEdge Management Trend Database stores the monitoring information that OpenEdge Management collects for databases, system resources, file resource, network resources, the AppServer, WebSpeed Transaction Server, and the NameServer. During configuration, you can choose whether to save monitoring information locally, remotely, or not at all. Before installation, you should decide if you want to save this data and where you want to save it.

OpenEdge Management automatically creates the OpenEdge Management Trend Database if you have an OpenEdge® Enterprise RDBMS, an OpenEdge® Workgroup RDBMS, or an OpenEdge® Personal database installed on the same machine where you are installing OpenEdge Management.

If you decide to save monitoring information remotely, the remote machine must have both a database (Enterprise or Workgroup) and OpenEdge Management installed. In other words, you cannot just copy a trending database to a remote machine.

The local instance of OpenEdge Management must communicate with a remote instance of OpenEdge Management to use the remote trending database.

• (In OpenEdge Management only) Determine how monitoring might affect system performance.

The more resources you monitor, the more system resources OpenEdge Management uses. If you plan to monitor a large number of database servers and network services in your configuration, you might want to consider configuring additional OpenEdge Management instances, both locally and remotely.

See OpenEdge Management CPU and memory requirements on page 29 for more information.

• Note that OpenEdge Management runs as a plug-in to the AdminServer; your resources can be administered by OpenEdge Explorer and command-line utilities, such as dbman or asbman. Therefore, you should be familiar with the AdminServer functionality. For more information, see OpenEdge Management and OpenEdge Explorer: Getting Started.

You can access online help while working in the management console. For details about the dbman or asbman utility, see OpenEdge Data Management: Database Administration.
If you do not preconfigure OpenEdge Management or OpenEdge Explorer to autostart, you can stop and start either one manually, as follows:

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

To open OpenEdge Management/OpenEdge Explorer in a browser, select **Start > Programs (or All Programs) > Progress > OpenEdge > Management Console**. (If you do not have OpenEdge Management installed and are using only OpenEdge Explorer, select **Start > Programs (or All Programs) > Progress > OpenEdge > OpenEdge Explorer**.)

The initial user name and password are admin/admin.

For details about using command-line options with OpenEdge Management or OpenEdge Explorer, see *Administering OpenEdge Management and OpenEdge Explorer* on page 67.

### 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 *Using the Console* on page 51 which covers the console's features and functionality in detail.

### Using the Database Administration Console

OpenEdge Management and OpenEdge Explorer both include the Database Administration Console, which you use to manage and work with databases enabled or multi-tenancy.

To open the Database Administration Console in a browser, select **Start > Programs (or All Programs) > Progress > OpenEdge > Database Administration Console**.

### 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

After setting up OpenEdge Explorer (and not OpenEdge Management), you are prompted to make initial configuration choices the first time you start it in the browser after the OpenEdge installation.
When you start the OpenEdge Explorer, do the following:

- Fill in all the fields in the **OpenEdge Explorer Configuration** page that appears, and click **Submit**.
- Select sign up for the customer experience improvement program on the **Customer Experience Improvement Program** page that appears and click **Submit**.
- Click **Start using OpenEdge Explorer** in the **Initial Configuration Completed** page that appears.

### Setting up OpenEdge Management

After installing OpenEdge Management, you are prompted to make initial configuration choices the first time you start it in the browser after the OpenEdge installation.

When you start the OpenEdge Management, do the following:

- Fill in all the fields in the **OpenEdge Explorer Configuration** page that appears, and click **Submit**.
  
  OpenEdge Management is partially initialized, and the **OpenEdge Management Getting Started** page appears.

- Define monitors for files, disks, and scripted databases, and click **Submit**.

- Select sign up for the customer experience improvement program on the **Customer Experience Improvement Program** page that appears and click **Submit**.

- Click **Start using OpenEdge Management** in the **Initial Configuration Completed** page that appears.

After you make your initial configuration choices, you can access and change certain configuration options that are specified 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).

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.
• From the Windows Desktop on your local host, select **Start > Programs (or All Programs) > Progress > OpenEdge > Management Console** to start OpenEdge Management/OpenEdge Explorer. If you have only OpenEdge Explorer installed, select **Start > Programs (or All Programs) > Progress > OpenEdge > OpenEdge Explorer**.

The logon window appears and requires you to enter your user name and password, as described in **Entering the default user name and password** on page 41.

### 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:** 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 OpenEdge 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 **Using the command-line interface** on page 89 for more information.

You can now make initial configuration choices, as described in **Choosing initial configuration options** on page 41.

### 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:

- 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.
- You can subsequently change your initial configuration decisions.
• OpenEdge Management and OpenEdge Explorer support the implementation of the HTTPS (TLS) protocol.

When you complete the initial configuration of OpenEdge Explorer, you can further modify your settings by enabling support for secure communication 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 enabled support for secure communication when setting up the Web server and when trending to a remote OpenEdge Management Trend Database.

See Setting Up Secure Communications on page 95.

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 on page 42
• Specifying the AutoStart option on page 43

Each of these options is described in the 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 on page 42
• Specifying the AutoStart option on page 43
• Specifying the location of the OpenEdge Management Trend Database on page 43
• Specifying the OpenEdge Management e-mail server and default operator on page 44

Each of these options is described in following sections.

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 Adding users as administrators or operators on page 70 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 **Using the command-line interface** on page 89 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. The password is encrypted using the SHA-256 hashing algorithm.

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.

If you clear this box, you must use the command-line interface to start OpenEdge Management or OpenEdge Explorer. See **Using the command-line interface** on page 89 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.

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, user name, and password of the remote OpenEdge Management Web server. The trend database must be locally configured at the remote location. The user credentials with the **Trending** role must be created on the remote OpenEdge Management Web server. See **Adding a new user** on page 70 for more information. 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 **Setting Up Secure Communications** on page 95 for more information.

**Note:** You can elect to store trend data in a remote OpenEdge Management Trend Database only if you install OpenEdge Management on both the local machine and the remote machine.

To specify the location of the OpenEdge Management Trend Database:

1. Go to the **OpenEdge Management Configuration** page's **Trend database location** section.
2. To store trend data locally:
a) Select the **Store trend data in a local OpenEdge Management database** option.

b) Specify the **Trend database location**. You can confirm the predefined explicit path, which matches where the trend database is located by default, or you can type a different path to the database.

   Note that if you enter a path location for the OpenEdge Management Trend Database that is different from the explicit path provided by default, you must also copy the OpenEdge Management Trend Database to the new location. You must use either the procopy or prodb command to preserve the schema integrity.

   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:
   a) Select the **Store trend data in a remote OpenEdge Management database** option.

   b) Enter the host name of the machine in the **Remote web server 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 web server port** field. This is the port number that the OpenEdge Management Web server uses to connect to the remote OpenEdge Management system.

   d) Select the **Use HTTP protocol?** option to use secure communication protocols to connect to the remote OpenEdge Management system.

   e) Enter the user name and password in the **Remote web server user** and **Remote web server password** fields, respectively.

   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 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 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 name** 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 require the default e-mail recipient to enter a user name and password, select the Mail server (SMTP) authentication option and then provide the user name and the password and confirm the password in the fields provided.

6. Select an option from Mail server(SMTP) SSL/TLS to specify if the server is SSL or TLS enabled.

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.

**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.
     - SMTP_MAIL creation is acknowledged.
     - A reminder to use the new password (when restarting OpenEdge Management) appears.

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 are setting up only OpenEdge Explorer.
   - If all the initial configuration values cannot be validated, warning messages appear.
Setting up the Getting Started page for OpenEdge Management

Certain 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 AdminServer and OpenEdge Management commonly recognize. For example:

- A managed database is a database that the AdminServer recognizes and manages. 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 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 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.

The following figure shows the Define monitors for external OpenEdge databases section.

Figure 8: Defining monitors for external OpenEdge databases section

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 conmgr.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.

Note: 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 AdminServer in the AdminServer field.
2. Enter the name of the database you want to display 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 working with database configurations, 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.

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.

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.
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 monitors only 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.

Click **Start using OpenEdge Management** to start using OpenEdge Management.
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. The management console also contains the Database Administration Console. For information about the Database Administration Console, see *OpenEdge Management™ and OpenEdge Explorer: Configuring Multi-tenancy.* For details, see the following topics:

- Starting OpenEdge Management or OpenEdge Explorer
- Using the management console
- Navigating the console
- 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 *Browser support* on page 31 for specifics about which browsers are supported.)

You use the management console to access all OpenEdge Management and OpenEdge Explorer functionality. In addition, you can access the Database Administration Console (to work with databases enabled with multi-tenancy) that is also available from the management console.
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.

Depending on whether you are accessing OpenEdge Management or OpenEdge Explorer from a Web browser or locally, choose either 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 form appears.

• To access OpenEdge Management or OpenEdge Explorer locally from the Windows Desktop, do one of the following:
  • If you have OpenEdge Management/OpenEdge Explorer installed, choose Start > Programs (or All Programs) > Progress > OpenEdge > Management Console.
  • If you have only OpenEdge Explorer installed, choose Start > Programs (or All Programs) > Progress > OpenEdge > OpenEdge Explorer.

