Progress®



# Introduction to OpenEdge Management

OpenEdge®

# Copyright

**© 2021 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.**

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

DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Icenium, Inspec, Ipswitch, iMacros, Kendo UI, Kinvey, MessageWay, MOVEit, NativeChat, NativeScript, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), SpeedScript, Stylus Studio, Stylized Design (Arrow/3D Box logo), Styleized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Habitat, Chef WorkStation, Corticon.js, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Everywhere, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, JustAssembly, JustDecompile, JustMock, KendoReact, NativeScript Sidekick, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Insight, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

**July 2021**

**Product version:** Progress OpenEdge 12.4

**Updated: 2021/06/29**

# Table of Contents

**Preface....9**

**Introduction to OpenEdge Management....11**

More about the Management Console....13
Access the Management Console....13
System requirements....14
Browser support....14
Accessing OpenEdge Management documentation....14
Understand OpenEdge Management architecture and deployment....16
OpenEdge Management system architecture....16
OpenEdge Management deployment....16
Configure or monitor resources on a remote AdminServer....19
Configuring remote resources with OpenEdge Explorer....20
Configure and monitor remote resources with OpenEdge Management....20
Resources that support remote monitoring....20
More about monitoring scripted and managed databases....23
Choose an OpenEdge Management deployment strategy....24
OpenEdge Management CPU and memory requirements....25
CPU use....25
Memory use....26
Optionally configuring the OpenEdge Management Trend Database....27
Get started with OpenEdge Management tasks....28

**Set Up OpenEdge Management for the First Time....31**

Prepare to set up OpenEdge Management....31
Use the management console ....33
Use the Database Administration Console....33
Complete the initial setup process ....33
Setting up OpenEdge Explorer....33
Set up OpenEdge Management....33
Start OpenEdge Management....34
Enter the default user name and password....34
Choose initial configuration options....35
Setting initial configurations for OpenEdge Explorer....35
Set initial configurations for OpenEdge Management....35
Set up the Getting Started page for OpenEdge Management....38
Understand managed and scripted databases ....38
Define OpenEdge Management monitors for previously scripted databases....38
Add a managed database ....39

Make changes to a managed database configuration ....40
Define OpenEdge Management monitoring and trending options for file systems and disks....40
Submit the Getting Started page for OpenEdge Management....41

**Use the Resources Tab....43**

Customize the Resources view....44
Check resource status and alert severity....44
View the contents of a AdminServer....45

**Set up Remote Resource Monitoring and Configuration....47**

Remote monitoring and configuration requirements....47
Prepare to enable remote monitoring and configuration....48
Unglue OpenEdge Management from OpenEdge....50
Reglue OpenEdge Management to OpenEdge....51
Set up for remote monitoring or configuration....51
Set up a remote AdminServer....52
Verifying that OpenEdge Management can see the remote AdminServer....52
Disabling remote monitoring of a remote AdminServer....52

**Administer OpenEdge Management....53**

Update configuration options....54
Add users as administrators or operators....55
Manage the authorized users list....56
Add a new user....56
Change passwords and descriptions....57
Change the administrator password ....58
Delete users....58
Customize the operator role....58
Manage access to the Database Administration Console....59
Configure user authentication....61
OpenEdge Authentication Gateway authentication....61
Configure user authentication for web server logins....63
Set OpenEdge Management user preferences....65
Set up a remote AdminServer....66
View a remote AdminServer....67
Edit a remote AdminServer....67
Delete a remote AdminServer....67
Set up secure communication-related security for a remote AdminServer....68
Change general configuration settings....70
Change OpenEdge Management Trend Database settings....71
Change OpenEdge Management e-mail alerts settings....72
Change OpenEdge Management resource monitoring settings....72
Set the OpenEdge Management graph cache....73

Configure process pooling....74
Process pooling modes....74
Set process pooling options....75
Create a new process pooling configuration....76
Delete a custom process pooling configuration....76
Set OpenEdge Management resource monitor defaults....76
Set OpenEdge Management distribute resource properties....77
Change the OpenEdge Management SNMP Adapter settings....78
Use the command-line interface....80
Set the log level for the AdminServer log file ....81
Configure OpenEdge Management log files....81

**Set Up Secure Communications....83**

Transfer data securely with the HTTPS protocol....83
Use the demo certificate or your own certificate....84
About common secure communication-related terminology....84
Get started: using the demo certificate....85
Configuration update errors or warnings....85
Identify trusted clients....85
Reconnect after updates....86
Change web server settings....86
Use advanced HTTP and HTTPS options with the web server....87
Use secure communication....89
Detect a certificate from an unknown Certificate Authority....89
When browsing in Internet Explorer....90
Use your own certificate....92
Use the keytool utility....92
Step 1: Create a keystore....93
Step 2: Generate a Certificate Signing Request....95
Step 3: Import the CA Certificate....96
Step 4: Import the signed certificate to the keystore....96

**Fathom Command-line References....99**

Use Proenv....100
Access help (help)....100
Start OpenEdge Management (start)....101
Stop OpenEdge Management (stop)....101
Check status (query)....102
Restart OpenEdge Management (restart)....102
Display configuration information (configinfo)....103
Clear an alert (clear)....103
Enable a resource (enable)....105
Disable a resource (disable)....106

List alerts (alertlist).....107
Additional options.....108
Fire an alert (firealert).....112
Dump configuration database (dump).....113
Load configuration database (load).....114
List resources (reslist).....114
Initialize new database (initcachedb).....115

**Index.....117**

# Preface

## Purpose

This manual describes how to get started using OpenEdge Management.

## Audience

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

## Organization

Introduction to OpenEdge Management on page 11

Provides an introduction to working with OpenEdge Management. Included are details about OpenEdge Management architecture, deployment options, and remote monitoring.

Set Up OpenEdge Management for the First Time on page 31

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

Use the Resources Tab on page 43

Describes the management console. Also describes the Database Administration Console, which you use to work with databases enabled for multi-tenancy.

Set up Remote Resource Monitoring and Configuration on page 47

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

Administer OpenEdge Management on page 53

Provides information about administering OpenEdge Management 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.

Set Up Secure Communications on page 83

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 OpenEdge Management to use the HTTPS protocol with the Web server. The topic explains the process of creating a keystore; requesting, obtaining, and then importing a signed certificate; and then adding the signed certificate to the keystore.

## Documentation conventions

See Documentation Conventions for an explanation of the terminology, format, and typographical conventions used throughout the OpenEdge content library.

# 1

# Introduction to OpenEdge Management

OpenEdge Management provides visibility into a broad range of configuration, performance and status information on resources. It offers a variety of capabilities to the administrator or user to manage and monitor the performance of OpenEdge resources to:

- Proactively detect, prevent and troubleshoot failures to improve reliability
- Collect and store necessary data for reports and future reference
- Display resource information and data for the benefit of the system administrator

From the **Management Console**, you can perform the following tasks to achieve these benefits by:

- Creating and deleting new instances of licensed resources
- Setting or modifying properties for these instances
- Starting or stopping the instances (where applicable)
- Viewing status of the instances
- Configuring and viewing log files of the instances
- Defining and running Jobs
- Defining and running Reports
- Working with database administration console

When you access the **Management Console**, the **OpenEdge Management** view appears depending on the availability or non-availability of the OpenEdge Management license.

## Access to OpenEdge Management

The OpenEdge Management is accessible only with a valid OpenEdge Management license. OpenEdge Management offers the following management and monitoring capabilities:

| Menu tab | Description |
|---|---|
| **Dashboard** | The Dashboard provides a single unified view of the configured priority OpenEdge resources, system and network information for viewing. The dashboard is a collection of various resources related metrics which may include statuses, performance graphs, jobs, alert details and so on.<br>See The Dashboard page in *Monitor OpenEdge Resources with OpenEdge Management*. |
| **Alerts** | Alerts aid in the management and monitoring of the resources. An alert notifies a user when a defined performance metric or event meets the configured threshold so that timely action can be taken. Alerts are associated with rules and configured to send e-mail notifications to IT personnel and execute scripts.<br>See Working with Alerts in *Use OpenEdge Management Alerts*. |
| **Library** | A pool of all actions, rule sets, email templates, search criteria, and schedules that you can create and associate with the various resources for monitoring.<br>See Using the OpenEdge Management Library in *Monitor OpenEdge Resources with OpenEdge Management*. |
| **Reports** | Reports help you to study and compare the performance of the resources for capacity planning and make other suitable business decisions. A user can create reports and report templates; define the report schedule for each type of report, view, print and save reports.<br>See Working with Report Instances *Use OpenEdge Management Reporting*. |
| **Jobs** | A job is a task or set of tasks that you can create and schedule for execution to aid in the management and monitoring of the OpenEdge resources.<br>See Working with Jobs in *Monitor OpenEdge Resources with OpenEdge Management*. |

### Quick access options

**Toggle Menu:** Located on the top-left of the **Management Console**, the toggle menu provides you quick access to view the details of resources such as all collections, name of the resource, type and status of the resource and the AdminServer details.

**User Options**: Located on the top-right of the Management Console, the **User Options** provides quick access to the configuration settings of the OpenEdge Management such as setting up a page as the default landing page, changing Web server configuration, adding and managing remote AdminServers.

For details, see the following topics:

- More about the Management Console
- Understand OpenEdge Management architecture and deployment
- Configure or monitor resources on a remote AdminServer
- Choose an OpenEdge Management deployment strategy
- OpenEdge Management CPU and memory requirements
- Optionally configuring the OpenEdge Management Trend Database
- Get started with OpenEdge Management tasks

# More about the Management Console

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 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 does 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.

## Access the Management Console

Depending on whether you are accessing OpenEdge Management from a web browser or locally, choose either of the following methods:

- To access OpenEdge Management 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 is installed, and the port is the web server port (by default, this port is 9090). A logon form appears.
- To access OpenEdge Management locally from the Windows Desktop, and OpenEdge Management is installed, choose **Start** > **Programs (or All Programs)** > **Progress** > **OpenEdge** > **Management Console**.

  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** page appears when the console opens.

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

You can access the **Mangement Console** from any browser that OpenEdge Management supports. (See Browser support on page 14 for specifics about which browsers are supported).

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

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 application server instance, for monitoring or configuration in the console.

In OpenEdge Management, 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.

# System requirements

Most of the system requirements for OpenEdge Management are the same as those for OpenEdge. For more information, see the *OpenEdge Platform and Product Availability Guide* on the Progress Information Hub at https://docs.progress.com.

# Browser support

A Web browser is required to run the OpenEdge Management or OpenEdge Explorer graphical user interface known as the management console. To see a list of supported browsers please see the Product Availability Guide.

**Note:** When HTTPS is enabled, HTTPS connections to OpenEdge Management supports only TLS1.2. Older versions of TLS and SSL are not supported.

# Accessing OpenEdge Management documentation

OpenEdge Management 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 guides.

  If no context-sensitive help exists for a particular page, the *Introduction to OpenEdge Management* 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 PDF and HTML format from Progress Communities:

```
https://community.progress.com/technicalusers/w/openedgegeneral/
1329.openedge-product-documentation-overview.aspx
```

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:

```
http://www.adobe.com/products/acrobat/readstep2.html
```

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

- *Configure OpenEdge Components with OpenEdge Management*

  Describes how to establish property and configuration settings for OpenEdge databases, DataServers (for Oracle, and MS SQL Server), NameServers, and application servers in OpenEdge Management. In addition, this manual also includes details about viewing status and log files.

- *Monitor OpenEdge Resources with OpenEdge Management*

  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.

- *Manage the OpenEdge Database with OpenEdge Management*

  Describes how to use OpenEdge Management to monitor and manage OpenEdge database resources.

- *Use OpenEdge Management Alerts*

  Presents alert concepts and procedures and provides a comprehensive reference section to assist you in working with the OpenEdge Management alerts feature.

- *Manage Servers, Data Servers, Messengers, and Adapters with OpenEdge Management*

  Describes how OpenEdge Management supports monitoring and managing specific resources associated with the OpenEdge server products, and DataServers (Oracle, and MS SQL Server).

- *Use OpenEdge Management Reporting*

  Provides detailed information about creating and working with report instances and templates.

- *Use the OpenEdge Trend Database*

  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.

- *Configure Database Multi-tenancy with OpenEdge Management*

  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.

- *Get Started with Database Multi-tenancy in OpenEdge Management*

  Describes how to get started using multi-tenancy in the Database Administration Console.

- *Manage Database Change Data Capture with OpenEdge Management*

  Describes how you can use the Database Administration Console in OpenEdge Management to manage Change Data Capture in databases.

# Understand 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 topics:


- OpenEdge Management system architecture on page 16
- OpenEdge Management deployment on page 16


## 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, table partitioning, and Change Data Capture.
- A database called the OpenEdge Management Trend Database that stores all data collected by agents for use in reporting.
- The OpenEdge Management process, which runs as a standalone web application on Progress Application Server (PAS). The foundation for PAS is Apache Tomcat Web server that includes a Java servlet for hosting web applications. For more information about PAS, see *Learn about about Progress Application Server for OpenEdge*.
- The AdminServer, which is a background process that provides a common point of management for the resources managed by OpenEdge Management.
- The Orient DB database, which stores monitoring plans and resource definitions.

