



HP Agile Manager

Software Version: 2.10

Installation and Administration Guide

Document Release Date: December 2014
Software Release Date: August 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2012-2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

Welcome to Agile Manager	7
Overview	8
System architecture	10
Agile Manager components	10
Basic configuration example	12
Clustered configuration example	13
System requirements	14
Linux prerequisites	16
Linux disk space requirements	16
Linux server required permissions	17
Install as a non-root user	17
Oracle prerequisites	19
Database requirements	19
Grant administrative user privileges	21
Enable Oracle RAC Support	24
Pre-installation checklist	27
Installation types	29
Install a clustered system	30
Upgrade your system	32
Recommended upgrade configuration	33
Upgrade Agile Manager	33
Install Agile Manager	36

- Connect to Oracle RAC 48
- Start/Stop the Agile Manager service 50
- Log in to Agile Manager 52
- Secure your system 53
 - Secure deployment 54
 - Secure attachment files 55
 - Secure the application server 55
 - Secure the network and communication 57
 - Secure system administration 60
 - Secure user authentication 60
 - Secure user authorization 61
 - Data integrity 62
 - Data encryption 63
 - Data logging 65
 - Configure an SSL connection 67
 - Integrate an Apache web server (example) 71
- Manage the application server 74
 - Change the heap memory size 74
 - Change the application server port number 75
 - Change the system administration schema password 75
 - Application server management tools 76
- Uninstall Agile Manager 78
- Troubleshooting 79
- Agile Manager system administration 81
 - Server settings 81
 - Configure application logs 82

Configure database settings	84
Configure an email notification server	85
System and user settings	85
Configure miscellaneous system settings	85
Define security settings	86
Define repository attachment settings	86
Define report settings	86
Update user licenses	87
Configure user authentication	88
Define system administrators and reset user passwords	90
System administrators	90
User passwords	91
Configure advanced parameters	91
Send Documentation Feedback	92

Welcome to Agile Manager

Agile Manager is an agile management solution for organizing, planning and executing agile projects. It can support single teams or multiple, geographically distributed teams across an enterprise. Agile Manager provides:

- A drag-and-drop interface that enables easy release and sprint planning, task allocation, and capacity management across teams and individuals
- Task and release planning boards that give all team members ready insight into the entire project landscape, the flow of work, and potential issues or bottlenecks
- Real-time feedback on progress through highly customizable dashboards, metrics, and KPIs, minimizing administration while increasing predictability
- Advanced development analytics that aggregate source code and build information to surface meaningful insights into application changes, allowing for precise risk analysis and more informed decisions

Overview

This document describes the components and supported architectures for an on premise Agile Manager system, as well as procedures for installing the application, managing your servers, and performing system administration tasks.

For details about how to use Agile Manager, see the *Agile Manager Help Center*, available from the application Help menu.

This document includes the following information:

- **"System architecture" on page 10.** Describes system components in basic and clustered configurations.
- **"Linux prerequisites" on page 16.** Describes requirements for the Linux application servers and related procedures.
- **"Oracle prerequisites" on page 19.** Describes requirements for the Oracle database servers and related procedures.
- **"Pre-installation checklist" on page 27.** Lists the details you will need to supply during installation and should have available before you begin.
- **"Installation types" on page 29.** Describes the types of installation procedures described in this guide.
- **"Install a clustered system" on page 30.** Describes the high level steps required to install the system in a clustered configuration.
- **"Upgrade your system" on page 32.** Describes the recommendations and steps for upgrading your Agile Manager to a new version.
- **"Install Agile Manager" on page 36.** Describes how to install your Agile Manager system.
- **"Start/Stop the Agile Manager service" on page 50.** Lists commands for starting and stopping the Agile Manager service.
- **"Log in to Agile Manager" on page 52.** Describes how to access Agile Manager and the Agile Manager Administration site after installation is complete and the server is started.