To access the Database Administration Console and work with multi-tenancy, choose Start > Programs (or All Programs) > Progress > OpenEdge > Database Administration Console.

The default browser displays the log on screen.

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.

Note: Your request for an OpenEdge Management or OpenEdge Explorer page from an external location may redirect to the logon screen. Once you log on, you are further redirected to the requested page.

When you log on after the first time, you use a new password you created. For OpenEdge Management, the console opens to Dashboard.

In addition to Dashboard, the menu bar in the management console consists of the following functional menu options: Resources, Alerts, Library, Reports, Jobs, and Database Administration. Each option provides access to a list of the relevant actions you can perform.

The Resources option provides access to various tasks, including the creation of a new OpenEdge resource, such as a database or an AppServer, for monitoring and/or configuration in the console.

For OpenEdge Explorer, the console also opens to the Resources page without the Alerts, Library, Reports, or Jobs menu options.

In OpenEdge Management or OpenEdge Explorer, you can click the User icon at the top-right and then click Log out to log off from the management console. You are redirected to the logon screen.

Using the management console

The management console consists of the following components:
Using the management console

- **Menu bar** — In OpenEdge Management, the menu bar provides the following options:
  - Dashboard
  - Resources
  - Alerts
  - Library
  - Reports
  - Jobs
  - Database Administration

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

- Resources
- Database Administration

- **User details menu** — The user details menu on the right shows the name of the logged-on user, the User icon, and the Options icon.

- **Menu icon** — The menu on the left provides access to different areas within OpenEdge Management or OpenEdge Explorer by presenting a collapsible and expandable tree-like structure on the Collection, Name, Type, Status, and AdminServer tabs.

- **Main screen area** — The main screen area displays the OpenEdge Management or OpenEdge Explorer components.

- **Footer bar** — The footer bar shows the Help Me, Support, Privacy, Terms of Use, and Service Agreement options.

- **Grid frame** — The layout for resources in the console. The grid frame displays all resources in local or remote AdminServer within OpenEdge Management or OpenEdge Explorer.

The Resources grid frame consists of the following features:

- **Select** — Check box to select one or more resources from the list of resources.

- **Search** — Field to search for resources using keywords, wildcard characters, or tag names. For example, Database, CPU?, or nhyd*.

- **Type** — Drop-down to filter resources based on their type. For example, AdminServer, AppServer, or Collection.

- **Status** — Drop-down to filter resources based on their status.

- **Group By** — Drop-down to filter resources based on AdminServer, Type, or Status.

- **Start** and **Stop** icons — Start or stop multiple resources simultaneously.

- **Columns** — Sort resources in an alphabetical order. The default view contains the Resource, Type, Status, and Alerts columns. Optionally, you can include the AdminServer column.

- **Resource Summary** — Displays summary of selected resource(s) or a Collection. Depending on the type of resource you select, you can start or stop the resource. You can also use the Collection tags to view a Collection's details page. For more information on using collections as tags, see

- **Alerts** — Displays alerts associated with the selected resource or collection.
Customizing the Resources view

You can customize the Resources view by adding or removing columns to the grid frame. The default view reappears if you either go back to the Resources view after accessing other pages in the console or if you restart the management console.

To customize the Resources view by adding or removing columns:

1. Click the drop-down at the end of a column Columns.
2. To add a column, select the check box.
3. To remove a column, clear the check box.

Note that you can alternatively select the drop-down list in the Resources page, or any of the other tabs’ dropdown lists for access to related tasks. For more information, see Accessing functions from the menu bar tabs for OpenEdge Management on page 54.

Viewing the contents of a AdminServer

When you click the AdminServer name, the AdminServer page appears.

The OpenEdge Management AdminServer 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 AdminServer 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 AdminServer's file systems, including the systems' overall capacity, free space, current usage, and other statistics
- **Disks** — A list of the AdminServer's disks and access to details about each one

Accessing functions from the menu bar tabs for OpenEdge Management

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

- **Dashboard** — Customizable private or shared collections of resources that include views of OpenEdge Management components
- **Resources** — Resources being monitored by OpenEdge Management. These include file, network, database, and system.
- **Alerts** — Open alerts
- **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 local and remote jobs
• **Database Administration** — Multi-tenancy functions
• **User details menu** — The user details menu on the right shows the name of the logged-on user, the **User** icon, and the **Options** icon

**Accessing functions from the menu bar tabs for OpenEdge Explorer**

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

• **Resources** — Resources being monitored by OpenEdge Explorer. These include file, network, database, and system.
• **Database Administration Console** — Functions related to multi-tenancy
• **User details menu** — The user details menu on the right shows the name of the logged-on user, the **Options** icon, and **Help** icon

**Navigating the console**

When you are working with OpenEdge Management or OpenEdge Explorer and you open the management console, you see a list of resources.

For example, if you are working with OpenEdge Management and you click **Library > Go to Library** in the console menu, you see the library-related components in different sections. Links in each section of the page provides access to relevant details about the component. A brief description of each link appears below the link itself.

Some management console pages have a breadcrumb trail that allows you to see where the current page is in relation to the Web site's hierarchy. You can navigate up to the parent level from the page being shown in the console.

**Checking resource status and alert severity**

Once you set up resources, OpenEdge Management and OpenEdge Explorer give you a visual indication to the general status of each resource monitor by using a small, colored icon. Each of the icons in the **Resource Status** list corresponds to a particular status.

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

Similarly, the **Alert severity** list corresponds to a severity warning status.

The following table briefly describes what each status/color combination represents.
Table 2: Resource status legend

<table>
<thead>
<tr>
<th>Status</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>Green</td>
<td>The resource monitor is currently working</td>
</tr>
<tr>
<td>Fail</td>
<td>Red</td>
<td>The most recent test involving the resource failed. This includes statuses such as tardy, timeout, and unreachable. Select <strong>Alerts</strong> or the specific monitor for possible alert details. This status can also identify an internal error that prevents the resource from being monitored.</td>
</tr>
<tr>
<td>Running</td>
<td>Green</td>
<td>The resource is currently running</td>
</tr>
<tr>
<td>Not Running</td>
<td>Blue</td>
<td>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 <strong>Not Running</strong> status to be generated for a database or off-line AdminServer.</td>
</tr>
<tr>
<td>Not Checked</td>
<td>Yellow</td>
<td>The resource monitor’s status is currently unknown. For example, at system startup, it is possible that the resource has not yet been polled.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Black</td>
<td>The resource monitor has been disabled and is not currently monitoring a resource</td>
</tr>
<tr>
<td>Inactive</td>
<td>White</td>
<td>There is no active monitoring plan at this time</td>
</tr>
<tr>
<td>Offline</td>
<td>Gray</td>
<td>The resource is currently offline</td>
</tr>
</tbody>
</table>

**Accessing Help**

From the management console footer bar, select **Help Me** to see context-sensitive help related to the active console page directly, and find OpenEdge Management and OpenEdge Explorer guides.

If no context-sensitive help exists for a particular page, the *OpenEdge Management and OpenEdge Explorer: Getting Started* topic appears. From there, you can select **Search** in the left pane of the management console to search for the specific details you want.
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 resource summary to the right of the resources grid. This information helps you assess—at a glance—properties of the selected resource. Properties vary depending on the selected resource.

• 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 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. 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.) On the console menu bar, click Options 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

You can monitor any resource remotely that you can monitor locally, 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.

For information about setting up local and remote connections for databases enabled for multi-tenancy, see *OpenEdge Management and OpenEdge Explorer: Configuring Multi-tenancy*. For details, see the following topics:

- Remote monitoring and configuration requirements
- Preparing to enable remote monitoring and configuration
- Setting up for remote monitoring or configuration
- Setting up a remote AdminServer
- Disabling remote monitoring of a remote AdminServer

Remote monitoring and configuration requirements

Remote monitoring and configuration require that you have:

- One OpenEdge installation.
For you to perform remote monitoring and configuration, the OpenEdge installation must include OpenEdge Management. For you to perform remote configuration only, OpenEdge Management is not required. You can use OpenEdge Explorer, which is installed with OpenEdge for certain products, as described in Optionally configuring the OpenEdge Management Trend Database on page 31.

One supported standalone installation of OpenEdge Release 11.3 or later, and 11.3 remote AdminServers.

In this standalone installation, neither OpenEdge Management nor OpenEdge Explorer can be enabled. If either is enabled, you must disable it in the Progress or OpenEdge product by running a script known as unglue.

You can monitor multiple AdminServers (AdminServers and/or standalone OpenEdge installations), and you must have system administrator or root permissions on each machine.

When OpenEdge Management is configured for remote monitoring on a host machine, messages are exchanged between it and one or more 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.

Preparing to enable remote monitoring and configuration

Before you enable remote monitoring or configuration, you identify one host machine and one or more non-host machines. Each non-host machine is known as a remote AdminServer.

At a minimum, the host machine must have OpenEdge installed on it along with OpenEdge Management or OpenEdge Explorer. As described in OpenEdge Explorer overview on page 19, OpenEdge Explorer is installed automatically with OpenEdge Management. OpenEdge Explorer is also installed with a number of OpenEdge components.