## OpenEdge Management deployment

You can deploy OpenEdge Management by installing it on:

- A single host
- Multiple hosts

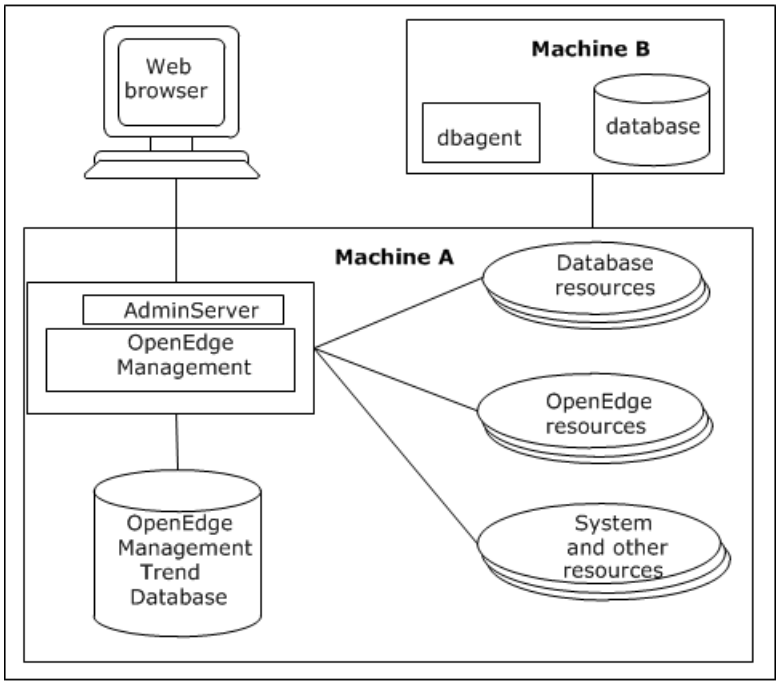
## Deploy OpenEdge Management on a single host

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. 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**



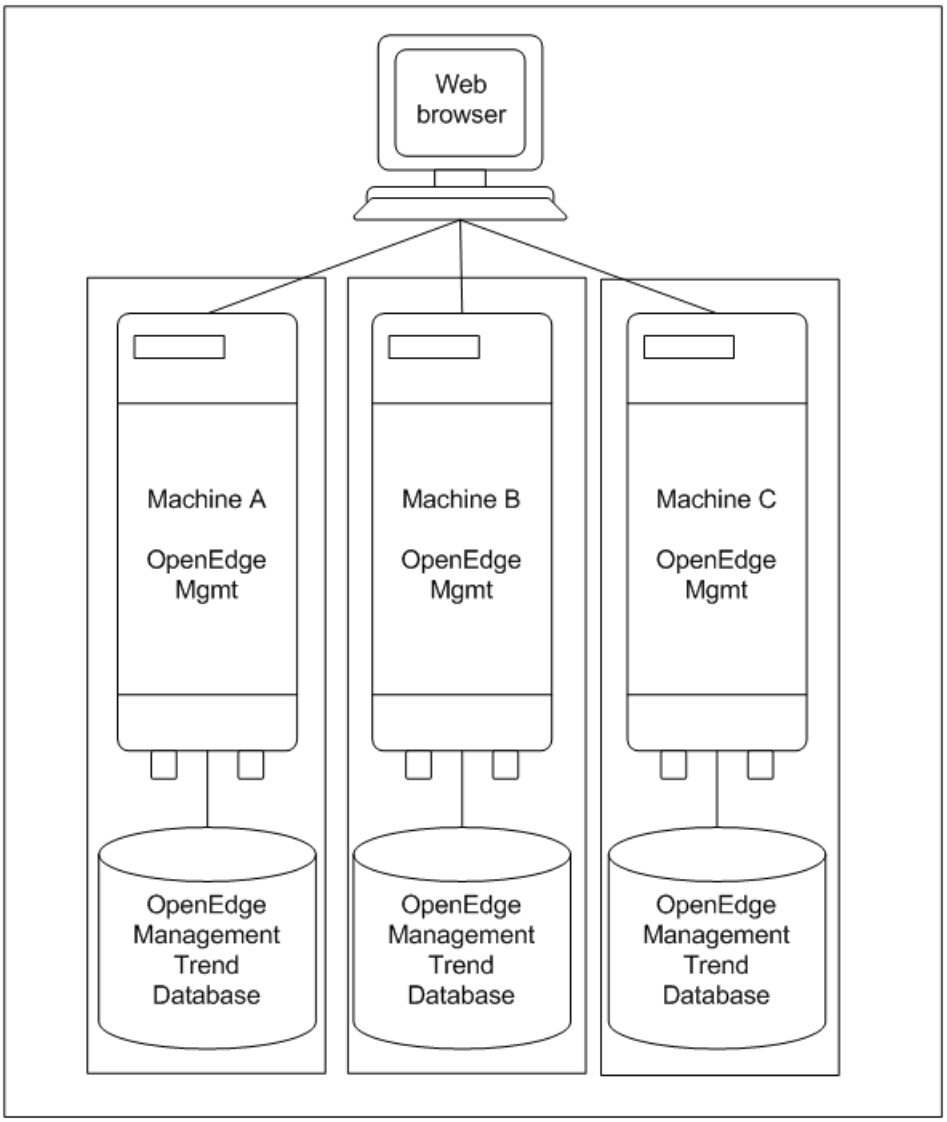

OpenEdge Management and AdminServer are running on Machine A. The OpenEdge Management Trend Database and all monitored resources are also on Machine A.

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

## Deploy 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.

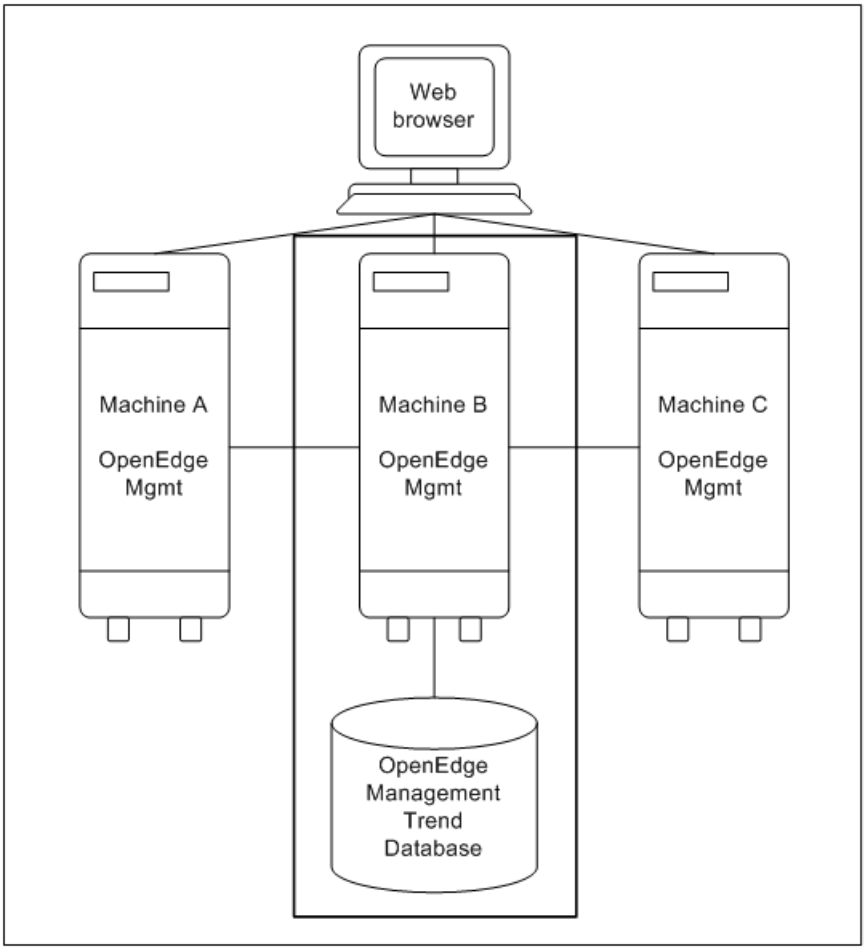
**Figure 2: Multiple-host OpenEdge Management installation**




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.

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




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 #iek1561029235253/i631365 and #iek1561029235253/i631478, 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.

# Configure or monitor resources on a remote AdminServer

If you have OpenEdge Management installed, you can monitor and configure resources running on a remote AdminServer.

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. A *remote AdminServer* is an AdminServer that you set up to be configured or monitored remotely by OpenEdge Management

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

For details about setting up remote AdminServers, see Set up Remote Resource Monitoring and Configuration on page 47

## 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 Set up for remote monitoring or configuration on page 51.

## Configure and monitor remote resources with OpenEdge Management

With OpenEdge Management, you can configure and 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 on the remote resource's host machine.

See Set up for remote monitoring or configuration on page 51 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.

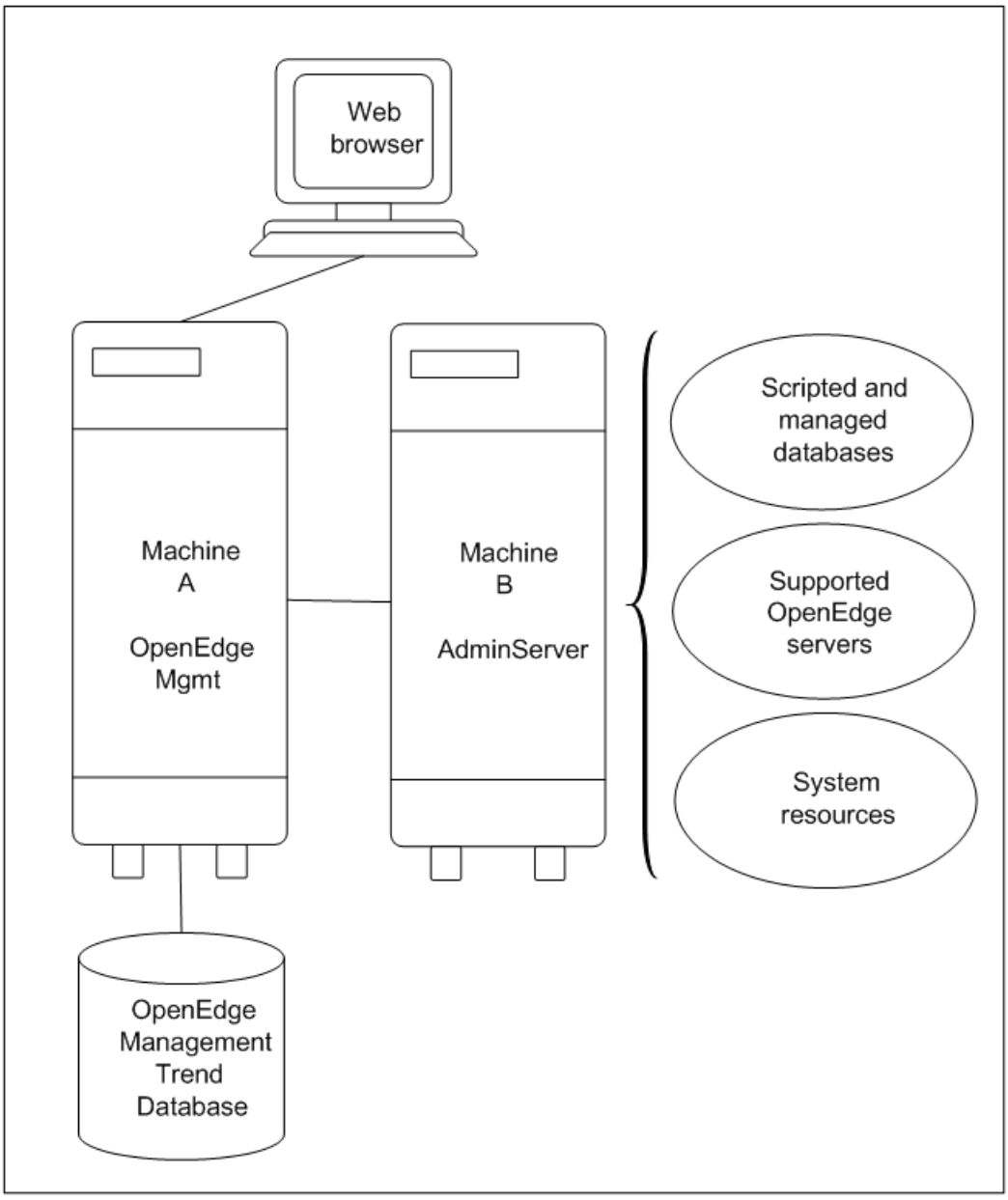
## Resources that support remote monitoring

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

- **Databases**
- **OpenEdge servers**
- **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**

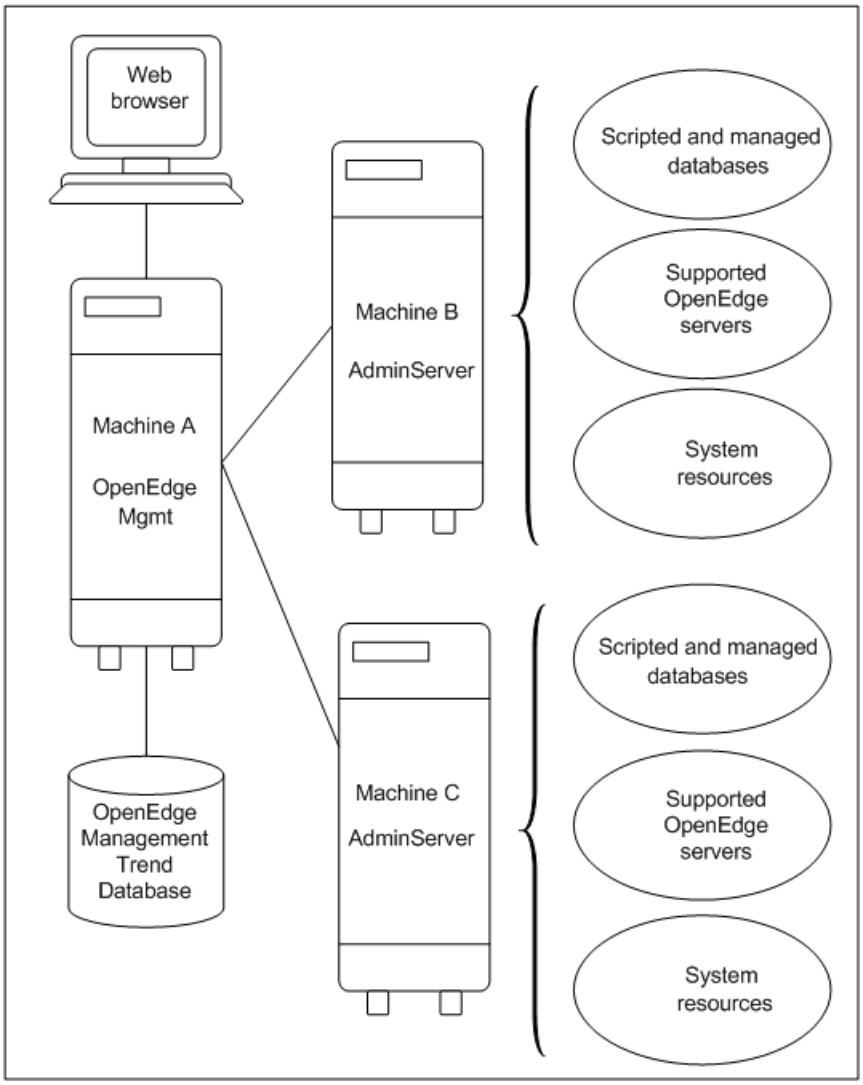



The illustration shown in Figure 4: Remote monitoring of resources on one machine on page 21 presents a single installation of OpenEdge Management on Machine A, which is monitoring the following resources on Machine B:

- **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 instance.
- **System resources**—System resources are CPU, disk, memory, and file system.

You can extend the deployment model shown in Figure 4: Remote monitoring of resources on one machine on page 21 to multiple hosts, as shown in Figure 5: Monitoring of resources on two machines on page 22.

**Figure 5: Monitoring of resources on two machines**




The illustration shown in Figure 5: Monitoring of resources on two machines on page 22 presents a single installation 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 installation 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.