- **"Secure your system" on page 53.** Describes best practices and procedures for securing your Agile Manager system.
- **"Manage the application server" on page 74.** Describes optional procedures that are performed after installation to manage your Linux server.
- **"Uninstall Agile Manager" on page 78.** Describes how to uninstall Agile Manager.
- **"Troubleshooting" on page 79.** Describes the log files you should check if you encounter errors during your installation.
- **"Agile Manager system administration" on page 81.** Describes how to configure servers, users, and other system settings.

System architecture

This chapter describes the supported Agile Manager system architectures and system components.

- ["Agile Manager components" below](#)
- ["Basic configuration example" on page 12](#)
- ["Clustered configuration example" on page 13](#)
- ["System requirements" on page 14](#)

Agile Manager components

The following table describes the Agile Manager system components.

Component	Description
Agile Manager application server	Hosts the Agile Manager application and web server, and runs on a Linux platform.
Database server	<p>Stores the following Agile Manager schemas:</p> <ul style="list-style-type: none">• System Administration schema. Stores information related to the Agile Manager system, such as users and mail notification settings.• Site schema. Stores all site information, such as workspaces, backlog items, and release details. <p>The schemas reside on an Oracle server. For details, see "Oracle prerequisites" on page 19.</p>

Component	Description
Firewall	Optional. For increased security, place a firewall between the Web browser (the Agile Manager client) and the Agile Manager application server.
LDAP server	Optional. Used when authenticating users via your LDAP system instead of creating users directly in Agile Manager. LDAP configuration is performed via the Administration site, after installation. For details, see " Configure user authentication " on page 88.
Load balancer	For use in a clustered configuration. When working with a load balancer, client requests are transmitted to the load balancer and distributed according to server availability within the cluster.
Mail server	Used to send mail notifications to users.
Site repository	Stores site files, such as attachments. By default, the repository is located on the same machine as the application server. This is useful for smaller setups. <ul style="list-style-type: none"> • For larger organizations, it is <i>advisable</i> to install the repository on a dedicated machine. • In clustered configurations, it is <i>required</i> to install the repository on a dedicated machine.
Synchronizer server	Optional. Used for ALM Synchronizer for Agile Manager application. Communicates with ALM, via the OTA API.
Tanuki wrapper	A Java service wrapper that allows Agile Manager to be installed and controlled like a native Windows Service. It also includes advanced fault detection software to monitor Agile Manager.
Web browser	The Agile Manager web client provides access to the Agile Manager application and Administration site.

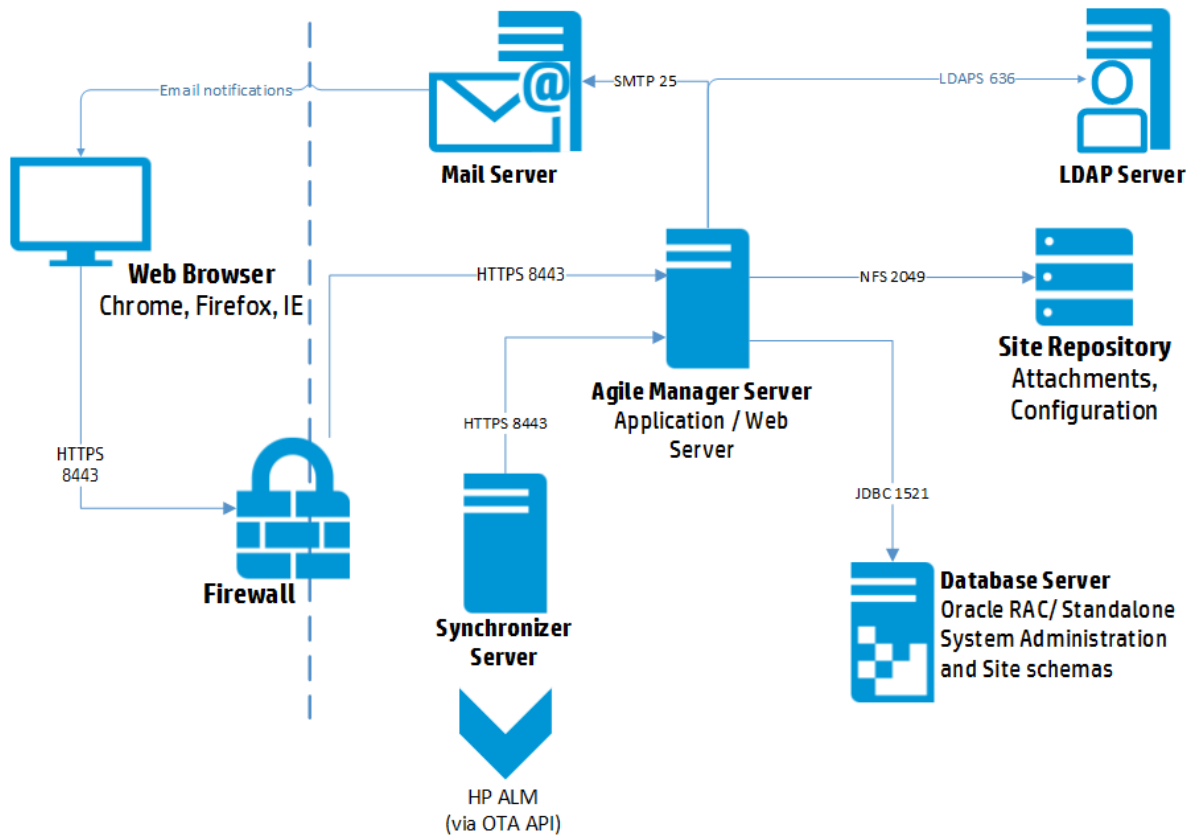
Note: To improve system performance, install the Agile Manager application and