The remote AdminServer must have an AdminServer installed on it but must not have an enabled installation of either OpenEdge Management or OpenEdge Explorer. If either one is enabled, we recommend that you run the unglue script to "unglue" OpenEdge Management or OpenEdge Explorer from OpenEdge before you enable the machine as a remote AdminServer.

When you run the unglue script on a remote AdminServer, you disable (but not uninstall) OpenEdge Management or OpenEdge Explorer. The ability to unglue OEE and OEM is useful when you want to set up one or several remote AdminServers for one host machine.

As shown in the scenario illustrated in the following figure, Machine A and Machine B have an installation of OpenEdge and OpenEdge Management. (OpenEdge Explorer is also installed.) Machine C has OpenEdge and OpenEdge Explorer installed.
In this scenario, each install of OpenEdge Management (on Machine A and Machine B) can monitor and configure only those resources local to the host on which it is installed (and each install of OpenEdge Management uses its own OpenEdge Management Trend Database). OpenEdge Explorer, on Machine C, configures only its local resources. No monitoring takes place on Machine C because OpenEdge Management is not installed.

An alternative to this scenario is to set up Machine A, for example, as a host machine and Machines B and C as remote AdminServers. To effect this setup, we recommend you run the unglue script on both Machines B and C before you enable either machine as a remote AdminServer. When you run unglue on Machine B, OpenEdge Management and OpenEdge Explorer are disabled. When you run unglue on Machine C, OpenEdge Explorer is disabled.

Should you later decide to discontinue using Machine B or Machine C as a remote AdminServer, you can run reglue, which re-enables OpenEdge Management or OpenEdge Explorer in the OpenEdge product. For details about reglue, see Regluing OpenEdge Management or OpenEdge Explorer to OpenEdge on page 63.

Ungluing OpenEdge Management or OpenEdge Explorer from OpenEdge

If the machine you intend to use as a remote AdminServer has OpenEdge Management and/or OpenEdge Explorer installed, we recommend you unglue either or both from OpenEdge before you set up the machine as a remote AdminServer.
You must have system administrator privileges on Windows and root privileges on UNIX to perform the unglue operation.

To unglue OpenEdge Management or OpenEdge Explorer:

1. Depending on whether you are working with a Windows or a UNIX installation, begin the unglue as follows:
   - To unglue on a Windows machine, select **Start > Programs (or All Programs) > Progress > OpenEdge > Proenv**.
   - To unglue on a UNIX machine, log in as root in a terminal window. If you do not know the root password for your system, consult with your system administrator.

2. At the prompt, type `unglue`, as shown here for a Windows install:

   ```
   unglue
   ```

   Details similar to the following appear:

3. Type `y` to continue, and press **ENTER**. The following details appear:

4. You must restart the AdminServer to complete the unglue process. At the prompt, type `proadsv -stop` (for a Windows install) to stop the AdminServer, and then `proadsv -start` to start the AdminServer.
You can now set up the machine as a remote AdminServer, as described in Setting up a remote AdminServer on page 64. To reglue OpenEdge Management or OpenEdge Explorer to the Progress or OpenEdge product, see Regluing OpenEdge Management or OpenEdge Explorer to OpenEdge on page 63.

Regluing OpenEdge Management or OpenEdge Explorer to OpenEdge

If you no longer intend to use a machine as a remote AdminServer, you can reglue OpenEdge Management and/or OpenEdge Explorer to OpenEdge.

You must have system administrator privileges on Windows and root privileges on UNIX to perform the reglue operation.

To reglue OpenEdge Management or OpenEdge Explorer:

1. Depending on whether you are working with a Windows or a UNIX installation, begin the reglue as follows:
   - To reglue on a Windows machine, select **Start > Programs (or All Programs) > Progress > OpenEdge > Proenv**.
   - To reglue on a UNIX machine, log in as root in a terminal window. If you do not know the root password for your system, consult with your system administrator.

2. At the prompt, type `reglue`, as shown here for a Windows install:

   ```
   reglue
   ```

   Details similar to the following appear:

3. Type `y` to continue, and press **ENTER**.

4. You must restart the AdminServer to complete the reglue process. At the prompt, type `proadsv -stop` (for a Windows install) to stop the AdminServer, and then `proadsv -start` to start the AdminServer.

If you want to set up remote monitoring and need to disable OpenEdge Management and/or OpenEdge Explorer, see Ungluing OpenEdge Management or OpenEdge Explorer from OpenEdge on page 61.
Setting up for remote monitoring or configuration

The order in which you set up machines for remote monitoring or configuration is important. The following are required:

- The remote AdminServer must be up when you establish the required settings on any intended remote AdminServer.
- OpenEdge Management must be up for setting up the remote AdminServer using the Options page.
- (Recommended) OpenEdge Management or OpenEdge Explorer be disabled on the remote AdminServer.

Setting up a remote AdminServer

You can monitor any resource remotely that you can monitor locally, 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.

You set up the remote AdminServer using the Options page. See Administering OpenEdge Management and OpenEdge Explorer on page 67 for details on how to set up a remote AdminServer.

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

After you setup the Remote AdminServer on the host machine, you see the remote AdminServer in the host machine's console.

To verify that the remote AdminServer is visible:

1. From the management console on the host machine, click Resources > Go to Resources.
2. Sort the resources by AdminServer. The local host and the newly added remote AdminServer appear in the tree view.

   The local host is identified by the following lifesaver icon:

   ![Lifesaver Icon]

Disabling remote monitoring of a remote AdminServer

If you want to stop remote monitoring, you can do one of the following:

- Clear the Monitored check box in the Manage Remote AdminServers page that was set at the time of setting up the Remote AdminServer. For more information on setting up the Remote AdminServer, see Setting up a remote AdminServer on page 64.
Disabling remote monitoring of a remote AdminServer

- Set the `isMonitored` property in the file, `management.properties`, to false. This disables the listeners of the activemq broker, and disallows OEM to connect to the specific Remote AdminServer.

**Note:** By default, the `management.properties` file is in the location, `$DLC\properties`. 
Administering OpenEdge Management and OpenEdge Explorer

You can fine-tune the initial OpenEdge Management or OpenEdge Explorer configuration and licensing decisions you made.
For details, see the following topics:

- Updating configuration options
- Adding users as administrators or operators
- Customizing the operator role
- Setting OpenEdge Management user preferences
- Setting up a remote AdminServer
- Changing general configuration settings
- Changing OpenEdge Management e-mail alerts settings
- Changing OpenEdge Management resource monitoring settings
- Setting the OpenEdge Management graph cache
- Configuring process pooling
- Setting OpenEdge Management resource monitor defaults
- Setting OpenEdge Management distribute resource properties
- Changing the OpenEdge Management SNMP Adapter settings
• Using the command-line interface
• Using the OpenEdge environment window Proenv
• Setting the log level for the AdminServer log file

Updating configuration options

You can use OpenEdge Management or OpenEdge Explorer to update configuration options. You can update options that are set during the initial setup process. You can also set other configuration options and develop a better understanding of which options work best for your environment.

From the management console menu bar, click Options. If you have OpenEdge Management installed, the Options page appears.

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 the following table.

Table 3: Configuration option availability

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Applicable in OpenEdge Management</th>
<th>Applicable in OpenEdge Explorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Users</td>
<td>Enables you to manage user accounts and to customize the operator role</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Preferences</td>
<td>Enables you to set the rate (if any) at which OpenEdge Management automatically refreshes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Remote AdminServers</td>
<td>Enables you to add and remove remote AdminServers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>General</td>
<td>Enables you to manage the OpenEdge Management startup configuration and the actions to perform for OpenEdge Management internal alerts</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trend Database</td>
<td>Enables you to configure the trend database</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Web Server Configuration</td>
<td>Enables you to configure the Web server HTTP and HTTPS settings. You can also set the login session timeout value.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Updating configuration options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Applicable in OpenEdge Management</th>
<th>Applicable in OpenEdge Explorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email alerts</td>
<td>Provides the SMTP host name and port along with the e-mail address of the default recipient for e-mail notification when an alert is generated. You can also configure SMTP settings, such as user name and password.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resource Monitoring</td>
<td>Enables you to manage whether to automatically poll resources, generate alerts, collect trend data, and include status changes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Graph Cache</td>
<td>Enables you to set the time period for collecting graph cache samples on selected resources and AdminServers</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Database Administration Console</td>
<td>Enables you to set the batch size for the database administration console</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Process Pooling</td>
<td>Maintains several instances of _progress running persistently. As an alternative to using the built-in process pooling, you can configure process pooling to use an AppServer.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource Monitor Defaults</td>
<td>Enables you to set default polling attributes for resource functions</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resource Property Distribution</td>
<td>Enables you to bulk copy resource properties to selected target resources</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SNMP Adapter</td>
<td>(If installed) enables you to start or stop the SNMP Agent. You can also set SNMP adapter settings, such as SNMP agent port and default SNMP trap port.</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

By choosing to use the HTTPS protocol for secure browser-to-instance or instance-to-instance communications, you can set trend database and Web server configuration settings. See Setting Up Secure Communications on page 95 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 functionalities. 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, click Options.