## Monitor 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 Set up Remote Resource Monitoring and Configuration on page 47.

## Monitor a managed database through a remote-enabled AdminServer

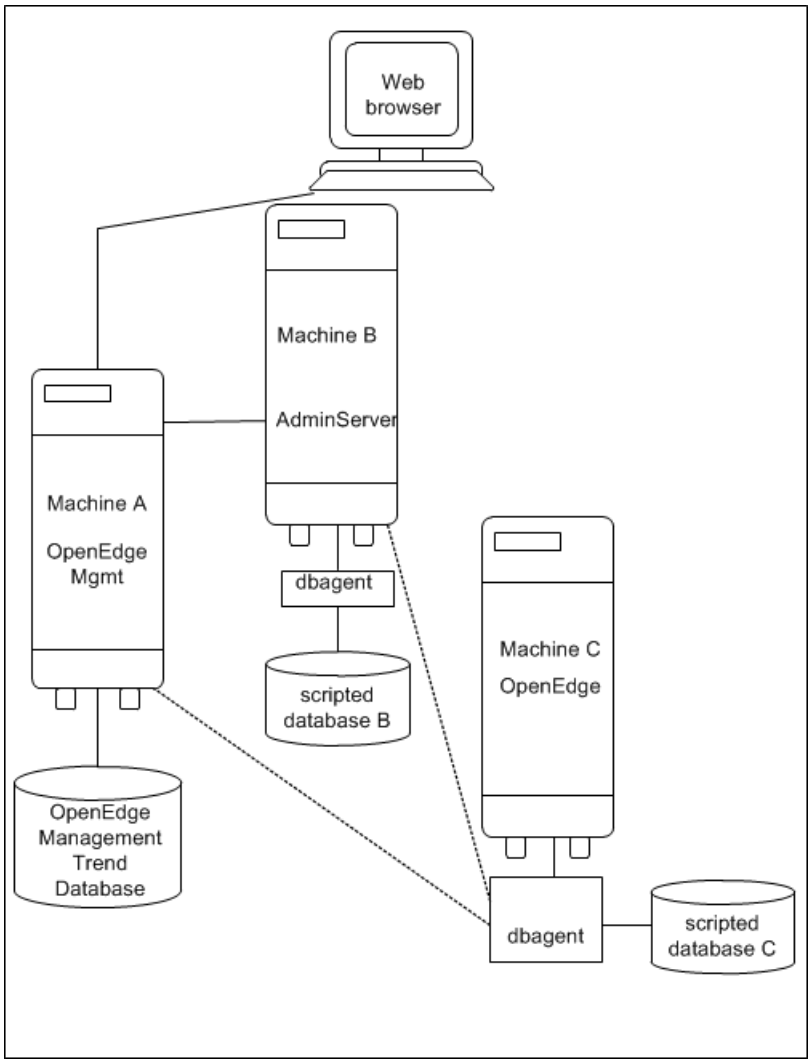
OpenEdge Management can monitor a managed database that has been autodiscovered running under a remote-enabled AdminServer.

## Monitor 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.

**Figure 6: Monitoring scripted databases on another machine**




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

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

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

# Choose 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:

- Do you want to minimize the impact of OpenEdge Management on your production machines? If so, you should consider installing OpenEdge Management on a machine dedicated to running OpenEdge Management and use OpenEdge Management remote resource monitoring capabilities.
- Do you want to view the status of all your resources from a single OpenEdge Management console? If so, you should consider using OpenEdge Management's remote resource monitoring capabilities.
- Do you need to run jobs on remote machines? OpenEdge Management provides support for remote jobs.
- Will you be monitoring resources outside of your network firewall? If so, you will need to perform the appropriate tunneling to allow OpenEdge Management through the firewall.

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

For more information about using OpenEdge Management with resources being managed by a remote AdminServer, see Set up Remote Resource Monitoring and Configuration on page 47

# 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 Set OpenEdge Management user preferences on page 65.

- **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 Set Up OpenEdge Management for the First Time on page 31), 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 Set Up OpenEdge Management for the First Time on page 31. 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 *Manage the OpenEdge Database*.

# Get 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**

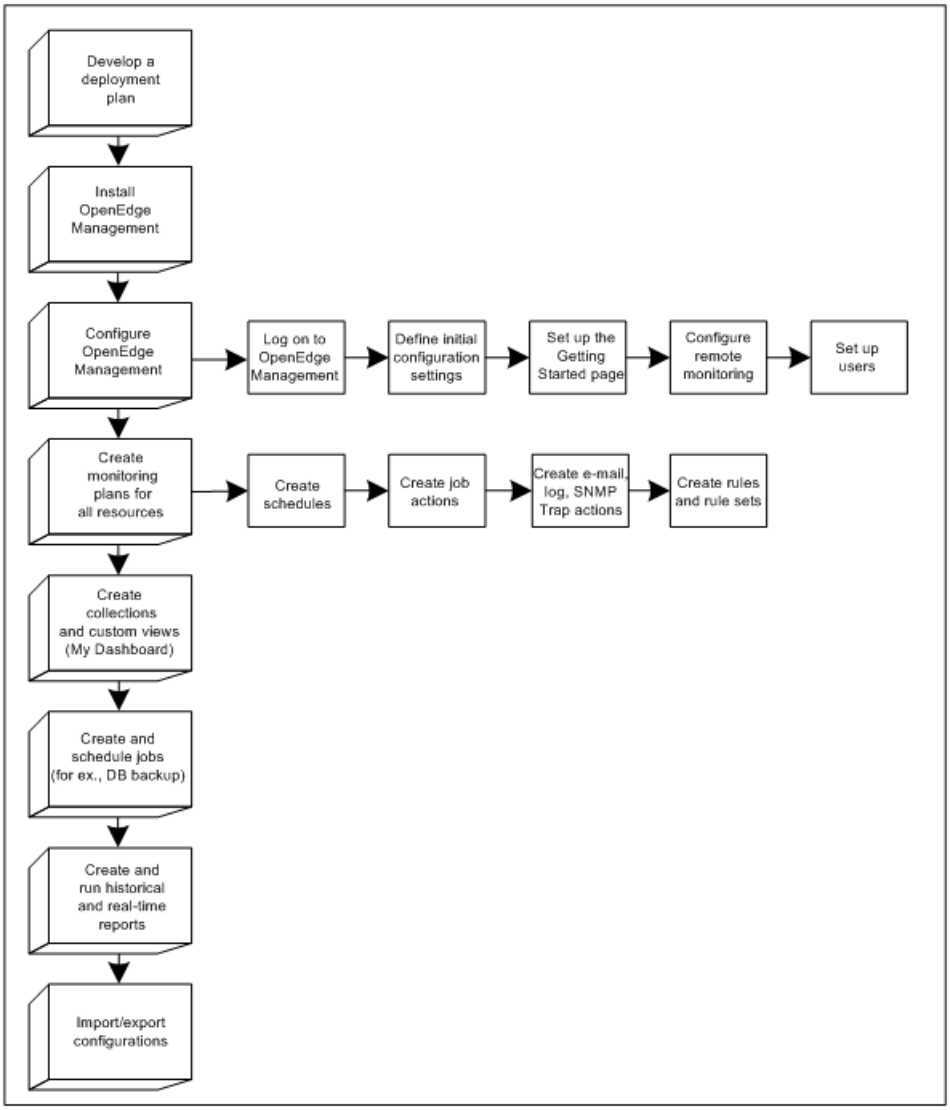



**Table 1: Documentation for major OpenEdge Management tasks (1 of 2)**

| For information on this task . . . | See . . . |
|---|---|
| Developing a deployment plan before you install OpenEdge Management | This guide |
| Setting up OpenEdge Management, which includes logging on and defining initial settings | This guide |

| For information on this task . . . | See . . . |
|---|---|
| Setting up OpenEdge Management for remote monitoring and configuration, and setting up users. | This guide |
| 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 | This guide |
| Using the HTTPS (TLS) protocol for communication between an OpenEdge Management web server and client | This guide |
| Creating new instances of resources, and setting or modifying their configuration properties | This guide |
| Creating monitoring plans for and managing system, network, file, and OpenEdge resources in OpenEdge Management | *Monitor OpenEdge Resources with OpenEdge Management* |
| Creating collections and custom views (**Dashboard**) in OpenEdge Management | *Monitor OpenEdge Resources with OpenEdge Management* |
| Creating and scheduling jobs in OpenEdge Management | *Monitor OpenEdge Resources with OpenEdge Management* |
| Importing and exporting configurations in OpenEdge Management | *Monitor OpenEdge Resources with OpenEdge Management* |
| Creating and running reports in OpenEdge Management | *Use OpenEdge Management Reporting* |
| Creating monitoring plans for and managing database resources in OpenEdge Management | *Manage the OpenEdge Database* |
| Creating monitoring plans for and managing OpenEdge server, DataServer, Messenger, and Adapter resources | *Manage Servers, Data Servers, Messengers, and Adapters with OpenEdge Management* |
| Understanding and working with OpenEdge Management alerts | *Use OpenEdge Management Alerts* |
| Managing your OpenEdge Management Trend Database by compacting and purging data, and understanding the trend database schema | *Use the OpenEdge Trend Database* |
| Managing and working with databases enabled for multi-tenancy | *Configure Database Multi-tenancy with OpenEdge Management* |
| Getting started with multi-tenancy in the Database Administration Console | *Get Started with Database Multi-tenancy in OpenEdge Management* |
| Creating and managing Change Data Capture policies using the Database Administration Console. | *Manage Database Change Data Capture with OpenEdge Management* |

# 2

# Set Up OpenEdge Management for the First Time

The following topics introduce the components of OpenEdge Management and describes how to set up each one.

For details, see the following topics:

- Prepare to set up OpenEdge Management
- Complete the initial setup process
- Start OpenEdge Management
- Choose initial configuration options
- Set up the Getting Started page for OpenEdge Management
- Understand managed and scripted databases
- Define OpenEdge Management monitors for previously scripted databases
- Define OpenEdge Management monitoring and trending options for file systems and disks
- Submit the Getting Started page for OpenEdge Management

## Prepare to set up OpenEdge Management

Consider the following factors before you set up OpenEdge Management 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.
- 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, and the application server. During configuration, you can choose whether to save monitoring information locally 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.

- 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 25 for more information.

- Your resources can be administered by OpenEdge Management and command-line utilities, such as dbman or asbman. Therefore, you should be familiar with the AdminServer functionality.

  You can access online help while working in the management console. For details about the dbman or asbman utility, see *Manage the OpenEdge Database*.

- Start the AdminServer to access your resources. You can start or stop the AdminServer using the following commands:

```
proadsv -start

proadsv -stop
```

  In Windows, AdminServer is registered as a Windows service. You can start or stop the **Progress OpenEdge AdminServer Service** service from the Windows Services utility.

- Start the OpenEdge Management. You can start and stop using the following commands:

```
fathom -start

fathom -stop
```

  In Windows, OpenEdge Management is registered as a Windows service. You can start or stop the **Progress OpenEdge Management Service for OpenEdge** service from the Windows Services utility.

  To access OpenEdge Management from a browser, select **Start** > **Programs (or All Programs)** > **Progress** > **OpenEdge** > **Management Console**.

  The initial user name and password are admin/admin.

  For details about using command-line options with OpenEdge Management, see Use the command-line interface on page 80.

## Use 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 More about the Management Console on page 13, which covers the console's features and functionality in detail.

## Use the Database Administration Console

OpenEdge Management includess 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**.

# Complete the initial setup process

The first time you start 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**.
- Click **Start using OpenEdge Explorer** in the **Initial Configuration Completed** page that appears.

## Set 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 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**.
- 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.

# Start OpenEdge Management

Choose one of the following to start OpenEdge Management:

- Execute the `fathom -start` command in the OpenEdge environment window `proenv`. For more information about command-line references, see Fathom Command-line References on page 99.
- In Windows, OpenEdge Management is registered as a Windows service at the time of installation and the **OpenEdge Management Service for OpenEdge** service is started automatically. If not started, however, you can start this service from the Windows Services utility.

---

**Note:** Note that OpenEdge Management is hosted on Progress Application Server and is not part of AdminServer, as in previous releases. Consequently, starting the AdminServer is not required to start OpenEdge Management.

---

To access OpenEdge Management from a web browser:

1. Ensure that the OpenEdge Management is started.
2. To access OpenEdge Management 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 is installed, and the port is the web server port (by default, the HTTP port is 9090 and the HTTPS port is 9443).

3. To access OpenEdge Management locally from the Windows Desktop, choose **Start** > **Programs (or All Programs)** > **Progress** > **OpenEdge** > **Management Console**.

The OpenEdge Management login window appears and you must enter your user name and password to login, as described in Enter the default user name and password on page 34.

# Enter the default user name and password

The first time you log on to OpenEdge Management, 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**.

   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.

   ---

   **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; namely, the first time you log on to OpenEdge Management. 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.

- The new password you provide on the configuration page does not take effect until you stop and restart OpenEdge Management. You do this by either shutting down and restarting the host machine or using the appropriate command-line interface (CLI) commands. See Use the command-line interface on page 80 for more information.

You can now make initial configuration choices, as described in Choose initial configuration options on page 35.

# Choose initial configuration options

When you log on to OpenEdge Management 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 support the implementation of the HTTPS (TLS) protocol.

  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.

  See Set Up Secure Communications on page 83.

## 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 change the Admin password. See Specify the administrator password on page 35.

When you finish setting this option on the page, click **Submit**.

## Set 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:

- Specify the administrator password on page 35
- Specify the location of the OpenEdge Management Trend Database on page 36
- Specify the OpenEdge Management e-mail server and default operator on page 37

Each of these options is described in following sections.

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

### Specify the administrator password

OpenEdge Management is initialized 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 Add users as administrators or operators on page 55 for more information.

The new password you provide on the **Configuration** page does not take effect until you stop and restart OpenEdge Management, by either shutting down and restarting the host machine or using the appropriate command-line interface (CLI) commands. See Use the command-line interface on page 80 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, 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 specify a location and port for OpenEdge Management Trend database.

## Specify 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 a local OpenEdge Management Trend Database. These storage options appear in the **Trend database location** section.

To specify the location of the OpenEdge Management Trend Database:

1. In the **OpenEdge Management Configuration** page, go to the **Trend database location** section.
2. In the **Trend database location** field, specify the location for the trend database.

   You can either use the predefined explicit path where the trend database is located by default, or type a different path to the database. For example, `C:\Progress\oemgmt\work\fathomdb\fathom.db`. Note that the inclusion of the `.db` extension in the path name is optional.

   OpenEdge Management provides a backup of the default trend database `fathom.bak` in the `$OEMgmt\db` directory. If you specify a location other than the default trend database location, OpenEdge Management extracts that backup and places it in the location you specified.