database servers on separate machines, connected over a LAN network.

Basic configuration example

In the basic Agile Manager configuration, the Agile Manager application server and the web server are embedded with the installation, and installed on the same machine.

The following diagram illustrates a basic Agile Manager system configuration.



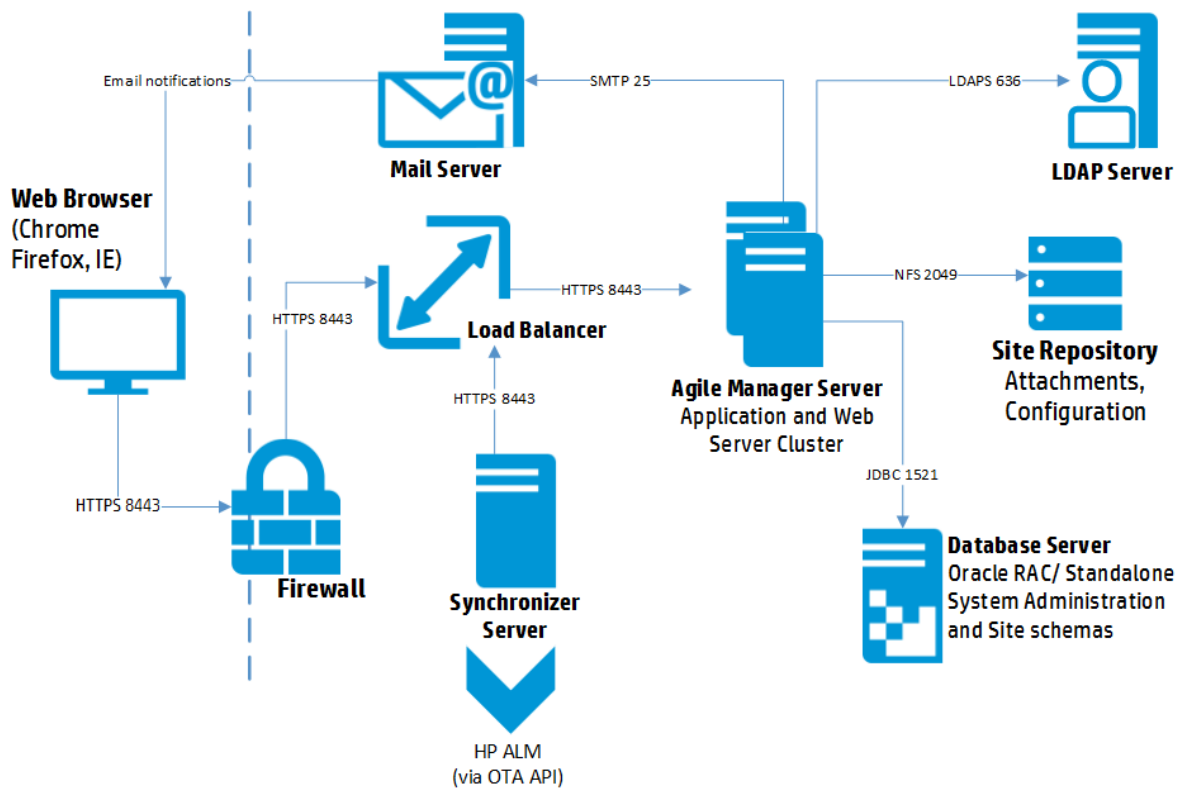
For more details, see "[Agile Manager components](#)" on page 10 and "[Install Agile Manager](#)" on page 36.