   The Options page appears.

2. Click Authorized Users.

   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: You cannot delete the predefined admin user, although you can modify its password.

Adding a new user

If you are logged in as an administrator in OpenEdge Management or OpenEdge Explorer, you can add new users.
The added user name, password, and description information is saved in the fathomRealm.properties file that is available in the `<OpenEdgeManagement-install-dir>/etc` folder. This information is saved in the following format:

```plaintext
<username>: [hash algorithm]:<password>[<salt>[:<iterations>]] [,<rolename> ...]
DESCRIPTION: <user description>
```

To add a new user:

1. From the **Authorized Users** page, click **Add User**. The **User** page appears.
2. Enter a unique user name in the **Name** field. The name can contain up to 32 alphanumeric characters. Spaces are not allowed in the name. Optionally, enter a user description.
3. Select a user role in the **Role** list: **Administrator**, **Operator** or **Trending**.

   **Note:** Only a user with the **Administrator** user role can create a user with the **Trending** user role.

4. Enter a password in the **Password** field. The password must be a minimum of 4 characters in length. The password is encrypted using the SHA-256 hashing algorithm.
5. Re-enter the password in the **Confirm password** field.
6. Click **Save**. The user name and description appears in the list of authorized users on the **Authorized Users** page. The fathomRealm.properties file gets updated as well.

   Optionally, you can add a new user by entering the credentials in the defined format directly in the fathomRealm.properties file.

   You can restore the default user name credentials by replacing the contents of the fathomRealm.properties file with the contents of the fathomRealm.properties.orig file that is present at the same folder location.

   **Note:**

   If you are adding users by entering credentials in the fathomRealm.properties file or if you are restoring the default credentials, you must stop and restart the OpenEdge Management or OpenEdge Explorer for the operation to take effect.

   Progress recommends using the OpenEdge Management or OpenEdge Explorer to add new users.

You can also add a new user by copying the details of an existing user from the list of authorized users and then modifying the user details.

To add a new user by copying an existing user:

1. Select the user from the **Authorized Users** page. The **User: <user name>** page appears.
2. Click **Copy**.
3. Modify the existing user details as required. You must enter new values in the **Name**, **New password**, and **Confirm new password** fields.
4. Click **Save**.
5. The user name and description appears in the list of authorized users on the **Authorized Users** page.
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. Administrators can edit the password or description of any user, but operators are restricted to editing only their own password and description.

If an administrator changes a user 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 login process 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.
2. Click Edit to edit the user details. The User: <user name> page appears.
   - If required, you can make changes in the Description field and also change your selection in the Role list.
3. Select the Change password? check box to change the password. The fields required to change the password are enabled.
4. Enter your current password in the Enter your password field.
5. Enter the new password once in the Password field, and then again in the Confirm Password field.
6. Click Save.
   - If the Enter your password field is left empty or if your current password is incorrect, you receive an error message.
   - The User page reappears, showing any changes that you might have made to the user name or description details. or Copy to either edit the user details or copy them as details for another user. If you copy the details, you must change the user name, since duplicate user names are not allowed.

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 Changing passwords and descriptions on page 72 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 a user:

1. Select the user from the Authorized Users list.
2. Click Delete. Click Yes to confirm the deletion
   - The deleted user’s access is stopped immediately.
Customizing the operator role

As an administrator, you can determine the functionalities that the operators can access. If you make no changes, the operators are restricted to read-only permissions.

The assigned role permissions are saved as JSON values in the `fathomRealm.policy` file that is available in the `<OpenEdgeManagement-install-dir>/etc` folder.

**Note:** The role permissions apply for every user that has been assigned to the Operator role.

To customize the operator role:

1. From the management console menu bar, click **Options**.
   
   The Options page appears.

2. Click **Authorized Users**.

   The Authorized Users page appears.

3. Click **Customize Operator Role**. The Operator Role Customization page appears.

   In OpenEdge Management, the page displays the following areas: Database operations, OpenEdge operations, Resource and monitor operations, and Task operations.

   In OpenEdge Explorer, the page displays only the Database operations and OpenEdge operations areas.

4. Use one of the following methods to set operator permissions:

   - Select an option to make it available for operators.
   - Click **Select All** to select all the options.
   - Click **Select None** to clear all the options.

   **Note:** If you select the Start/Stop Database option under Database, the Start/Stop Agent option is automatically selected. However, you can select Start/Stop Agent without selecting Start/Stop Database.

   For the operator, only the Stop Agent option is available under Scripted Database.

5. Click **Submit** to apply the permission settings.

   You can restore the default roles and permissions by replacing the contents of the `fathomRealm.policy` file with the contents of the `fathomRealm.policy.orig` file that is present at the same folder location.

   **Note:** If you are restoring the default roles and permissions, you must stop and restart the OpenEdge Management or OpenEdge Explorer for the operation to take effect.
Managing access to the Database Administration Console

As an administrator, you can customize the operator role to manage access to the Database Administration Console (Database Administration) of OpenEdge Management or OpenEdge Explorer. You can set the following permissions:

- **Disallow Read Access** — If this option is selected, Database Administration is disabled for the operator.

- **Allow Create Connections** — If this option is selected, Database Administration is enabled for the operator. The operator can create a new database connection. The operator can also create a copy of or delete an existing database connection.

- **Allow Edit Connections** — If this option is selected, Database Administration is enabled for the operator. The operator can edit an existing database connection.

Without any Database Administration Console permissions assigned, by default, the operator can use existing database connections. For more information on creating, editing, and using database connections, see *OpenEdge Management and Explorer: Configuring Multi-tenancy* and *OpenEdge Management and Explorer: Managing Table Partitioning in Databases*.

The assigned role permissions are saved as JSON values in the fathomRealm.policy file that is available in the `<OpenEdgeManagement-install-dir>/etc` folder. The following sample shows the default Database Administration Console permission for the operator role:

```json
{
   "roles" : [
      { // Administrator roles
      },
      { "name" : "PSCOper"
      },
      "grants" : [ {
      // Other operator roles
      },
      { "object" : "dac.*", 
      "actions" : "read"
      }
      ],
      },
      { // Trend user roles
      }
   ]
}
```

The following table shows the assigned JSON values in the fathomRealm.policy file for the permissions to the Database Administration Console:

**Table 4: Permissions to the Database Administration Console**

<table>
<thead>
<tr>
<th>Permission</th>
<th>JSON value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disallow Read Access</td>
<td>&quot;actions&quot; : &quot;&quot;</td>
</tr>
<tr>
<td>Allow Create Connections</td>
<td>&quot;actions&quot; : &quot;create&quot;</td>
</tr>
<tr>
<td>Allow Edit Connections</td>
<td>&quot;actions&quot; : &quot;write,read&quot;</td>
</tr>
</tbody>
</table>
To manage access to the Database Administration Console:

1. In the **Options** page, click **Customize Operator Role**. The **Operator Role Customization** page appears.
2. In the **Database operations** area, select the operator permissions under **Database Administration Console**.
3. Click **Submit** to apply the permission settings.

**Note:** If you are moving from an older version of OpenEdge Management or OpenEdge Explorer to version 11.6 and you still want to continue using the `fathomRealm.policy` file from the older version, you must add information related to the Database Administration Console permissions in the file.

### 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

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

1. From the management console menu bar, click **Options**.
   - The **Options** page appears.
2. Click **User Preferences**.
   - The **User Preferences** page appears.
3. Set the time value for automatically refreshing pages in the **Automatically refresh pages** list.

**Note:** Consider your page refresh requirements before setting the value. Frequently refreshing pages add to the OpenEdge Management processing time.

4. Click **Set** to submit the set time value.

### Setting up a remote AdminServer

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

To set up a remote AdminServer:
1. From the management console menu bar, click **Options**.
   
   The **Options** page appears.

2. Click **Remote AdminServers**.
   
   The **Remote AdminServer Configuration** page appears and displays a list of AdminServers.

3. Click **New** to add a Remote AdminServer information:
   a) In the **Host** field, enter the host name of the machine used to run OpenEdge Management or OpenEdge Explorer.
   b) Select the **SSL** option to secure the communication between OpenEdge Management or OpenEdge Explorer and the remote AdminServer. The default SSL protocol is TLS version 1.2.
      
      If the **SSL** option is selected, the default certificates provided by OpenEdge are used. For information on setting up the SSL protocol mechanism for remote AdminServers with user-defined certificates, see **Setting up secure communication-related security for a remote AdminServer** on page 77.
   
   c) In the **Port** field, enter the port number used to run the AdminServer.
   d) Select the **Monitored** option to enable the monitoring of remote AdminServer resources.
   e) Enter the **Username** and **Password** to specify the user information used to access the AdminServer. This can also be information about the machine on which the AdminServer resides.

4. Click **Save**. The configured AdminServer is displayed in the list of AdminServers.

**Viewing a remote AdminServer**

You can view a configured remote AdminServers based on the status of the AdminServers. The **Show online and offline** bullet by default view displays all the AdminServers being managed.