   If you already have a trend database placed in the specified location, OpenEdge Management uses that trend database.

   Alternatively, you can either copy the OpenEdge Management trend database `fathom.db` to the specified location using the `procopy` or `prodb` command, or restore the trend database backup `fathom.bak` to the specified location using the `prorest` command.

3. In the **Trend database port** field, type the port number.

---

**Note:** If the local AdminServer is offline, the **Trend database location** and **Trend database port** fields are disabled.

---

You can also specify the location of the Trend Database later by selecting **Options** > **Trend Database** once the local AdminServer is online.

## Specify 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*.

## Submit the OpenEdge Management Configuration page

After 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 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 Management options, the **Getting Started** page automatically appears.

If all the initial configuration values cannot be validated, warning messages appear.

# Set 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 *Monitor OpenEdge Resources with OpenEdge Management* for more details.

# Understand 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 t 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.

# Define 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.

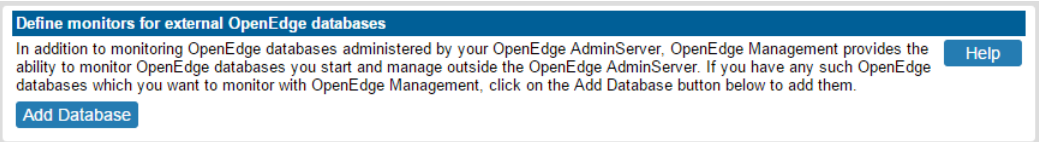
---

**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.

# Add 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.

## Make changes to a managed database configuration

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

**Note:** From within OpenEdge Management, you can use the **Control** page to start and stop a database configuration. For more information about working with database configurations, see *Configure OpenEdge Components with OpenEdge Management*.

# Define 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 databasesand 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.

# Submit 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.

# 3

# Use the Resources Tab

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.

For details, see the following topics:

- Customize the Resources view
- Check resource status and alert severity
- View the contents of a AdminServer

# Customize 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 Use the Resources Tab on page 43.

# Check resource status and alert severity

Once you set up resources, OpenEdge Management gives 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 and color combination represents.

**Table 2: Resource status legend**

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

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

# View 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

# 4

# Set up Remote Resource Monitoring and Configuration

You can monitor any resource remotely that you can monitor locally, if 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 topic describes how to set up OpenEdge Management for remote monitoring and configuration.

For information about setting up local and remote connections for databases enabled for multi-tenancy, see *Configure Database Multi-tenancy with OpenEdge Management*.

For details, see the following topics:

- Remote monitoring and configuration requirements
- Prepare to enable remote monitoring and configuration
- Set up for remote monitoring or configuration
- Set 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.

In this standalone installation, OpenEdge Management cannot be enabled. If it is enabled, you must disable it in the Progress or OpenEdge product by running the *unglue* script.

You can monitor multiple AdminServers (AdminServers 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. Therefore, it is important that the machines involved have their universal time setting coordinated. You can do this by making sure that the machines subscribe to an NTP time service.

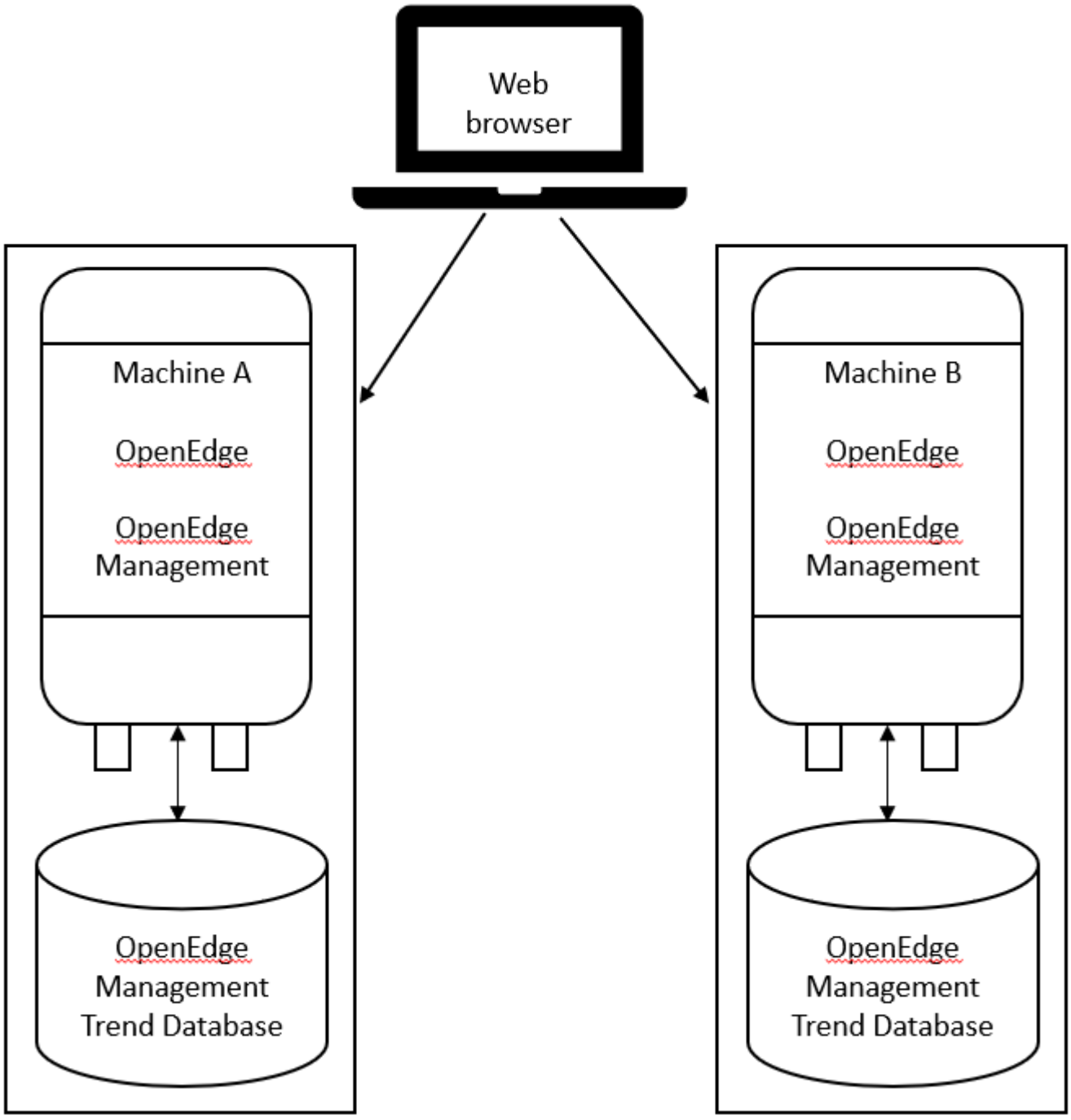
# Prepare to enable remote monitoring and configuration

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.

The remote AdminServer must have an AdminServer installed on it but must not have an enabled installation of OpenEdge Management. If OpenEdge Management is enabled, Progress recommends that you stop the openedge management service before you enable the machine as a remote AdminServer.

As shown in the scenario illustrated in the following figure, Machine A and Machine B have an installation of OpenEdge and OpenEdge Management.




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).

An alternative to this scenario is to set up Machine A, for example, as a host machine and Machine B as a remote AdminServer. To effect this setup, we recommend you stop the OpenEdge Management service on Machine B**before** you enable that machine as a remote AdminServer.

Should you later decide to discontinue using Machine B as a remote AdminServer, you can run restart the OpenEdge Management service, which re-enables OpenEdge Management in the OpenEdge product.

# Unglue OpenEdge Management from OpenEdge

If the machine you intend to use as a remote AdminServer has OpenEdge Management installed, we recommend you unglue OpenEdge Management from OpenEdge before you set up the machine as a remote AdminServer.

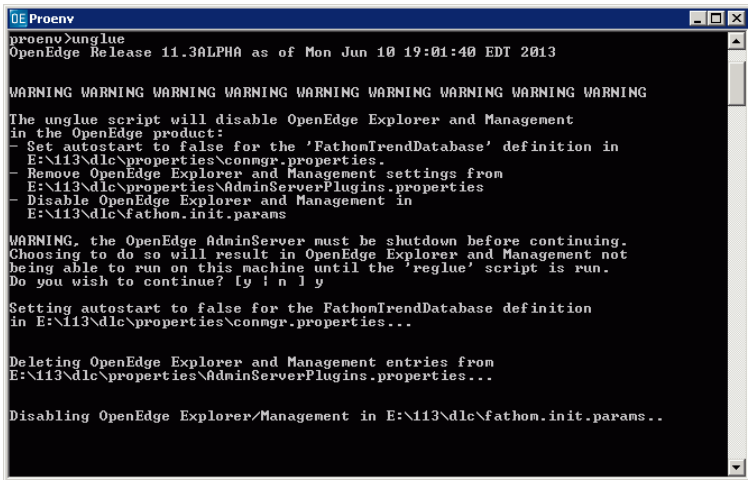
You must have system administrator privileges on Windows and root privileges on UNIX to perform the unglue operation.

To unglue OpenEdge Management:

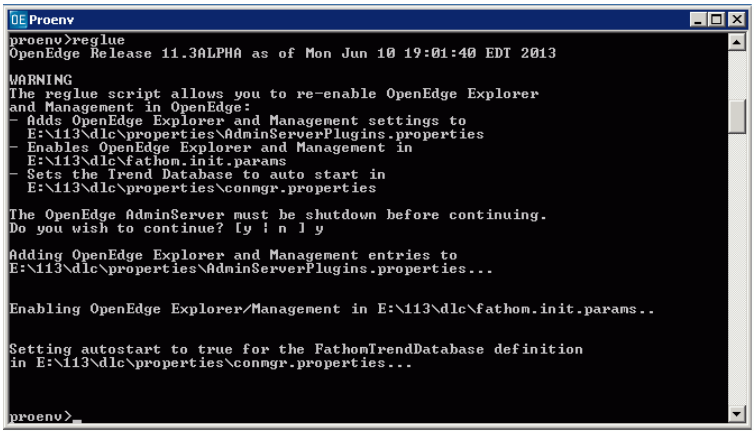
1. Depending on whether you are working with a Windows or a UNIX installation, begin the unglue as follows:
   - To unglue on a Windows machine, select **Start** > **Programs (or All Programs)** > **Progress** > **OpenEdge** > **Proenv**.
   - To unglue on a UNIX machine, log in as root in a terminal 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 Set up a remote AdminServer on page 52. To reglue OpenEdge Management to the Progress or OpenEdge product, see Reglue OpenEdge Management to OpenEdge on page 51.

## Reglue OpenEdge Management to OpenEdge

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

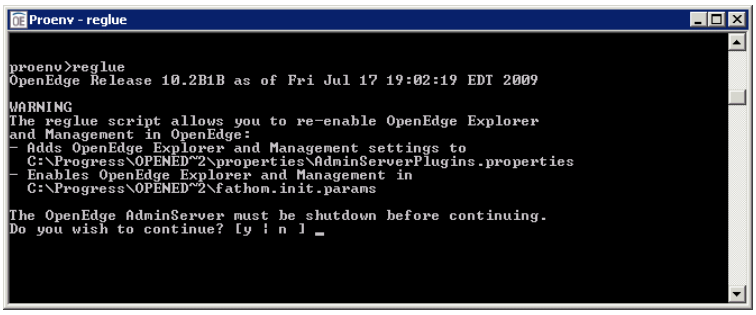
You must have system administrator privileges on Windows and root privileges on UNIX to perform the reglue operation.

To reglue OpenEdge Management:

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, see Unglue OpenEdge Management from OpenEdge on page 50.

# Set 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 is disabled on the remote AdminServer.

# Set 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 for details on how to set up a remote AdminServer.

## Verifying that OpenEdge Management 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:

# 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 Set up a remote AdminServer on page 52.
- 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`.

---

# 5

# Administer OpenEdge Management

You can fine-tune the initial OpenEdge Management configuration and licensing decisions you made.

For details, see the following topics:

- Update configuration options
- Add users as administrators or operators
- Customize the operator role
- Configure user authentication
- Set OpenEdge Management user preferences
- Set up a remote AdminServer
- Change general configuration settings
- Change OpenEdge Management Trend Database settings
- Change OpenEdge Management e-mail alerts settings
- Change OpenEdge Management resource monitoring settings
- Set the OpenEdge Management graph cache
- Configure process pooling
- Set OpenEdge Management resource monitor defaults
- Set OpenEdge Management distribute resource properties
- Change the OpenEdge Management SNMP Adapter settings

- Use the command-line interface
- Set the log level for the AdminServer log file
- Configure OpenEdge Management log files

# Update configuration options

You can use OpenEdge Management 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.

When you are working with OpenEdge Management, you can make modifications in one or more of the areas described in the following table.

**Table 3: Configuration option availability**

| Option | Description | Applicable in OpenEdge Management |
|---|---|---|
| **Authorized Users** | Enables you to manage user accounts and to customize the operator role | Yes |
| **User Preferences** | Enables you to set the rate (if any) at which OpenEdge Management automatically refreshes | Yes |
| **Remote AdminServers** | Enables you to add and remove remote AdminServers | Yes |
| **General** | Enables you to manage the OpenEdge Management startup configuration and the actions to perform for OpenEdge Management internal alerts | Yes |
| **Trend Database** | Enables you to configure the trend database | Yes |
| **Web Server Configuration** | Enables you to configure the web server HTTP and HTTPS settings. You can also set the login session timeout value. | Yes |
| **Email alerts** | 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. | Yes |

| Option | Description | Applicable in OpenEdge Management |
|---|---|---|
| **Resource Monitoring** | Enables you to manage whether to automatically poll resources, generate alerts, collect trend data, and include status changes | Yes |
| **Graph Cache** | Enables you to set the time period for collecting graph cache samples on selected resources and AdminServers | Yes |
| **Database Administration Console** | Enables you to set the batch size for the database administration console. Batch size determines the number of records from the database that are displayed on the Database Administration Console Configuration page. The default batch size is set to 100. | Yes |
| **Process Pooling** | 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. | Yes |
| **Resource Monitor Defaults** | Enables you to set default polling attributes for resource functions | Yes |
| **Resource Property Distribution** | Enables you to bulk copy resource properties to selected target resources | Yes |
| **SNMP Adapter** | (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. | Yes |

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 Set Up Secure Communications on page 83 for details about using the secure protocol.

# Add users as administrators or operators

OpenEdge Management provides 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 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.

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. They define who can log in using a web browser.

# Manage the authorized users list

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

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.