You can view AdminServers based on the following status values:

- **Show online and offline**
- **Show only online**
- **Show only offline**
- **Show only auto-discovered**

**Deleting a remote adminserver**

You can delete a configured remote adminserver per your requirements.

To delete a remote AdminServer:

1. From the management console menu bar, click **Options**.
   
   The **Options** page appears.

2. Click **Remote AdminServers**.
   
   The **Remote AdminServer Configuration** page appears with a list of AdminServers.

3. Select one of the AdminServers from the list, and click **Delete**. Click **Yes** in the confirmation dialog.
Setting up secure communication-related security for a remote AdminServer

You can set up secure communication-related properties for a remote AdminServer to ensure that communication between OpenEdge Management or OpenEdge Explorer and a remote AdminServer is secure. For more information on setting up a remote AdminServer, see Setting up a remote AdminServer on page 75.

The following table lists all the properties in management.properties file at the %DLC%\properties location:

<table>
<thead>
<tr>
<th>Property</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslEnable</td>
<td>0</td>
<td>Enables you to set the cryptographic protocols and ciphers for secure communication with a remote AdminServer. To set the default cryptographic protocols and ciphers for the remote AdminServer, set this property value to 1. You must reset the remote AdminServer and OpenEdge Management or OpenEdge Explorer for the setting to take effect.</td>
</tr>
<tr>
<td>enabledProtocols</td>
<td>TLSv1.2</td>
<td>Supported values: SSLv3, TLSv1, and TLSv1.1. If you want to change the default cryptographic protocol for the remote AdminServer, enter this property in the management.properties file. The property accepts a comma-separated list of valid cryptographic protocols that are set for secure communication.</td>
</tr>
<tr>
<td>enabledCipherSuites</td>
<td></td>
<td>If you want to change the default cryptographic protocol for the remote AdminServer, enter this property in the management.properties file. The property accepts a comma-separated list of valid cryptographic protocols that are set for secure communication.</td>
</tr>
<tr>
<td>tcpEnable</td>
<td>1</td>
<td>Enables unsecure connections to remote AdminServer. To disable it, set the property value to 0. This only affects the TCP connection for incoming management connections. It does not affect TCP connections for outgoing OpenEdge Management connections to a remote AdminServer.</td>
</tr>
<tr>
<td>sslPort</td>
<td>7278</td>
<td>Specifies the port using which OpenEdge Management receives the incoming secure connections</td>
</tr>
<tr>
<td>Property</td>
<td>Default value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>port</td>
<td>6835</td>
<td>Specifies the port using which OpenEdge Management receives non-secured connections</td>
</tr>
<tr>
<td>keyAlias</td>
<td>default_server</td>
<td>Specifies the alias set for a private/public key. If this property is not set, the server certificate alias that is provided by OpenEdge is used.</td>
</tr>
<tr>
<td>keyAliasPasswd</td>
<td>-NA-</td>
<td>Specifies the password set for the alias of the private/public-key. This password is expected to be encoded. You can use the OpenEdge provided genpassword utility for encoding your passwords. For information on the genpassword utility, see <em>OpenEdge Getting Started: Installation and Configuration</em>. If this property is not set, the password of the default alias that is provided by OpenEdge is used.</td>
</tr>
<tr>
<td>keyStorePath</td>
<td>-NA-</td>
<td>Specifies the key store location. If this property is not set, the default value is <code>$DLC/keys</code>.</td>
</tr>
<tr>
<td>sslRequireClientAuth</td>
<td>0</td>
<td>When set to 1, this property specifies that an incoming secure connection must provide a valid client certificate to connect to the AdminServer.</td>
</tr>
<tr>
<td>keyStorePasswd</td>
<td>-NA-</td>
<td>Specifies the password used for accessing the custom keystore. This password is expected to be encoded. You can use the OpenEdge provided genpassword utility for encoding your passwords. For information on the genpassword utility, see <em>OpenEdge Getting Started: Installation and Configuration</em>.</td>
</tr>
<tr>
<td>noHostVerify</td>
<td>0</td>
<td>When set to 1, OpenEdge Management disables host verification when connecting to a remote AdminServer that has a private key.</td>
</tr>
</tbody>
</table>

**Note:** By default, host verification is bypassed when the `default_server` key is used.

Using the secure communication properties, you can implement secure communication for the Remote AdminServers in the following ways:

- **Without private key information:** This is the basic and default secure communication configuration used when you set up a cryptographic protocols-enabled Remote AdminServer in the *Remote Adminserver Configuration* page. Using this configuration, you are using the
OpenEdge-provided server certificate from the certificate store. This configuration does not require any private key information.

This is the recommended setting for testing the secure communication configuration of a remote AdminServer.

• **With private key information for the Remote AdminServer:** Using this configuration, you can create and store your server certificate on the server side for OpenEdge Management to connect to the remote AdminServer and validate the private key provided by the remote AdminServer.

You must perform the following steps to configure a cryptographic protocol-enabled remote AdminServer with private key information on the remote AdminServer:

1. Generate a private/public key and certificate for the remote AdminServer that requires secure communication. You can use OpenEdge-provided utilities for generating the key and certificate. For more information about managing the OpenEdge key and Certificates Stores, see the *OpenEdge Getting Started: Installation and Configuration* guide.

2. Open the `management.properties` file from `$DLC\properties` and edit the properties to point to the private/public key and certificate information.

3. Restart OpenEdge Management for the settings to take effect.

• **With private key information for the remote AdminServer and OpenEdge Management:** In this configuration, you create and store your server and client certificates in OpenEdge Management and remote AdminServer, respectively, for OpenEdge Management to connect to the remote AdminServer. You must validate the private key provided by the remote AdminServer on a OpenEdge Management end, and validate the private key provided by OpenEdge Management on a remote AdminServer end.

You must perform the following steps to configure an cryptographic protocol-enabled remote AdminServer with private key information on the remote AdminServer:

1. Generate a private key and certificate for the remote AdminServer and OpenEdge Management for secure communication. You can use OpenEdge-provided utilities for generating the key and certificate. For more information about managing the OpenEdge key and Certificates Stores, see the *OpenEdge Getting Started: Installation and Configuration* guide.

2. Open the `management.properties` file from `$DLC\properties` and edit the properties to point to the private/public key and certificate information. Ensure that the `sslRequireClientAuth` property is set to 1.

3. Configure the remote AdminServer to authorize the private-key information that it receives from OpenEdge Management.

4. Restart OpenEdge Management and the remote AdminServer for the settings to take effect.

## Changing general configuration settings

You can change the following current general configuration settings:

- Automatically starting OpenEdge Management or OpenEdge Explorer when the AdminServer starts.
• The action OpenEdge Management or OpenEdge Explorer should perform, if any, for internal alerts. You can select an action from the Action to perform on internal OpenEdge Management alerts list for internal alerts.

For example, for the OpenEdge Management Trend Database, you set set the action value to Default_Action for a set of default actions to be taken in response to the status, availability, or performance of the monitored resource.

To change the general settings:

1. From the management console menu bar, click Options.
   The Options page appears.
2. Click General.
   The OpenEdge Management General Configuration page appears.
3. Set the following options, as required:
   • Select the Start OpenEdge Management automatically option to start OpenEdge Management or OpenEdge Explorer automatically when the AdminServer starts.
   • Select the Prompt for comments on alert clear option to provide a comment (Optional) in the Clear Alert dialog box which appears while clearing an alert.
   • Select the Require comments on alert clear option to ensure that a comment is required in the Clear Alert dialog box whenever an alert is cleared.
   • (OpenEdge Management only) Select an option from the Action to perform on internal OpenEdge Management alerts option to specify an action that OpenEdge Management performs when an internal alert is triggered.
4. Click Submit. The OpenEdge Management 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, click Options.
   The Options page appears.
2. Click Email alerts.
   The OpenEdge Management Email Alerts Configuration page appears.
3. Enter the SMTP host name in the Mail server (SMTP) host name field. Check with your e-mail administrator if you do not know the e-mail host name.
4. Enter the port used by the SMTP host in the Mail server (SMTP) port field. On most systems, this is port 25.
5. 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.
6. Enter the default domain value in the Default Domain field.
7. If you require the default e-mail recipient to enter a user name and password, select the **Mail server (SMTP) authentication** option and then provide the user name and the password and confirm the password in the fields provided.

8. Select an option from **Mail server(SMTP) SSL/TLS** to specify if the server is SSL or TLS enabled.

9. Set the **Mail server(SMTP) SSL/TLS enabled protocols** options to change the default cryptographic protocols. By default, remote trending databases support **TLSv1**, **TLSv1.1**, and **TLSv1.2**.

10. Enter comma-separated cipher suite values in the **Mail server(SMTP) SSL/TLS enabled cipher suites** field to manually set cipher suites. By default, OpenEdge Management and OpenEdge Explorer supports all the cipher suites that are provided by the SSL implementation of the Java Secure Socket Extension (JSSE).

11. Click **Submit**.

### Changing OpenEdge Management resource monitoring settings

You can manage 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 the **Collect trend data** option is not selected, the **Include status changes** option is disabled.

These resource monitor options allow you to disable specific OpenEdge Management functionalities. 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, click **Options**.
   The **Options** page appears.