# Add a new user

If you are logged in as an administrator in OpenEdge Management, 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>*`\conf` folder. This information is saved in the following format:

```
<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 for the operation to take effect.

   Progress recommends using the OpenEdge Management 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.

# Change passwords and descriptions

Whether you are an administrator or an operator, you can change your own unique password 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. When the user provides the correct password, the user can resume working. However, if the user does not enter the correct password, the user login process fails and access is denied.

To change the password 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, then you must change the user name, because duplicate user names are not allowed.

## Change the administrator password

During the initial access of OpenEdge Management, 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 Change passwords and descriptions on page 57 for more information.

## Delete 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.

# Customize 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>*`\conf` 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**.

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, then you must stop and restart the OpenEdge Management for the operation to take effect.

# Manage 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. 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 about creating, editing, and using database connections, see *Configure Database Multi-tenancy with OpenEdge Management* and *Manage Database Table Partitioning with OpenEdge Management*.

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

```
{
        "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**

| Permission | JSON value |
|---|---|
| **Disallow Read Access** | `"actions" : ""` |
| **Allow Create Connections** | `"actions" : "create"` |
| **Allow Edit Connections** | `"actions" : "write,read"` |

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 upgrading from an older version of OpenEdge Management, 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.

# Configure user authentication

In earlier releases, OpenEdge Management handled user authentication to the management console based on the login information saved in a property-file. This file is available in the OpenEdge Management installation directory and contains the login information of the user such as username, password, and role.

Along with property-file based authentication, OpenEdge Management now supports OpenEdge Authentication Gateway authentication, a Security Token Service (STS) based authentication. OpenEdge Management provides an interface which allows you to select OpenEdge Authentication Gateway as the authentication mechanism to log into the management console. However, if OpenEdge Authentication Gateway authentication is not selected, the existing property-file based authentication will be the default authentication mechanism.

As an OpenEdge administrator, using the management console, you can manage the users and configure the type of authentication you want them to use.

For information about OpenEdge Authentication Gateway authentication in OpenEdge, see *Learn about the OpenEdge Authentication Gateway*.

## OpenEdge Authentication Gateway authentication

To implement OpenEdge Authentication Gateway authentication for user logins in OpenEdge Management, OpenEdge Management is introduced as a new client to the OpenEdge Authentication Gateway server.

---

**Note:** Before implementing OEAG authentication in OpenEdge Management, ensure that the OEAG server is running.

---

When you choose OEAG authentication as the authentication type and log into the management console by providing the credentials such as username and password, the credentials are converted into an OEAG authentication request token. The authentication request token is then sent to the OEAG server for authentication and the server returns an authentication response token. The authentication response token is stored as a part of your web console session until the session expires or you log out.

OpenEdge Management allows you to configure OEAG authentication for Web server logins and validate the authentication tokens returned by the OEAG server.

### Support for multiple domains

For logins using OpenEdge Authentication Gateway authentication, OpenEdge Management supports a username with or without its domain name, and even with a blank domain. For example, the username field in OpenEdge Management login page accepts `test`, `test@domain`, or `test@domain.com` as username.

By default, the OpenEdge Authentication Gateway server is configured with a blank domain. When logging into the management console with the default credentials, you need not provide the domain name. In this case, the management console does not display the fully qualified username after you log in. When logging into the management console with usernames other than the default one, you must provide the domain name. The management console displays the fully qualified username after you log in.

## Access OpenEdge Management resources

OpenEdge Management performs authentication and authorization checks for every call made to each resource by a client. The client can be a web browser or Progress Developer Studio for OpenEdge using HTTP. After the user authentication is successful, specific permission is required to access a resource and perform an action on that resource such as starting a server or changing a property.

---

**Note:** Progress Developer Studio uses basic HTTP authentication to authenticate requests to OpenEdge Management. OpenEdge Management does not cache authentication credentials. When using Progress Developer Studio as a client for OpenEdge Management that is configured to use OpenEdge Authentication Gateway authentication, a Progress Developer Studio authentication request to OpenEdge Management results in sending the request to the OpenEdge Authentication Gateway server. This set up is not considered efficient.

---

If you are an administrator, you can configure user permissions based on the role of the user in OpenEdge Management. OpenEdge Management provides the following roles with default configuration:

- **PSCAdmin**—This role has full permissions within OpenEdge Management.
- **PSCOper**—This role has limited permissions which can further be modified by an administrator.
- **PSCTrend**—This role has permissions to access very few resources that are required to provide remote trending operations via HTTP call from one OpenEdge Management installation to another.

In property-file based authentication, the property-file in the OpenEdge Management installation directory stores and assigns the role information to a user. When you enable OpenEdge Authentication Gateway authentication in OpenEdge Management, instead of a property-file, the authentication token returned by the OpenEdge Authentication Gateway server assigns the role information to a user.

To perform authentication and authorization checks, OpenEdge Management retrieves the user role information from the authentication token returned by the OpenEdge Authentication Gateway server. If the user role information contains one of the roles supported by OpenEdge Management, the authentication request will be successful allowing the user to log into the management console.

## Limitations to access OpenEdge Management pages

When you enable OpenEdge Authentication Gateway authentication in OpenEdge Management, access to few pages in the management console is limited or restricted. The limitations are:

- Changing your password after your first login is disabled.
- **Create User** and **Change my password** links under the **Authorized Users** link are disabled.
- Creating, viewing, or editing the users using the **Authorized Users** page is disabled.
- For a user with PSCOper role, access to the **Authentication Configuration** page is disabled.

You can configure collections and views as part of user preferences which are stored based on the fully qualified username.

For navigating to **Authorized Users** and **Authentication Configuration** pages, see Configure user authentication for web server logins on page 63.

# Configure user authentication for web server logins

As an administrator, you can set preferences in OpenEdge Management that enable users to choose an authentication type for web server logins. You can configure these preferences in the **Authentication Configuration** page, and the configuration information is stored in the `fathom.properties` file.

To configure user authentication:

1. In the OpenEdge Management console, click the **Options** icon.

   The **Options** page appears.

2. Click **Authorized Users** to open the security home page and then select the **Authentication Configuration** tab.

   The **Authentication Configuration** page appears.

3. To allow OpenEdge Management to use its built-in authentication mechanism (property-file based authentication), select **Use OpenEdge Management Internal Authentication**.

4. To allow OpenEdge Management to use OpenEdge Authentication Gateway based authentication, select **Use OpenEdge Authentication Gateway Authentication**.

   If you select OpenEdge Authentication Gateway based authentication, along with the **Authentication gateway URL**, you must provide one domain and its access code at the least.

Provide the required information in the following fields:

- **Authentication gateway URL**—The URL which OpenEdge Management uses to connect to the OpenEdge Authentication Gateway server to authenticate users during a connection.

  You must provide valid HTTPS URLs; HTTP URLs are not allowed. When providing the URL, ensure that it does not point directly to localhost (127.0.0.1). Instead, you can use the DNS name with which OpenEdge Management connects to the OpenEdge Authentication Gateway server.

- **Disable SSL host verification**—Selecting the check box turns off host verification for a TLS connection to the OpenEdge Authentication Gateway server.

  Though disabling host name verification is considered unsafe, you can disable it for testing purposes where the OpenEdge Authentication Gateway server is not set up with a valid server certificate. However, it is always recommended to enable host name verification once the server certificate is setup.

  To secure authentication requests from OpenEdge Management, the OpenEdge Authentication Gateway server certificate must be installed in the `$DLC/certs` directory using certutil. For information about creating and deploying OpenEdge Authentication Gateway server certificate, see *Learn about the OpenEdge Authentication Gateway*.

- **Client authentication header name**—(Optional) The HTTP authentication header name for the OpenEdge Authentication Gateway server.

  The default name **x-oests-token** in this field matches with the default value in the OpenEdge Authentication Gateway server, and is used when the server requires a client key to perform authentication. You can change it only if the OpenEdge Authentication Gateway server is configured to accept a different token name.

- **SNI hostname**—Specify the hostname that you want the OpenEdge Authentication Gateway Authentication for OpenEdge Management to connect to. Use this parameter if the OpenEdge Authentication Gateway server implements the Server Name Indication (SNI) and is configured with multiple hosts that are bound to a single IP. If you use the **SNI hostname** parameter, the OpenEdge Authentication Gateway Authentication sends the hostname during the TLS handshake, enabling the OpenEdge Authentication Gateway server to return the correct TLS certificate to the OpenEdge Authentication Gateway Authentication for OpenEdge Management.

  ---

  **Note:** The OpenEdge Authentication Gateway Authentication for OpenEdge Management will not be established if the SNI hostname parameter has no match with the hostname included in the certificate.

  ---

- **Enabled SSL protocols**—The TLS protocols that are to be enabled. The default protocol is **TLSv1.2**.

  It is recommended to use protocol versions equally or more secure than TLSv1.2 to maintain the highest level of security, unless the OpenEdge Authentication Gateway server is configured to use a lesser secure protocol.

- **Enabled SSL cipher suites**—The TLS cipher suites that are to be enabled.

- **Role prefix**—The prefix provided to the user roles by the OpenEdge Authentication Gateway server. This allows OpenEdge Management to work with the OpenEdge Authentication Gateway server that is configured to use other authentication mechanisms such as LDAP.

  OpenEdge Management removes the prefix from any role returned from the OpenEdge Authentication Gateway server in order to match the role against the internally defined roles. For example, if the OpenEdge Authentication Gateway server returns a role `ROLE_PSCAdmin` with a prefix `ROLE_`, OpenEdge Management ignores the prefix and considers the role name as `PSCAdmin`.

5. Provide the domains and their access codes in the Domain configuration grid as described in Validate authentication tokens on page 65.

   When modifying the domain configuration, it is recommended to disable HTTP and access the web interface through an HTTPS connection with a signed server certificate. This avoids exposing the domain names and domain access codes as clear text when sent across a network.

6. Click **Submit**.

   After submitting the changes made to the authentication mechanism, you must restart the Web server for the changes to take effect. Your current login session expires when you restart the Web server, so log into the management console again.

---

**Note:** If you lock yourself out, edit the `fathom.properties` file to restore the default login mechanism and restart fathom using `fathom -stop/fathom -start`.

---

## Validate authentication tokens

OpenEdge Management validates the authentication tokens returned by the OpenEdge Authentication Gateway server. To validate the tokens, you must configure OpenEdge Management with the domains and their access codes that match with the ones configured in the OpenEdge Authentication Gateway server. The domain access codes configured in OpenEdge Management are stored in a Java keystore in the `$OEMgmt/conf` directory.

You can add domains and their access codes which require access to OpenEdge Management, and delete the existing ones using the Domain configuration grid in the **Authentication Configuration** page. These domains and access codes are read-only entries and cannot be edited. By default, a blank domain with a blank access code is provided in the grid for testing purposes.

---

**Note:** Atleast one domain must be configured for OpenEdge Management to validate the tokens.

---

To add a domain and its access code:

1. In the Domain configuration grid, click **Create**.
2. Provide the name of the domain in the **Domain Name** field.
3. Provide the access code of the domain in the **Access Code** field.
4. Click **Save**.

   The new domain name and its access code appears in the grid.

   When adding a domain and its access code, ensure that you click **Save** in the grid before submitting your preferences in the **Authentication Configuration** page. Optionally, you can click **Cancel** to cancel the action.

To delete an existing domain and its access code:

5. In the Domain configuration grid, select the domain and its access code which you want to delete.
6. Click **Delete**.

# Set 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 the setting the value. Frequently refreshing pages add to the OpenEdge Management processing time.

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

# Set up a remote AdminServer

You can remotely monitor a resource 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, choose one of the following:

   - Click **Options** > **Remote AdminServers**.
   - Click **Resources** > **Remote** > **AdminServers**.

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

2. Click **NEW**.
3. In the **Add AdminServer** window that appears, perform the following:

   a) In the **Host** field, specify the host name of the machine used to run OpenEdge Management.

   b) In the **Management port** field, specify the port number used to the run the AdminServer.

   c) (Optional) Select the **Use encrypted connection** option to secure the communication between OpenEdge Management and the remote AdminServer. The default encryption protocol is TLS 1.2.

   If this option is selected, the default certificates provided by OpenEdge are used. For information on setting up the TLS protocol mechanism for remote AdminServers with user-defined certificates, see Set up secure communication-related security for a remote AdminServer on page 68.

   d) (Optional) In the **User** and **Password** fields, specify the username and password 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.

   OpenEdge Management displays an error if invalid information is provided. You can click **TRY AGAIN** to make necessary changes to the information you provided earlier.

# View a remote AdminServer

You can view the details of a configured remote AdminServer based on their status using the **Remote AdminServer Configuration** page.

In the **Remote AdminServer Configuration** page, select a status from the following options: **Show online and offline** (selected by default), **Show online**, **Show offline**, and **Show only auto-discovered**.

Upon selecting the status, the page displays the following information:

- **Name**—The name of the Remote AdminServer container.
- **Status**—The status of the AdminServer: **Online**, **Offline**, or **Not Checked**.
- **Host**—The host name of the machine on which OpenEdge Management is running.
- **Port**—The port number used to the run the AdminServer.
- **Encrypted Connection**—Specifies whether the connection is encrypted or not. A check mark indicates that the connection is encrypted.
- **OpenEdge Version**—The version of OpenEdge release.
- **OS**—The Operating System of the remote AdminServer.

Optionally, you can click **REFRESH** to view updated information.

# Edit a remote AdminServer

You can edit the configuration of a remote AdminServer using the **Remote AdminServer Configuration** page. The Edit button is enabled only when the remote AdminServer is offline and disabled when the remote AdminServer is online.

To edit a remote AdminServer:

1. From the management console menu, choose one of the following:
   - Click **Options** > **Remote AdminServers**.
   - Click **Resources** > **Remote** > **AdminServers**.

   The **Remote AdminServer Configuration** page appears and displays a list of AdminServers.
2. Select an AdminServer from the list, and click **EDIT**.

   The **Edit AdminServer** page appears.
3. Modify the information as required and click **SAVE**.

   Optionally, you can click **REFRESH** to view updated information.

# Delete a remote AdminServer

You can delete a remote AdminServer using the **Remote AdminServer Configuration** page.

To delete a remote AdminServer:

1. From the management console menu, choose one of the following:
   - Click **Options** > **Remote AdminServers**.

- Click **Resources** > **Remote** > **AdminServers**.

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

2. Select an AdminServer from the list, and click **DELETE**.

   Optionally, you can use the **CTRL** key to select multiple AdminServers.

3. Click **YES** to confirm deletion.

# Set 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 and a remote AdminServer is secure. For more information on setting up a remote AdminServers, see Set up a remote AdminServer on page 66.

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

| Property | Description |
|---|---|
| `sslEnable` | **Default value**: `0`<br>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 for the setting to take effect. |
| `enabledProtocols` | **Default value**: `TLSv1.2`<br>**Supported values**: `SSLv3`, `TLSv1`, and `TLSv1.1`<br>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. |
| `enabledCipherSuites` | 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. |
| `tcpEnable` | **Default value**: 1<br>Enables unsecure connections to remote AdminServer.<br>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. |
| `sslPort` | **Default value**: 7278<br>Specifies the port using which OpenEdge Management receives the incoming secure connections |

| Property | Description |
|---|---|
| `port` | **Default value**: 6835<br>Specifies the port using which OpenEdge Management receives non-secured connections |
| `keyAlias` | **Default value**: default_server<br>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. |
| `keyAliasPasswd` | **Default value**: -NA-<br>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 about the genpassword utility, see *Manage OpenEdge Keys and Certificates*.<br>If this property is not set, the password of the default alias that is provided by OpenEdge is used. |
| `keyStorePath` | **Default value**: -NA-<br>Specifies the key store location. If this property is not set, the default value is `$DLC/keys`. |
| `sslRequireClientAuth` | **Default value**: 0<br>When set to 1, this property specifies that an incoming secure connection must provide a valid client certificate to connect to the AdminServer. |
| `keyStorePasswd` | **Default value**: -NA-<br>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 about the genpassword utility, see *Manage OpenEdge Keys and Certificates*. |
| `noHostVerify` | **Default value**: 0<br>When set to 1, OpenEdge Management disables host verification when connecting to a remote AdminServer that has a private key.<br>**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 pair 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 *Manage OpenEdge Keys and Certificates*.
  2. Open the `management.properties` file from `$DLC\properties` and edit the properties to point to the private-public key pair 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 *Manage OpenEdge Keys and Certificates*.
  2. Open the `management.properties` file from `$DLC\properties` and edit the properties to point to the private-public key pair 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.

# Change general configuration settings

You can change the following current general configuration settings:

- Prompt for a comment while clearing an alert.
- A comment is required to clear an alert.
- The action OpenEdge Management 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 **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.
   - 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.

# Change OpenEdge Management Trend Database settings

You specify the local database path name and the local database port when you initially configure OpenEdge Management. (These initial configuration steps are described in Set Up OpenEdge Management for the First Time on page 31. However, you can also specify them using the **OpenEdge Management Trend Database Configuration** page.

To change trend database configuration settings:

1. From the OpenEdge Management console, click **Options**.

   The **OpenEdge Management options and configuration** page appears.

2. Click **Trend Database**.

   The **OpenEdge Management Trend Database Configuration** page appears and displays the current trend database settings.

3. In the **Trend database location** field, specify the location for the trend database.

   You can either use the predefined explicit path where the trend database is located by default, or type a different path to the database. For example, `C:\Progress\oemgmt\work\fathomdb\fathom.db`. Note that the inclusion of the `.db` extension in the path name is optional.

   OpenEdge Management provides a backup of the default trend database `fathom.bak` in the `$OEMgmt\db` directory. If you specify a location other than the default trend database location, OpenEdge Management extracts that backup and places it in the location you specified.

   If you already have a trend database placed in the specified location, OpenEdge Management uses that trend database.

   Alternatively, you can either copy the OpenEdge Management trend database `fathom.db` to the specified location using the `procopy` or `prodb` command, or restore the trend database backup `fathom.bak` to the specified location using the `prorest` command.

4. In the **Trend database port** field, type the database port number. For example, `1234`.

5. Enter the user name and password in the **Trend database user** and **Trend database password** fields, respectively.
6. Click **SUBMIT**.

**Note:** If the local AdminServer is offline, all the Trend database configuration fields are disabled.

# Change 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, 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 `SSLv3`, `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 supports all the cipher suites that are provided by the TLS implementation of the Java Secure Socket Extension (JSSE).
11. Click **Submit**.

# Change OpenEdge Management resource monitoring settings

You can enable or disable specific OpenEdge Management functionalities using the resource monitoring options in the **OpenEdge Management Resource Monitoring Configuration** page. For example, if the OpenEdge Management Trend Database is going to be taken down for maintenance, you can choose to turn off trending, but allow the rest of the OpenEdge Management functionalities to run.

To change the OpenEdge Management resource monitoring settings:

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

   The **Options** home page appears.

2. Click **Resource Monitoring**.

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

3. In the **General** section, select the following options as required:

   - **Poll resources**—Enables polling for all resources.
   - **Generate alerts**—Generates alerts after polling.
   - **Collect trend data**—Collects resource trend data.
   - **Include status changes**—Includes status changes of a resources in its trend data.

   Each option in this section is independent of the others, except for **Include status changes**. If the **Collect trend data** option is not selected, the **Include status changes** option is disabled.

4. In the **CPU Monitoring** section, select one of the following options:

   - **System Wide**—Monitors only the usage of system-wide CPU resource and removes all other CPU resources available for an AdminServer.
   - **Individual CPU Monitoring**—Monitors the usage of individual CPU resources available for an AdminServer, including the usage of system-wide CPU resource.

   These options allow you to choose how you want to manage and monitor the CPU resources in both local and remote AdminServer environments.

5. Click **Submit**.

# Set 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.

Progress recommends 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.

# Configure process pooling

To reduce processing overhead and improve Web request performance, OpenEdge Management provides 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 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 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 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

## Set 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.

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, `http://localhost:8810/apsv/` 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**.

## Create 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.

## Delete 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 and click **Delete**. Click **Yes** in the confirmation dialog.

# Set 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:

- Application server

- Databases
- DataServers (Oracle, and MS SQL Server)
- File
- NameServer
- Network
- Progress Application Server for OpenEdge (PAS for OpenEdge)
- SonicMQ Adapter
- System

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 *Monitor OpenEdge Resources with OpenEdge Management*. For more information about selecting resource monitor defaults for databases, see the relevant section in *Manage the OpenEdge Database*. For more information about selecting resource monitor defaults for OpenEdge server components, see the relevant section in *Manage Servers, Data Servers, Messengers, and Adapters with OpenEdge Management*.

# Set 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:

- Application werver
- CPU
- Database
- FileSize
- HTTP
- LogFile
- Memory

- NameServer
- PAS
- REST
- TCP

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.

# Change the OpenEdge Management SNMP Adapter settings

OpenEdge Management provides an SNMP management agent (SNMP Adapter) for responding to administrative information queries from your SNMP management console or SNMP manager. For information about SNMP version support, see the *OpenEdge Platform & Product Availability Guide* on the Progress Information Hub at https://docs.progress.com.

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 OpenEdge Management 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 OpenEdge Management alerts is stored in the OpenEdge Management MIB file, `PSC-FM-MIB.txt`, available at the `<OpenEdge-install-dir>/conf` 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 OpenEdge Management SNMP security configuration. For example, if you are using SNMP version 3 with `AuthNoPriv` in OpenEdge Management, 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 5: SNMP version 3 security levels**

| Security level | Description |
|---|---|
| **No Authentication and No Privacy** | This level does not require you to set any authentication and privacy options. |

| Security level | Description |
|---|---|
| **Authentication but No Privacy** | This level requires you to set the following authentication options:<br>• **Authentication Protocol**—The authentication mechanism that is used to generate a hash of the authentication password.<br>• **Authentication Password**—The SNMP security authentication password. |
| **Authentication and Privacy** | This level requires you to set the authentication options and the following privacy options:<br>• **Privacy Protocol**—The encryption protocol used to encrypt SNMP communications.<br>**Note:** If the JVM does not support a given encryption protocol, the protocol is not displayed as an available option. To use an additional protocol, you can update the security policy configuration from Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.<br>• **Privacy Password**—The SNMP security privacy password. |

- **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.

# Use the command-line interface

OpenEdge Management provides 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 Set Up Secure Communications on page 83 for details.

Specifically, the command-line interface allows you to:

- Start, query, and stop OpenEdge Management.
- View configuration information of the OpenEdge Management environment.
- View the list of resources.
- Enable or disable a resource.

- Dump the contents of the OpenEdge Management 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 command-line references, see Fathom Command-line References on page 99.

# Set the log level for the AdminServer log file

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

To set the log level in Windows or on UNIX:

1. Open the following file in a text editor:

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

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

   `-DLogLevel=`*`n`*

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

# Configure OpenEdge Management log files

The OpenEdge Management log (`fathom.log`) records the activity of your OpenEdge Management. A new OpenEdge Management log file is created each day and its corresponding date is appended to the name of the log file—for example, `fathom.2018-02-13.log`. These log files contain the details of each log entry such as the date and time of the entry, the level of the information recorded, and its corresponding thread and message.

OpenEdge Management log files are located in the `$OEMgmt/logs` (`C:\Progress\oemgmt\logs`) folder. You can modify the configuration of these log files using the `logging.xml` file located in the `$OEMgmt/conf` folder. For more details about configuring log files, see https://www.slf4j.org/docs.html.

# 6

# Set Up Secure Communications

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

The following topics describe how to use the HTTPS protocol with the web server for OpenEdge Management.

For details, see the following topics:

- Transfer data securely with the HTTPS protocol
- About common secure communication-related terminology
- Get started: using the demo certificate
- Change web server settings
- Use secure communication
- Use your own certificate
- Use the keytool utility

## Transfer data securely with the HTTPS protocol

As you work with OpenEdge Management, make sure that data being transferred between the web browser and the web server is secure. 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 web server. The HTTPS protocol with TLS 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, a web browser and the web server) can authenticate each other's identity.

## Use the demo certificate or your own certificate

To help you get started using the cryptographic protocol, OpenEdge Management includes 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 in the following topics.

# About common secure communication-related terminology

As you prepare to establish secure communications of OpenEdge Management 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*.

**TLS 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 Oracle, 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.

**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 CA. 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 CA.

**procertm utility**

A utility you can use to add any CA'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`).

# Get 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 provides and set up the HTTPS protocol for communication with the Web server.

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

## Configuration update errors or warnings

In the event when you make an update to the web server 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.

## Identify trusted clients

As you update the configuration of the web server, you can optionally identify one or more trusted clients who are allowed to connect to the OpenEdge Management 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.

## Reconnect after updates

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

# Change web server settings

When you initially configure OpenEdge Management, you specify the web server port you want to use. You cannot select the HTTPS protocol for the web server at this stage, but you can update the configuration options after the installation is complete. You can change the port number and specify 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, after OpenEdge Management is installed for the first time:

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

   The **Options** page appears.

2. Click **Web Server Configuration**.

   The **OpenEdge Management Web Server Configuration** page appears with current Web server settings.

3. Select the following transfer protocol options per your requirements:

   - **Enable HTTP protocol**
   - **Enable HTTPS protocol**

     You can select both protocols at once.

   Specify the port numbers in their respective **HTTP port** and **HTTPS port** fields.

4. To automatically upgrade insecure connection requests to secure connection requests, select **Upgrade insecure HTTP requests to HTTPS**.

   **Note:** You must select **Enable HTTPS protocol** to select this option.

   Selecting this option along with **Enable HTTP protocol** and **Enable HTTPS protocol** allows the Web server to redirect all insecure HTTP connection requests to secure HTTPS connection requests. Deselecting this option can result in a less secure connection, so it is recommended that you configure OpenEdge Management with a valid certificate and use this option. For more information about using certificates, see Use your own certificate on page 92.

5. Set the login session timeout value in the **Timeout for logins** list. The default value is **30 minutes**.

   **Note:** You must log out and log in to enable the session timeout value.

   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 `$OEMgmt/conf` 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.

6. Set one of the following options:

   - If you want to work with the demo keystore, click **Submit**. See Use secure communication on page 89 for details about using an HTTPS connection.
   - If you are an advanced user and you want to change the keystore information, see Use advanced HTTP and HTTPS options with the web server on page 87.

# Use 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.
- Identify trusted clients for HTTP or HTTPS.

To use the advanced options:

1. In the **OpenEdge Management Web Server Configuration** page, click **Advanced Options**.

   The expanded **OpenEdge Management Web Server Configuration** page appears.

2. Under **HTTP Configuration**, specify the name of one or more trusted clients in the **Trusted clients** field. Use a comma-delimited list to specify more than one trusted client.

   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`).

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

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

The **Keystore pass phrase** and **Alias** fields are 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 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.

4. In the **Trusted clients** field, specify the name of one or more trusted clients. Use a comma-delimited list to specify more than one trusted client.
5. Click **Submit**. A message appears confirming that the configuration has been successfully updated.
6. Click **OK**.

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

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

| Property | Description |
|---|---|
| `sslEnable` | **Default value**: `0`<br>Enables you to change the cryptographic protocols and ciphers for secure communication with a web server. If you enable TLS for the web server in OpenEdge Management, this property is set to `true`. |

| Property | Description |
|---|---|
| SSLEnabledProtocols | **Default value**: TLSv1.2<br>**Supported values**: SSLv3, TLSv1, and TLSv1.1<br>If you want to change the default cryptographic protocol for the web server, 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 web server, 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. |

**Note:** Transport Layer Security (TLS) is the new version of SSL.

# Use secure communication

After 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 by using the HTTPS protocol.

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

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

Where:

*host-name*

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

*port-number*

The port on which HTTPS is listening for secure communications.

The login window appears.

## Detect 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 9: 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 10: Certificate details**



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

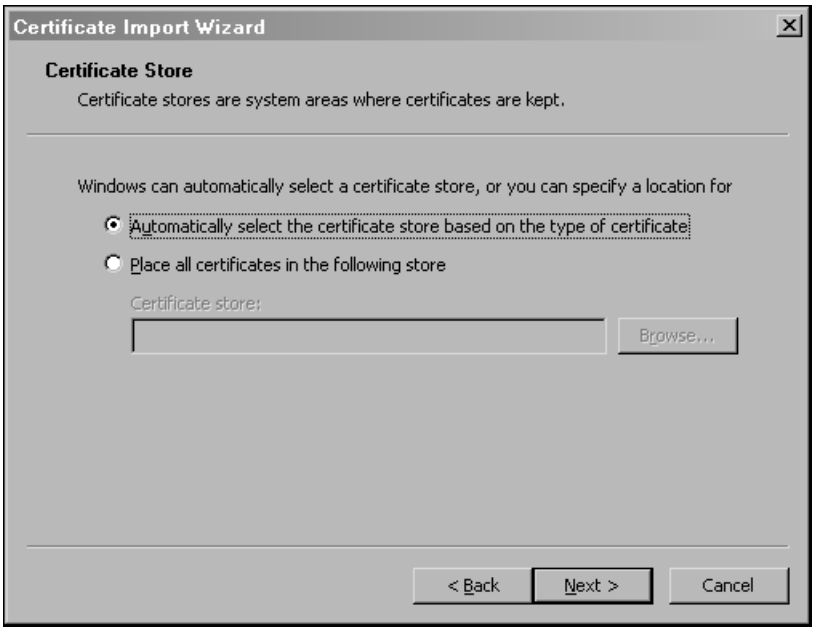
## Install a certificate in Internet Explorer

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.