2. Click **Resource Monitoring**.
   The **OpenEdge Management Resource Monitoring Configuration** page appears.

3. Select or clear the required options.

4. Click **Submit**.
Setting the OpenEdge Management graph cache

OpenEdge Management graphing includes a persistent data cache. You can determine the time period for which graph data cache samples are collected on a per-resource-instance basis. The default graph cache setting is 15 days. If you change the setting to a longer period, more disk space is used to store the growing cache. Consequently, the more data that has been stored, the more data there is to be represented in a graph. This results in higher CPU usage at the time a graph using the data is created.

It is recommended that you start with the 15-day default graph cache setting. You can then increase the value, if required, by small increments to test the impact on disk space and CPU activity. Alternatively, you can set certain resource types to the 15-day default and set others to a different time period, such as 12 hours to save memory and CPU usage.

To set the OpenEdge Management graph cache:

1. From the management console menu bar, click **Options**.
   
   The **Options** page appears.
2. Click **Graph Cache**.
   
   The **Graph Cache Database Configure** page appears.
3. In the **Sample time period to collect** field, type the graph cache time period you want to apply to the resources. Set the time unit to **hours** or **days**. The default time period is 15 days.
4. Select the resources to which you want to apply the selected graph cache time period:
   a) In the **List resource of type** list, set the resource types either by selecting from the available resources or by selecting the wildcard ( * ).
   b) In the **for AdminServer** field, set the AdminServers either by selecting from those available or by selecting the wildcard ( * ).

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

5. Click **Apply Filter**. The resource types that match the filter specifications appear in the **Available** list.
6. Select the resources:
   - Click **Select All** to select all the resources in the **Available** list and then click the right arrow.
   - Click on each resource you want to select and then click the right arrow.

   The resources appear in the **Selected** list. The information in the angular brackets to the right of each resource name is the current graph cache setting for that resource.
7. Click **Apply to selected**. Click **OK** in the confirmation dialog that appears.

   You can verify that the time period has been changed correctly by selecting the resources and AdminServers and then clicking **Apply Filter**. The **Available** list displays the resources with the updated graph cache setting in the angular brackets.
**Configuring process pooling**

To reduce processing overhead and improve Web request performance, OpenEdge Management and OpenEdge Explorer provide built-in process pooling. Process pooling maintains several instances of _progress_ running persistently. As an alternative to using built-in process pooling, you can configure process pooling to use an AppServer.

You can disable process pooling to stop instances running in the background. If you disable process pooling, however, you might notice a short delay as you navigate through certain Web pages, such as the **Tenant details** page for a database enabled for multi-tenancy.

Built-in process pooling is configured with global settings that apply to all local and remote AdminServers that are running under the OpenEdge Management or OpenEdge Explorer instance. You can also configure process pooling for each AdminServer that allows you the flexibility to vary settings individually for remotely residing databases.

**Process pooling modes**

Process pooling is available in the following three modes:

- **Built-in pooling**
- **AppServer pooling**
- **Disabled pooling**

Using built-in pooling, OpenEdge Management handles a set of OpenEdge client processes. When the ABL APIs are called, these processes improve performance by eliminating the overhead of starting and stopping a process each time. You can control the maximum number of _progress_ processes that are kept alive at any time. The processes do not maintain a persistent connection to the database. Instead, each request to OpenEdge Management or OpenEdge Explorer from a Web browser causes one of the AVMs (_progress.exe) to connect to a database and then run the proper data administration API. Built-in pooling is the default process pooling mode.

Using AppServer pooling, it is the AppServer, instead of the OpenEdge client process, that runs the ABL APIs. Each request from OpenEdge Management or OpenEdge Explorer is sent through the specified AppServer using a specified AppServer URL to call the ABL API. The Java Open Client is used to connect to the specified AppServer.

You can set up AppServer pooling to manage the calls to the database by using the AppServer instead of through an _progress_ AVM managed by OpenEdge Management. You control the number of agents with the AppServer settings.

**Note:** The AppServer for pooling must be dedicated to OpenEdge Management (in other words, the AppServer must not be in use by other ABL clients), and it should be configured to use the state-reset mode. In addition, there must be no database connections defined for the agents.

When you disable pooling, you use the least amount of memory. However, you also experience the least effective performance. A new AVM is started on each request from the Database Administration Console. A new database connection is made on the startup of each OpenEdge client process (_progress_), and the ABL API is run using the `-p` startup parameter.

You can disable pooling in the following cases:
• If you experience issues using either built-in or AppServer pooling
• If you prefer not to have _progress running continuously
• If performance is not the primary focus

Setting process pooling options

You can choose the process pooling mode and set values for relevant properties.

To set process pooling options:
1. From the management console menu bar, click Options.
   The Options page appears.
2. Click Process Pooling.
   The Process Pooling Configuration page appears and allows you to set system-wide process pooling defaults for all local and remote AdminServers being managed by this instance of OpenEdge Management or OpenEdge Explorer.
3. Select the mode from the following options:
   • Disabled
   • Use built-in pooling
   • Use OpenEdge AppServer
4. Depending on the selected mode, enter the following information:
   • For the built-in processing mode:
     • Port — The port number for the process pooling server. The default value is 4444.
     • Maximum agents — The maximum number of agents. The default value is 3.
     • Timeout — The maximum time, in milliseconds, to wait before starting _progress. The default value is 1500.
     • Log File — The file system path to the log file for the agents.
   • For the OpenEdge AppServer mode:
     • AppServer URL — The URL used to connect to the AppServer. If you do not specify a URL, AppServer://localhost:5162/appService is used.
     • AppService name — The name of the application service to use on the AppServer. The service name is used to identify the set of brokers that are expected to respond to requests. If you do not provide an AppService name, the default AppServer application service is used.
5. Click Submit.

Creating a new process pooling configuration

You can create a new process pooling configuration and use it, rather than the global settings, for one or more AdminServers.
You can also use the Restore option to cancel the editing of an existing configuration or creation of a new one.

To create a new process pooling configuration:

1. From the **Process Pooling Configuration** page, click **Customize > New**.
2. Select the AdminServer in the **AdminServer** list. You can set the required configuration of the selected AdminServer.
3. Select one of the following functions:
   - Click **Submit**. The configuration is saved and is displayed in the grid.
   - Click **Restore**. The new or edited configuration settings are not saved.

### Deleting a custom process pooling configuration

You can delete a custom process pooling configuration for a specific AdminServer. When you delete the custom configuration, the process pooling settings for that AdminServer revert to the global process pooling settings.

To delete a custom process pooling configuration:

1. From the **Process Pooling Configuration** page, click **Customize**.
2. Select a configuration in the grid and click **Delete**. Click **Yes** in the confirmation dialog.

### Setting OpenEdge Management resource monitor defaults

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

- AppServer
- AppServer Internet Adapter
- Databases
- DataServers (ODBC, Oracle, and MS SQL Server)
- File
- NameServer
- Network
- OE Web Server
- Pacific Application Server for OpenEdge (PAS for OpenEdge)
- SonicMQ Adapter
- System
- WebSpeed Messengers
- WebSpeed Transaction Server
- Web Services Adapter
To choose the default options:

1. From the management console menu bar, click **Options**.

   The **Options** page appears.

2. Click **Resource Monitor Defaults**.

   The **OpenEdge Management Resource Monitoring Defaults** page appears.

3. Click a resource category. The defaults page for the selected category appears.

4. Set the default value(s).

5. Click **Submit**. A dialog appears confirming that the values have been successfully updated.

You can click **Restore Defaults** in the category defaults page to revert to the original OpenEdge Management defaults for that category.

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*.

## Setting OpenEdge Management distribute resource properties

The **Resource Property Distribution** option enables you to distribute resource monitor polling properties from an existing resource to one or more other resources. You can change a number of existing resource monitors to have the same polling properties and possible rules, by selecting one of the following source types:

- AppServer
- CPU
- Database
- FileSize
- HTTP
- LogFile
- Memory
- NameServer
- PAS
- REST
- TCP
- WebSpeed

To distribute resource polling properties:
1. From the management console menu bar, click **Options**.
   The **Options** page appears.

2. Click **Resource Property Distribution**.
   The **Distribute Resource Properties** page appears.

3. In the **Resource Selection** section:
   a) Select a source AdminServer in the **Source Container** list.
   b) Select a source type in the **Source Type** list.
   c) Select a source resource in the **Source Resource** list.
   d) Select the AdminServer in the **Target Container** list to which you want to distribute resource polling properties. The resources associated with the selected target AdminServer appear in the **Target Resources** section.
   e) Select the **Remove and replace existing rules** to distribute resource rules along with polling properties.

4. From the **Available Targets** list, select the resources and click the right-arrow. The selected resources appear in the **Selected Targets** list.

5. Click **Submit** to start distributing the polling properties. Click **OK** in the confirmation dialog.
   The **Resource definition distribution summary** page displays the resources for which the polling properties have been updated.

---

**Changing the OpenEdge Management SNMP Adapter settings**

OpenEdge Management and OpenEdge Explorer provides an SNMP management agent (SNMP Adapter) for responding to administrative information queries from your SNMP management console or SNMP manager. OpenEdge supports SNMP versions 2c and 3. OEM defaults to SNMP version 2c.

In response to the queries from your manager, the information that the SNMP agent retrieves is called a variable binding and is uniquely identified by an object identifier (OID). For instance, the OID 1.3.6.1.2.1.1.3 is defined for the 'up-time of agent' value.

All SNMP messages are sent as protocol data units (PDU). A PDU consists of a header and a variable binding. A PDU can be of the following types: GET, SET, BULKGET, GETNEXT, or NOTIFICATION. A PDU of the GET or NOTIFICATION type is an asynchronous notification and also called a trap. The manager can set alerts in OEM to receive traps when an alert is triggered. In response to receiving a trap, the manager performs a recording action, such as sending an e-mail or recording a statistic. Depending on your SNMP environment configuration, the trap is sent to a specific host or to a broadcast address. The description for all the traps for possible OEM alerts is stored in the OEM MIB file, **PSC-FM-MIB.txt**, available at the `<OpenEdge-install-dir>/config` location.

In SNMP version 2c, you can assign users to read and write access to the SNMP agent. SNMP version 3 adds security enhancements to the SNMP version 2c functionality. SNMP version 3 authenticates users to access the SNMP agent and relies on a User-based Security Model (USM) for providing 3 security levels:

- Communication without authentication and privacy (**NoAuthNoPriv**)
- Communication with authentication and without privacy (**AuthNoPriv**)
- Communication with authentication and privacy (**AuthPriv**)
The minimum security level required is **NoAuthNoPriv**.

**Note:** The security configuration of the SNMP manager must match the OEM SNMP security configuration. For example, if you are using SNMP version 3 with **AuthNoPriv** in OEM, the SNMP manager must be configured to use SNMP version 3 with **AuthNoPriv**.

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

To change the SNMP Adapter settings:

1. From the management console menu bar, click **Options**.
   
   The **Options** page appears.

2. Click **SNMP Adapter**.
   
   The **SNMP Adapter** page appears and displays the SNMP agent status and information.

3. Click **Edit**. You can set the **SNMP version** and one or more of the following settings:

   - **SNMP Version** — The version of SNMP.
   - **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 default port number is **8002**.
   - If you set the SNMP version as **Version 2c**, set the following options:
     
     - **Default SNMP read community** — The community that specifies who has permissions to read which variables.
     - **Default SNMP 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.)
   - If you set the SNMP version as **Version 3**, set the following options:
     
     - **Security Name** — The SNMP security user name. This user name is required to access the SNMP agent.
     - **Security Level** — The SNMP security level. You can select from 3 security levels:

<table>
<thead>
<tr>
<th>Security level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Authentication and No Privacy</td>
<td>This level does not require you to set any authentication and privacy options.</td>
</tr>
</tbody>
</table>
### Security level Description

<table>
<thead>
<tr>
<th>Security level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication but No Privacy</strong></td>
<td>This level requires you to set the following authentication options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authentication Protocol</strong> — The authentication mechanism that is used to generate a hash of the authentication password (SHA or MD5).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authentication Password</strong> — The SNMP security authentication password.</td>
</tr>
<tr>
<td><strong>Authentication and Privacy</strong></td>
<td>This level requires you to set the authentication options and the following privacy options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Privacy Protocol</strong> — The encryption protocol used to encrypt SNMP communications (AES256, 3DES, AES, AES128, or AES192).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the JVM does not support AES192 and AES256, these protocols are not displayed as available options. To support these protocols, you can update the security policy configuration from Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Privacy Password</strong> — The SNMP security privacy password.</td>
</tr>
</tbody>
</table>

- **Autostart SNMP** — The option to autostart the SNMP agent.

4. Click **Submit**.
   You can click **Cancel** to ignore the changes made.

5. Optionally, click **Stop SNMP Agent** to stop the SNMP agent.
   You can click **Start SNMP Agent** to start the SNMP agent.

---

**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 Setting Up Secure Communications on page 95 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 environment window Proenv

As a convenience, you can execute both OpenEdge Management and OpenEdge command-line utilities from the OpenEdge environment window. Access this window by choosing Start > Programs (or All Programs) > Progress > OpenEdge > Proenv. The environment window sets the shell environment variables needed for executing both OpenEdge Management and OpenEdge commands, as shown in the following figure.

Figure 10: Proenv 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>
```

The following table describes the options you can use when starting or stopping from the command line.
Table 6: Command-line options for starting and stopping

<table>
<thead>
<tr>
<th>Option syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-host</td>
<td>Host where the AdminServer process resides.</td>
</tr>
<tr>
<td>-port</td>
<td>Port where the AdminServer runs. Default is 20931.</td>
</tr>
<tr>
<td>-timeout &lt;time&gt;</td>
<td>Time, in seconds, for OpenEdge Management or OpenEdge Explorer to wait for a response. The default is 240 seconds.</td>
</tr>
<tr>
<td>-user &lt;user-name&gt;</td>
<td>Username on machine where the AdminServer resides. The default is current user.</td>
</tr>
<tr>
<td>-password &lt;user-password&gt;</td>
<td>Password associated with the specified username. This is not needed for local connection.</td>
</tr>
</tbody>
</table>

**Note:** Use of the -password parameter might allow others to see your password in clear text.

| -ssl                   | Connect to OpenEdge Management only if secure communication is enabled on the WebServer. If secure communication is not enabled on the WebServer, using this parameter results in an error message. |

Examples of starting, querying, and stopping from the command line

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:
**Dumping, backing up, and restoring the configuration database**

Using the command-line interface, you can dump either the OpenEdge Management or the OpenEdge Explorer configuration database files, even when it 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:

**Syntax**

```
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. Since Fathom is a plugin to the AdminServer, you cannot issue the fathom -dump command unless both the AdminServer and OpenEdge Management/OpenEdge Explorer are running, or they are both not running.