# Use your own certificate

If you want to use a certificate other than the demo included with OpenEdge Management, 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 Use the keytool utility on page 92 for details.
- Use an existing certificate that you have already acquired from a third-party CA. To use the existing certificate, follow Step 3: Import the CA Certificate on page 96 and Step 4: Import the signed certificate to the keystore on page 96.

# Use 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: Create a keystore

Before you obtain a digital certificate, you must create a keystore to hold the identity and CA certificates. Creating a keystore also places 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 keystore, 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-install-dir>/conf/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 6: Distinguished name string components**

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

`-alias`

A value that identifies a specific certificate/key pair. You must provide a unique alias for each certificate and 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 and key pair. In the example shown here, the keypass is `coyote`.

`-keystore`

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

In the example shown earlier in this section, `myIdentityKeystore.jks` is the keystore name. If the keystore file were located in the default location for OpenEdge Management, for example, it would be in the `Progress\oemgmt\conf` directory.

`-storepass`

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

`-validity`

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

`-keyalg`

The algorithm being used to create the certificate signature.

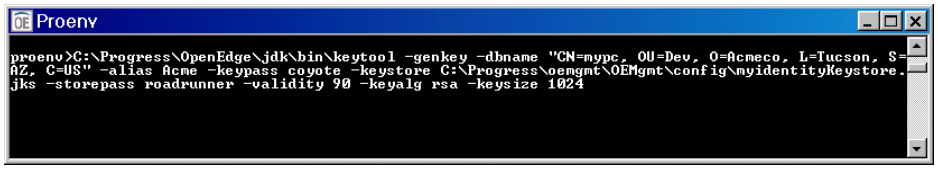
Use this option to override the default value of `dsa` by specifying `rsa`, which is the default used by the Jetty Web server and required by Internet Explorer and Netscape.

`-keysize`

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

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

**Figure 11: 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\conf` 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: Generate a Certificate Signing 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 CSR 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 Symantec, 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: Create a keystore on page 93) by importing the CA certificate and your new site certificate.

## Step 3: Import 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: Import the signed certificate to the keystore

To add the signed certificate to the keystore, 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 certificate 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 OpenEdge Management the first time, choosing to download and install the CA certificate.

# 7

# Fathom Command-line References

You can use the OpenEdge environment window `proenv` for managing and administering OpenEdge Management.

The following topics describe the usage and syntax of fathom commands.

For details, see the following topics:

- Use Proenv
- Access help (help)
- Start OpenEdge Management (start)
- Stop OpenEdge Management (stop)
- Check status (query)
- Restart OpenEdge Management (restart)
- Display configuration information (configinfo)
- Clear an alert (clear)
- Enable a resource (enable)
- Disable a resource (disable)
- List alerts (alertlist)
- Fire an alert (firealert)
- Dump configuration database (dump)
- Load configuration database (load)

- List resources (reslist)
- Initialize new database (initcachedb)


# Use Proenv

In Windows, you can access the Proenv utility by selecting **Start** > **Programs (or All Programs)** > **Progress** > **OpenEdge** > **Proenv**. In UNIX, you can use `proenv.sh` located in the `$DLC/bin` folder. This utility sets the shell environment variables needed for executing both OpenEdge Management (fathom) and OpenEdge commands.

When using the Proenv utility, most of the fathom commands are executed using the OpenEdge Management web server, which is registered as a Windows service at the time of OpenEdge Management installation. The utility determines whether the Web server is registered as a Windows service and executes the command accordingly.

For fathom commands executed using the web server, the following switches are generic and optional:

- **`-httpport`**—The port on which OpenEdge Management is running. If this switch is not specified, the utility uses the current port number mentioned in the `catalina.properties` file located in the `$OEMGMT/conf` folder.
- **`-user`**—The username for OpenEdge Management. Progress recommends that you specify this switch. If this switch is not specified, the utility uses the current username of your machine.
- **`-password`**—The password for the username you provided. Using this switch in the command might allow others to see your password in cleartext. So, Progress recommends that you specify the password only when prompted.

However, some fathom commands such as `-start`, `-stop`, `-query`, `-dump` (offline), and `-load` (offline) are executed without using the web server. Therefore, the switches `-httpport`, `-user`, `-password` are not required.

The commands `-start`, `-stop`, `-query`, and `-restart` use the `tcman` service located in the `$OEMGMT/bin` folder. When executing the `-start` and `-stop` commands, you can use the `-quiet` switch to keep the output information to a minimum.

---

**Note:** When OpenEdge Management is registered as a Windows service, you must have appropriate permissions to execute the `-start` or `-stop` commands. Alternatively, you can start or stop OpenEdge Management from the Windows Services utility.

---

# Access help (help)

## Description

Displays the help options for any command.

## Syntax

```
fathom -help -command
```

### Example

The following command is an example to view the help options for `-stop` command:

```
fathom -help -stop
```

# Start OpenEdge Management (start)

## Description

Starts OpenEdge Management.

## Syntax

```
fathom -start option
```

**Table 7: Command-line options for starting**

| Option syntax | Description |
|---|---|
| `-timeout` <*time*> | Time, in seconds, for OpenEdge Management to wait for a response. The default is 240 seconds. |

**Note:** To start OpenEdge Management as a Windows service, edit the `appserver.properties` file located in the `$OEMGMT/conf` folder and set the value of `psc.as.service` to `true`.

## Example

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

# Stop OpenEdge Management (stop)

## Description

Stops OpenEdge Management.

## Syntax

```
fathom -stop option
```

**Table 8: Command-line options for starting**

| Option syntax | Description |
|---|---|
| `-timeout <time>` | Time, in seconds, for OpenEdge Management to wait for a response. The default is 240 seconds. |

### Example

```
fathom -stop -timeout 30
```

# Check status (query)

### Description

Checks the status—initializing, running, not running, or stopped—of OpenEdge Management.

### Syntax

```
fathom -query option
```

**Table 9: Command-line options for starting**

| Option syntax | Description |
|---|---|
| `-timeout <time>` | Time, in seconds, for OpenEdge Management to wait for a response. The default is 240 seconds. |

### Example

```
fathom -query
```

# Restart OpenEdge Management (restart)

### Description

Restarts OpenEdge Management.

### Syntax

```
fathom -restart option
```

**Table 10: Command-line options for restarting**

| Option syntax | Description |
|---|---|
| `-timeout <time>` | Time, in seconds, for OpenEdge Management to wait for a response. The default is 240 seconds. |

### Example

```
fathom -restart -timeout 120
```

# Display configuration information (configinfo)

### Description

Displays configuration information of the OpenEdge Management environment.

This command provides details about operating system environment, Fathom and core product, Java environment, and library and system paths.

### Syntax

```
fathom -configinfo
```

# Clear an alert (clear)

### Description

Clears an alert from OpenEdge Management.

### Syntax

```
fathom -clear option [-comment '<comment text>']
```

The following table lists options to use with the fathom `-clear` command.

**Table 11: Clear alert command options**

| Option syntax | Purpose | How to use |
|---|---|---|
| `-httpport <port-number>` | Identifies the port number if it is not the default port of 9090 | Provide the `-httpport` option followed by the port number. |
| `-comment '<comment-text>'` | Provides a comment when clearing an alert | Provide the `-comment` option followed by the comment text. The text must be enclosed in single quotation marks. |
| `-alert <alert-name>`<br>`[-AdminServer <AdminServer>] \|`<br>`[-resource <resource>] \|`<br>`[-restype <resource type>]` | Clears all instances of a particular alert for one specific resource, or for all resources within a specific AdminServer | Provide the `-alert` command followed by the `alert name`. Then provide either the `resource name` or the `resource type`.<br>Options are defined as follows:<br>• **`-AdminServer`**— The name of a AdminServer as defined in OpenEdge Management.<br>• **`-alert`**— The name of the alert as defined in OpenEdge Management.<br>• **`-resource`**—The name or the reference key of the resource as defined in OpenEdge Management. See Additional options on page 108 for details about the reference key.<br>• **`-restype`**—The resource type. The type of resource is limited to one of the following: database, file, network, openedge, or system. |
| `-alertid <alert id number>` | Clears an alert by its number (regardless of the resource or its type) | Provide the `-alertid` option followed by its number. |
| `-all[-restype <resource type>] \|`<br>`[-resource <resource>] \|`<br>`[-alert <alert name>] \|`<br>`[-AdminServer <AdminServer>] \|`<br>`[-severity <severity>]` | Clears:<br>• All alerts<br>• All alerts for a particular resource type<br>• All alerts for a particular resource<br>• All instances of a particular alert for all resources<br>• All alerts for a specific AdminServer<br>• All alerts for a specific severity | Provide the `-all` command without an option to clear all alerts, or with one of these options to clear particular alerts:<br>• **`-restype`**—The resource type. The type of resource is limited to one of the following: database, file, network, openedge, or system.<br>• **`-resource`**—The name or the reference key of the resource as defined in OpenEdge Management. See Additional options on page 108 for details about the reference key.<br>• **`-alert`**—The name of the alert as defined in OpenEdge Management. |

| Option syntax | Purpose | How to use |
|---|---|---|
| | | • **`-AdminServer`**—The name of a AdminServer as defined in OpenEdge Management.<br>• **`-severity`**—The alert severity: Severe, Error, Warning, or Informational. |

### Example

OpenEdge Management polls your Sports2020 database and sends an alert for Record Waits High (the alert sent when waits for records are above a defined threshold). To clear this alert from the command line, enter the following:

```
fathom -httpport 8080 -clear -alert RecordWaitsHigh -comment 'Cleared by Admin'
```

# Enable a resource (enable)

### Description

Enables a resource.

### Syntax

```
fathom -enable option
```

`-user`

(Optional) The username for OpenEdge Management. Progress recommends that you specify this switch. If this switch is not specified, the utility uses the current username of your machine.

`-password`

(Optional) The password for the username you provided. Using this switch in the command might allow others to see your password in cleartext. So, Progress recommends specifying the password only when prompted.

**Table 12: Command-line options for enabling a resource**

| Option syntax | Description |
|---|---|
| `-resource <resource-name>` | Enables a specific resource. |

| Option syntax | Description |
|---|---|
| `-restype <resource-type>` | Enables all the resources that belong to a resource type: `database`, `file`, `network`, `openedge`, or `system`. |
| `-Fathom` | Enables polling for all resources.<br>This option does not change the status of individual resources. |

### Example 1

The following command is an example to enable the `asbroker1` resource using the `-resource` switch:

```
fathom -enable -user admin -resource asbroker1
```

### Example 2

You can also enable a resource without using the `-resource` switch, but ensure that you specify the `resource-name` or the `resource-key` next to the `-enable` switch.

Consider the following examples:

```
fathom -enable asbroker1 -user admin
```

```
fathom -enable localhost:resource.openedge.appserver.asbroker1 -user admin
```

# Disable a resource (disable)

### Description

Disables an OpenEdge Management resource.

### Syntax

```
fathom -disable option
```

`-user`

(Optional) The username for OpenEdge Management. Progress recommends specifying this switch. If this switch is not specified, the utility uses the current username of your machine.

`-password`

(Optional) The password for the username you provided. Using this switch in the command might allow others to see your password in cleartext. So, Progress recommends specifying the password only when prompted.

**Table 13: Command-line options for disabling a resource**

| Option syntax | Description |
|---|---|
| `-resource <resource-name>` | Disables a specific resource. |
| `-restype <resource-type>` | Disables all the resources that belong to a resource type: `database`, `file`, `network`, `openedge`, or `system`. |
| `-Fathom` | Disables polling for all resources.<br>This option does not change the status of individual resources. |

### Example 1
The following command is an example to disable the `asbroker1` resource using the `-resource` switch:

```
fathom -disable -user admin -resource asbroker1
```

### Example 2
You can also disable a resource without using the `-resource` switch, but ensure that you specify the `resource-name` or the `resource-key` next to the `-disable` switch.

Consider the following examples:

```
fathom -disable asbroker1 -user admin
```

```
fathom -disable localhost:resource.openedge.appserver.asbroker1 -user admin
```

# List alerts (alertlist)

### Description
Displays the list of alerts for a resource.

### Syntax

```
fathom -alertlist -resource resource-name
```

You can display an alert list by specifying one of the `-alertlist` command group selection options on the command-line. The following table identifies and describes each group selection option.

**Table 14: Alert list command group selection options**

| Option syntax | Purpose | How to use |
|---|---|---|
| `-alert` | To view a list of all instances of a particular alert | Provide the name of the alert you want to see. |
| `-resource` | To view a list of alerts for a particular resource | Provide the name of the resource whose alerts you want to see listed. |
| `-AdminServer` | To view alerts associated with a specific AdminServer | Provide the name of the AdminServer whose alerts you want to see listed. |
| `-restype` | To view a list of alerts for a particular resource type | Provide the resource type whose alerts you want to see listed. The resource type is limited to one of the following: database, file, network, system, or openedge. |
| `-severity` | To view a list of alerts of a particular severity | Provide the severity level of alerts you want to see listed: severe, error, warning, or informational. |

**Note:** Ensure that you specify only one option when using this command. Specifying multiple options results in an error.

### Syntax

```
fathom -httpport 8080 -alertlist <group selection option> [keyword value]
```

You can also use two additional options, the `-detail` and `-verbose` options, presented in , with the group selection options highlighted in Table 15: Alert list command options to display additional details on page 109 with the group selection options highlighted in Table 14: Alert list command group selection options on page 108.

Although the command line does not limit the number of options you can type into the command line, only the last group selection option identified on the command line is processed.

The following figure identifies a command line that generates a group selection based on the `-restype` option where the resource type is identified as system. Note that the resource name, listed in the **Resource** column, specifies the AdminServer name and associated resource name. Although this level of detail provides more information about a resource, it does not completely eliminate the possibility of confusion among resources with similar or identical names.

## Additional options

The following table describes the additional options `-detail` and `-verbose`.

**Note:** Unlike the group selection options highlighted in Table 14: Alert list command group selection options on page 108, the `-detail` and `-verbose` options will be processed regardless of the position in which you enter them on the command line.

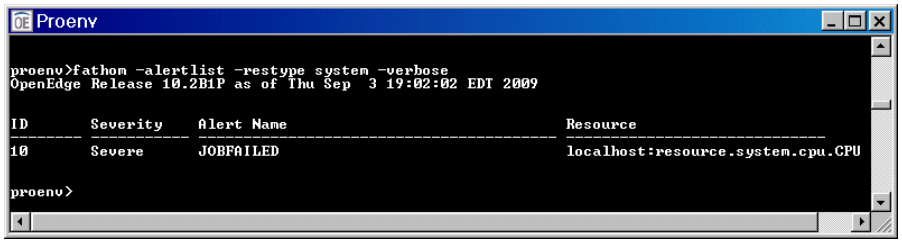
**Table 15: Alert list command options to display additional details**

| Option syntax | Purpose | How to use |
|---|---|---|
| `-detail` | To format the display to provide a block of information about the alert, shown in the command line.<br>The block of information matches what you see when you display the alert in the console. See Table 16: Alert list details on page 110 for a summary of the alert list details. | Provide the `-detail` option along with the option whose alert information you want to see listed. |
| `-verbose` | To change the resource column of the displayed alerts from the generic format *`AdminServer:resource`* name to the fully qualified resource key.<br>See Figure 12: -restype group option with verbose option results on page 109 to see an example of how to use the `-verbose` option. | Provide the `-verbose` option along with the option whose alert information you want to see listed. |

Figure 12: -restype group option with verbose option results on page 109 identifies a command line that generates a group selection based on the `-restype` option that also includes the `-verbose` option. Note that the resource name, listed in the **Resource** column, specifies the *fully qualified resource key*. A fully qualified resource key is the most complete reference to a resource. The default format for a fully qualified resource key identifies each resource by its AdminServer name, the resource category to which the resource belongs, and the specific resource type and associated resource name.

In Figure 12: -restype group option with verbose option results on page 109, the fully qualified resource key information identifies **localhost** as the AdminServer, the resource category as **system**, and the specific cpu resource name as **CPU**.

**Figure 12: -restype group option with verbose option results**




**Note:** The AdminServer name **localhost** is logically the same as the AdminServer name for the system where OpenEdge Management is installed and running.

Use the fully qualified resource key to:

- Ensure that you are not confusing one resource name with another one that is either identical or similar. For example, it is possible to confuse a wsbroker1 on one AdminServer with another wsbroker1 on a different AdminServer. Referencing a resource by its explicit fully qualified resource key eliminates confusion as to what resource you are working with.
- Provide easy access to the complete resource information. You can cut and paste the fully qualified resource key into the command line when you use the `-resource` group option.

**Note:** Due to the use of the colon in the fully qualified resource key between the AdminServer name and the resource category information, this format might need to be put in quotation marks on UNIX systems.

The following table lists the details that can appear in the alert list.

**Table 16: Alert list details**

| Name | Description |
|---|---|
| `Alert ID` | The number given to the alert. |
| `Alert name` | The name of the alert. |
| `Alert severity` | Whether the alert is considered an error, a warning, or informational or severe in nature. |
| `Alert message` | The content of the alert message; for example, notification that the Database Resource known as the OpenEdge Management Trend Database has been enabled. |
| `Alert count` | The number of times the alert has occurred. |
| `AdminServer` | The name of the AdminServer to which the resource belongs. |
| `Resource` | The name of the resource; for example, OpenEdge Management Trend Database. |
| `Last fire date` | The time and date when the alert was last fired. |
| `First fire date` | The time and date when the alert was first fired. |
| `Has been seen?` | Whether the alert has been seen yet (either `true` if it has been seen or `false` if it has not been seen). |
| `Seen by` | If the alert has been seen, the name of the user who saw it. (If the alert has not been seen, the `Seen by` field does not appear.) |

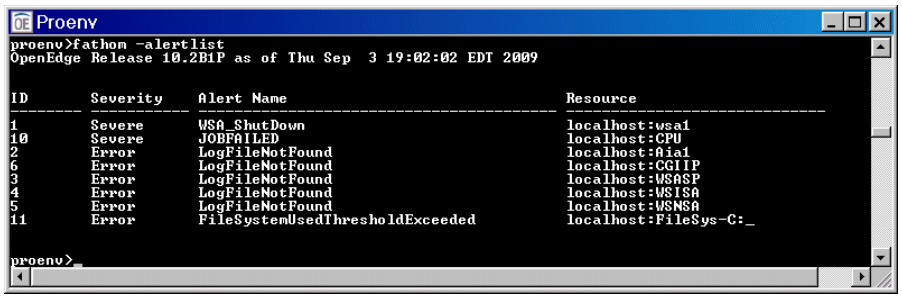
## Examples

Enter the following command to see a list of existing OpenEdge Management alerts from the command line:

```
fathom -alertlist
```

Information about the current alerts appears, as shown below.

**Figure 13: -alertlist in the command line**



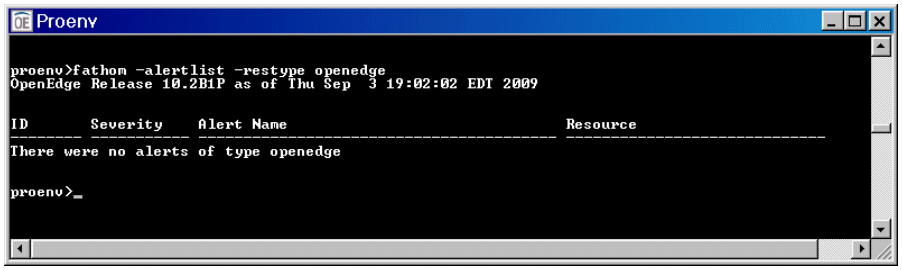

In Figure 13: -alertlist in the command line on page 111 there are eight alerts across a number of resources. As identified in the **Resource** column, all of these resources are on the **localhost** AdminServer. The alert ID numbers (**ID**) and severity (**Severity**) are also provided.

Enter the following command for a list of alerts for all OpenEdge server resources:

```
fathom -alertlist -restype openedge
```

You see any alerts that exist for any OpenEdge server resources (**openedge**) listed. If there are no existing alerts, you receive the message shown below.

**Figure 14: -alertlist for openedge resource type**



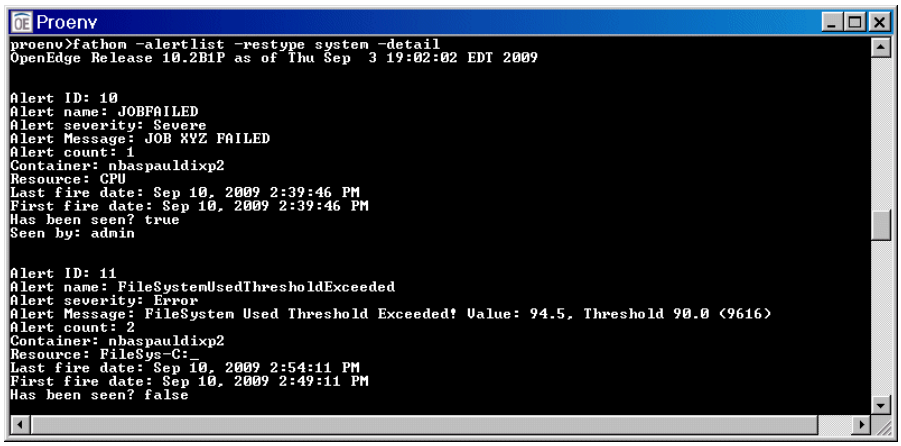

To see specific details about the alerts that exist for system resources, use either the `-detail` option or the `-verbose` option.

Enter the following command to examine the results of using the `-detail` option:

```
fathom -alertlist -restype system -detail
```

The details appear, as shown below.

**Figure 15: -alertlist command used with -detail option**

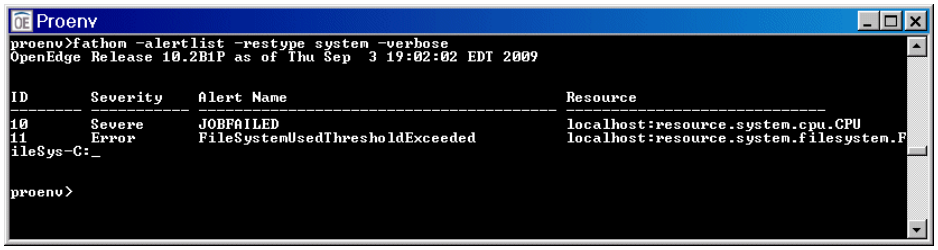



Enter the following command to examine the results of using the `-verbose` option:

```
fathom -alertlist -restype system -verbose
```

The details appear, as shown below.

**Figure 16: -alertlist command used with -verbose option**




# Fire an alert (firealert)

## Description

Fires an alert in OpenEdge Management.

## Syntax

```
fathom -firealert [alertmessage]
```

OpenEdge Management also supports generation of application-specific alerts. In your application, you can send alerts to OpenEdge Management using the `-firealert` options.

### Example

To fire an alert for a CPU resource, you can use the following command:

```
fathom -firealert JOBFAILED -resource CPU -msg 'JOB XYZ FAILED'
```

To view the alert details of a CPU resource, you can use the following command:

```
fathom -alertlist -detail -resource CPU
```

# Dump configuration database (dump)

### Description

Dumps the configuration database.

You can dump either the OpenEdge Management 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.

### Syntax

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

The resulting file will be in XML format and contains 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.

### Example

You can also use the `-httpport` switch, as follows, to identify the port of the OpenEdge Management web server:

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

Where `<filename>` is the name of the xml file created, which contains the dumped contents of the configuration database and `<port-number>` is the port on which OpenEdge Management is running. The default port number is `9090`.

If the `<port-number>` is not specified, the Proenv utility uses the current port number mentioned in the `catalina.properties` file located in the `$OEMGMT/conf` folder.

# Load configuration database (load)

## Description

Loads the configuration database using the dump file.

**Note:** OpenEdge Management must be offline when you run the `-load` command.

## Syntax

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

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

# List resources (reslist)

## Description

Displays the list of OpenEdge Management resources.

## Syntax

```
fathom -reslist option
```

`-user`

(Optional) The username for OpenEdge Management. Progress recommends specifying this switch. If this switch is not specified, the utility uses the current username of your machine.

`-password`

(Optional) The password for the username you provided. Using this switch in the command might allow others to see your password in cleartext. So, Progress recommends specifying the password only when prompted.

**Table 17: Command-line options for viewing resource list**

| Option syntax | Description |
|---|---|
| `-container <container-name>` | Displays the list of resources for that container. |
| `-restype <resource-type>` | Displays all the resources that belong to a resource type: `database`, `file`, `network`, `openedge`, or `system`. |

**Note:** Ensure that you specify only one option, either `-container` or `-restype`, when using this command. Specifying multiple options results in an error.

### Example

The following command is an example to retrieve the list of available database resources:

```
fathom -reslist -user admin -restype database
```

# Initialize new database (initcachedb)

### Description

Allows for faster creation of cache database. This deletes the existing database, disables the `.wal` file, and then recreates the database. Turning off the `.wal` file reduces the writes to disk significantly.

### Syntax

```
fathom -initcachedb -help
```

### Example

The following command is an example to create the cache database using the `-initcachedb` command. This prints a message with help indicating that the new graph cache will be created.

```
fathom -initcachedb -help
```

# Index


## A

Adding a new user *56*
Admin password
  entering *35*
  updating *35*, *58*
Administrator users *55*
AdminServer
  remote *19*, *48*
  viewing the contents of *45*
Alert list
  command options *108*
  examples *108*
Alerts
  clearing
    from the command line *103*
Authentication Configuration *63*

## B

Browser support *14*

## C

Clearing alerts
  in the command line *103*
Command-line interface
  clearing alerts *103*
Commands
  alertlist
    additional options *108*
    group selection options *107*
  firealert *112*
  fully qualified resource key *108*
Configuration process
  establishing values
    on the Getting Started page *38*
    on the OpenEdge Explorer Configuration page *35*
    on the OpenEdge Management Configuration page *35*
  initial configuration options *33*, *35*
  specifying and initially changing the admin password *35*
Configuring
  OpenEdge Explorer *33*
  OpenEdge Management
    before you begin *31*
    completing *33*
    initial options for *35*
Configuring *(continued)*
  OpenEdge Management for remote monitoring and property configuration *47*
CPU requirements *25*

## D

Dashboard page *13*
Database Migration Utility
  adding a managed database page by using *39*
Databases
  managed *38*
  scripted *38*
Deleting users *58*
Deploying OpenEdge Management
  on a single host *17*
  on multiple hosts *18*
  strategy for *24*
Detail control bar *13*
Detail menu *13*, *43*
Disabled status *44*
Disabling
  OpenEdge Management *50–51*

## E

E-mail server *37*

## F

Fail status *44*

## G

Getting Started page
  defining options for file systems and disks *40*
  managed and unmanaged databases *38*

## H

HTTPS protocol
  using with OpenEdge Management *83*, *96*

## I

Inactive status *44*
Installation
  OpenEdge product support for *14*
  trending databases *31*

## L

List control bar *13*

## M

Managed and scripted databases
adding *38*
defined *38*
Managed databases
monitoring *23*
Management console
accessing *13*
and logging on to OpenEdge Management *13*
detail control bar *13*
detail menu *13*
list control bar *13*
main screen area *13*
menu bar *13*
resource statuses in *44*
using *13*
using to start OpenEdge Management *13*
Memory requirements *26*
Menu bar *13*, *43*
Monitoring remote OpenEdge Management resources *20*, *47*, *52*, *66*
Monitoring resources *31*

## N

Not Checked status *44*
Not Running status *44*

## O

Offline status *44*
OpenEdge Authentication Gateway Authentication *63*
OpenEdge Management
configuring
before you begin *31*
deployment *16*, *18*
getting started *28*
OpenEdge Management Configuration page
accessing during the configuration process *34*
admin password *35*
submitting *37*
OpenEdge Management Trend Database
optionally configuring *27*
Operator users
Customizing operator role *58*
Managing access to DAC *59*

## P

Pass status *44*
Password
when logging on *34*

## R

Reglue
running *51*
Remote AdminServer
setting up *52*
Remote configuration
setting up *52*
Remote monitoring
and configuration *47*
configuring *47*
setup verification *52*
Requirements
CPU and memory *25*
Resource statuses *44*
Resources
detail menu *43*
menu bar *43*
Resources to monitor *31*

## S

Scripted databases
monitoring *23*
SMTP_MAIL network resource monitor *37*
Startup options
default alert operator *37*
e-mail server *37*
Status indicators *44*
System
architecture
agents *16*
console *16*
database *16*
performance *31*
requirements *14*
System Activity report *45*
System information report *45*

## T

Trending databases *31*

## U

Unglue
running *50–51*
User information
adding *56*
changing password *57*
changing the admin password *58*
deleting *58*

User information *(continued)*
establishing *55*
maintaining *55*
User name
when logging on *34*
Users
adding *56*
administrators *55*
Users *(continued)*
deleting *58*
operators *55*

## W

Web Server Authentication *63*