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

**Syntax**

```
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.

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.

OpenEdge Management or OpenEdge Explorer must be online when you run the -dump command.

To dump the data:

1. Select Start > Programs (or All Programs) > Progress > OpenEdge > Proenv.
2. Dump the fathom configuration database 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 configuration 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 the following figure appears.
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


3. Add the following to the jvmargs line:

   -DLogLevel=n

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

For details, see the following topics:

- Transferring data securely with the HTTPS protocol
- Understanding common secure communication-related terminology
- Getting started: using the demo certificate
- Changing Web server settings
- Changing OpenEdge Management Trend Database settings
- Using the procertm utility
- Using Secure Communication
- 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 TLS version 1.2 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 cryptographic 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 secure communication on a production system), you can generate your own certificate or use one that you acquire from a certificate authority.

Instructions for setting up secure communications by either method are provided here.

Understanding common secure communication-related 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 secure communication 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 select the HTTPS protocol for the Web server in the initial configuration (as described in Setting Up OpenEdge Management or OpenEdge Explorer for the First Time on page 37), you can make that choice later by updating the configuration options. You can change the port number and also decide whether to use HTTP only, HTTPS only, or both HTTP and HTTPS. If you select both the HTTP and HTTPS protocols, you can define a list of trusted clients for both protocols.

For example, you can restrict clients that attempt to access OpenEdge Management without cryptographic protocols. For HTTP, you might add the local host (or a subnet of HTTP local users) as a 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 and localhost must be defined as a trusted client.

To change the Web server settings:

1. From the management console menu bar, click *Options*.
   
The *Options* page appears.
2. Click *Web Server Configuration*.
   
The *OpenEdge Management Web Server Configuration* page appears and displays the current Web server settings.
3. Set the following protocol options:
   
   • Select the *Enable HTTP protocol* option to allow HTTP connections. Type the port number in the *HTTP port* field.
   
   • Select the *Enable HTTPS protocol* option to allow HTTPS connections. Type the port number in the *HTTPS port* field.
   
   • Select both the options to allow both HTTP and HTTPS connections. Type the port numbers in the *HTTP port* field and the *HTTPS port* field.
4. Set the login session timeout value in the *Timeout for logins* list. The default value is 30 minutes.

**Note:** You must logout and log on again for the session timeout value to take effect.

You can also set the login session timeout value in the fathom.properties file by setting the websessiontimeout property with a positive value in seconds. This file is available in the $DLC/properties folder. The entered value is added to the *Timeout for logins* list.

For example, if you set the websessiontimeout property value as 30, the session timeout value is set to 30 seconds and the value is added to the *Timeout for logins* list. If you set the property value as 0, session timeout is disabled.
Note: Only users with the Administrator role can set the login session timeout value. Users with the operator role can only view this value.

5. Set one of the following options:

- If you want to work with the demo keystore, click Submit. See Using Secure Communication on page 106 for details about using an HTTPS connection.
- If you are an advanced user and you want to change keystore information, see Using advanced HTTP and HTTPS options with the Web server on page 100.

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 OpenEdge Management Web Server Configuration page, click Advanced Options.
   The expanded OpenEdge Management 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 specify trusted clients by host IP address, IP address range with the * wildcard (such as 123.123.123.*), or subnet in the CIDR notation (such as 123.123.123.0/16).
   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 secure communication. 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 cryptographic protocols.

• **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.

To set the cryptographic protocol and cipher for a WebServer, you must set the following properties in the `fathom.properties` file that is available at `$DLC/properties`:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| sslEnable                 | **Default value:** 0  
Enables you to change the cryptographic protocols and ciphers for secure communication with a WebServer. If you enable SSL for the WebServer in OpenEdge Management and OpenEdge Explorer, this property is set to true. |
| SSLEnabledProtocols       | **Default value:** TLSv1.2  
**Supported values:** SSLv3, TLSv1, and TLSv1.1  
If you want to change the default cryptographic protocol for the WebServer, enter this property in the `fathom.properties` file. The property accepts a comma-separated list of valid cryptographic protocols that are set for secure communication. |
| SSLEnabledCipherSuites    | If you want to change the default cryptographic ciphers for the WebServer, enter this property in the `fathom.properties` file. The property accepts a comma-separated list of valid cryptographic ciphers that are set for secure communication. |
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, remote Web server port, user name, and password of the remote OpenEdge Management Web server. The user credentials with the Trending role must be created on the remote OpenEdge Management Web server. See Adding a new user on page 70 for more information. (These initial configuration steps are described in Setting Up OpenEdge Management or OpenEdge Explorer for the First Time on page 37.

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:
  a) From the management console menu bar, click Options. The Options page appears.
  b) Select Trend Database. The OpenEdge Management Trend Database Configuration page appears and displays the current trend database settings.
  c) Select Store trend data in a local OpenEdge Management database.
  d) Type the database path name (for example, C:\Progress\oemgmt\db\Fathom.db). (Note that the inclusion of the .db extension is optional when you provide the path name.)
  e) Type the database port number (for example, 1234).
  f) Enter the user name and password in the Local database user and Local database password fields, respectively.
  g) Click Submit.

- To store trend data in a remote OpenEdge Management instance:
  a) From the management console menu bar, click Options. The Options page appears.
  b) Select Trend Database. The OpenEdge Management Trend Database Configuration page appears and displays the current trend database settings.
  c) Select Store trend data in a remote OpenEdge Management instance.
  d) Type the host name in the OpenEdge Management host name field.
  e) 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.
  f) Enter the user name and password in the OpenEdge Management user and OpenEdge Management password fields, respectively.
  g) Select the Use HTTP protocol? option to use secure communication protocols to connect to the remote OpenEdge Management system.
  h) To use HTTPS, select the Use HTTPS protocol option.
  i) Set one of the following options:
• If you want to work with the demo keystore and are not using a proxy server, click **Submit**. See *Using Secure Communication* on page 106 for details about using an HTTPS connection.

• If you are an advanced user and you want to change keystore information or to use a proxy server, see *Using advanced HTTPS options when trending remotely* on page 103.

## 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. Type the keystore name in the **Keystore path name** field to use a keystore other than the demo keystore.

3. Set the **Enabled protocols** options to change the default cryptographic protocols. By default, remote trending databases support TLSv1, TLSv1.1, and TLSv1.2.

4. Enter comma-separated cipher suite values in the **Enabled cipher suites** field to manually set cipher suites. By default, OpenEdge Management and OpenEdge Explorer supports all the cipher suites that are provided by the SSL implementation of the Java Secure Socket Extension (JSSE).

5. If you want to use a proxy server, do the following:
   a) Select the **Use a Proxy server** option.
   b) Type the host name in the **Proxy host name** field.
   c) Type the server port number in the **Proxy server port** field.

6. Click **Submit**. A message appears confirming that the configuration has been successfully updated.

7. Click **OK**.

**Note:** The changes that 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 secure communication 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.

When the remote management console’s issuing Certificate Authority is not already present, you must do the following:

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**

```bash
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 Secure Communication

Once you configure the Web server to use secure communication, 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:

```plaintext
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 secure communications.

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, the message shown in the following figure appears.

Figure 12: 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 the following figure.
Figure 13: Certificate details

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

Installing certificate in Internet Explorer

To install the certificate:

1. Click Install Certificate. The Certification 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 Using the keytool utility on page 110 for details.

• Use an existing certificate that you have already acquired from a third-party CA. To use the existing certificate, follow Step 3: Importing the CA Certificate on page 113 and Step 4: Importing the signed certificate to the store on page 114.

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 <Full-path-to-OpenEdgeManagement/OpenEdge Explorer-install-dir>/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 the following table.

**Table 7: Distinguished name string components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>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.)</td>
</tr>
<tr>
<td>OU</td>
<td>The name of your organization or department.</td>
</tr>
<tr>
<td>O</td>
<td>The name of your company.</td>
</tr>
<tr>
<td>L</td>
<td>The name of your city.</td>
</tr>
<tr>
<td>S</td>
<td>The name of your state.</td>
</tr>
<tr>
<td>C</td>
<td>The name of your country.</td>
</tr>
</tbody>
</table>

-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 earlier in this section, **myIdentityKeystore.jks** is the repository name. If the keystore file were located in the default location for OpenEdge Management, for example, it would be in the **Progress\oemgmt\config** directory.

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

A sample of creating a keystore appears in the following figure.

**Figure 14: Creating a keystore**

This sample command 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 Progress\oemgmt\config directory, which is the default location for an installation of OpenEdge Management.
- 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 Step 1: Creating a keystore repository on page 110) 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 56
Adding a new user 70
Admin password
    entering 42
    updating 42, 72
Administrator users 70
AdminServer
    remote 23, 60
    viewing the contents of 54
Alerts
    option in the OpenEdge Management menu bar 54
AutoStart option 43

B
Browser support 31

C
Command-line interface
    and setting environment 90
    help 93
    using to start and stop 90
Configuration process
    establishing values
        on the Getting Started page 46
        on the OpenEdge Explorer Configuration page 42
        on the OpenEdge Management Configuration page 42
    initial configuration options 39, 41
    specifying and initially changing the admin password 42
Configuring
    OpenEdge Explorer 39
    OpenEdge Explorer for remote property configuration 59, 64, 75
    OpenEdge Management
        completing 40
        for remote monitoring and property configuration 59
    OpenEdge Management or OpenEdge Explorer
        before you begin 38
        initial options for 41
CPU requirements 29

D
Dashboard page 52
Database Migration Utility
    adding a managed database page by using 47
Databases
    managed 46
    scripted 46
Deleting users 72
Deploying OpenEdge Management
    on a single host 21
    on multiple hosts 21
    strategy for 28
Detail control bar 52
Detail menu 52
Disabled status 55
Disabling
    OpenEdge Management or OpenEdge Explorer 61, 63

E
E-mail server 44

F
Fail status 55

G
Getting Started page
    defining options for file systems and disks 48
    managed and unmanaged databases 46

H
Help
    command line 93
    option in the OpenEdge Explorer menu bar 55
    option in the OpenEdge Management menu bar 54
HTTPS protocol
    using with OpenEdge Management 95, 114

I
Inactive status 55
Installation
    OpenEdge product support for 31
    trending databases 38
OpenEdge Management (continued)
  getting started 34
    overview 18
OpenEdge Management Configuration page
  accessing during the configuration process 41
  admin password 42
  AutoStart option 43
  submitting 45
OpenEdge Management Trend Database
  optionally configuring 31
Operator users
  Customizing operator role 73
  Managing access to DAC 74
Options
  in the OpenEdge Explorer menu bar 55
  in the OpenEdge Management menu bar 54–55
Pass status 55
Password
  when logging on 41
Proenv window 90
Reglue
  running 63
Remote AdminServer
  setting up 64
Remote configuration
  setting up 64
Remote monitoring
  and configuration 59
  configuring 59
  setup verification 64
Reports
  option in the OpenEdge Management menu bar 54
Requirements
  CPU and memory 29
Resource statuses 55
Resources
  option in the OpenEdge Explorer menu bar 55
  option in the OpenEdge Management menu bar 54
Resources to monitor 38
Scripted databases
  monitoring 26–27
SMTP_MAIL network resource monitor 44
Startup options
  default alert operator 44
  e-mail server 44
Status indicators 55
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
</tr>
<tr>
<td>architecture</td>
</tr>
<tr>
<td>agents 20</td>
</tr>
<tr>
<td>console 20</td>
</tr>
<tr>
<td>database 20</td>
</tr>
<tr>
<td>performance 38</td>
</tr>
<tr>
<td>requirements 31</td>
</tr>
<tr>
<td>System Activity report 54</td>
</tr>
<tr>
<td>System information report 54</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>T</td>
</tr>
<tr>
<td>Trending databases 38</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>U</td>
</tr>
<tr>
<td>Unglue</td>
</tr>
<tr>
<td>running 61, 63</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>W</td>
</tr>
<tr>
<td>Web server port</td>
</tr>
<tr>
<td>identifying in the command-line interface 90</td>
</tr>
</tbody>
</table>

User information
   adding 70
   changing password 72
   changing the admin password 72
   deleting 72
   establishing 70
   maintaining 70

User name
   when logging on 41

Users
   adding 70
   administrators 70
   deleting 72
   operators 70