Clustered configuration example

Agile Manager supports clustering. A cluster is a group of application servers that run as if they were a single system. Each application server in a cluster is referred to as a node.

Clusters provide mission-critical services to ensure maximum scalability. The load balancing technique within the cluster is used to distribute client requests across multiple application servers, making it easy to scale to a large number of users.

The following diagram illustrates a clustered Agile Manager system configuration.



For more details, see ["Agile Manager components"](#) on page 10 and ["Install a clustered system"](#) on page 30.

Consider the following in a clustered environment:

Cluster considerations	
Operating system version	Each node must use the same operating system version, including all patches, updates, or hot fixes.
Agile Manager version	Each node must use the same version of Agile Manager.
System administration database schema	All nodes must point to the System Administration database schema.
Shared resources	<p>All nodes must have access to:</p> <ul style="list-style-type: none"> • All database servers • The System Administration database schema • The site repository <p>By default, the repository is located on the first node in the cluster, and therefore all other nodes must have access to the first node. If you install the repository on a dedicated machine, each node must have access to that machine.</p>

System requirements

Note: Agile Manager can be installed on any virtual machine that has the necessary system requirements.

Hardware Minimum Requirements	
CPU	Linux® Quad Core AMD64 processor or equivalent x86 compatible processor
Memory (RAM)	8 GB minimum

Free disk space	16 GB minimum
Application Server Requirements	
TCP Port	8080 must be free, or 8443 for secure connections
Database Server Requirements	
Database size	<ul style="list-style-type: none"> • Without ALI. 50 MB initial size; average projects may eventually reach 1 GB or more • With ALI. 5 GB initial size <p>Size requirements will vary between projects. Size depends on the number of backlog items expected in the system, and the number of changes expected each day.</p> <p>If you plan on configuring ALI, size also depends on the number of builds per day, the number of commits, and the number of files.</p>
Supported Environments	
Operating system	Red Hat Enterprise Linux 6.2 or 6.3 (64 Bit) SUSE Linux Enterprise 11 Service Pack 3
Database	Oracle 11.2.0.3
Client Machines	
Supported browsers	<p>Chrome 23 and above</p> <p>Firefox 16 and above</p> <p>Internet Explorer 9 and 10</p> <p>Note: If you are using Internet Explorer 9, make sure that the Chrome Frame plug-in is disabled.</p>
Screen resolution	1680x1050 (recommended) or 1024x768

Linux prerequisites

This chapter describes the following prerequisites for your Linux application server:

["Linux disk space requirements" below](#)

["Linux server required permissions" on the next page](#)

By default, the Agile Manager installer requires a **root** user. You can also install as a non-root user with sudo permissions. For details, see ["Install as a non-root user" on the next page](#).

See also:

- ["System requirements" on page 14](#)
- ["Oracle prerequisites" on page 19](#)
- ["Pre-installation checklist" on page 27](#)

When you're ready to install, continue with ["Install a clustered system" on page 30](#) or ["Install Agile Manager" on page 36](#).

Linux disk space requirements

Verify that your server machine meets the Agile Manager disk space requirements listed in ["System requirements" on page 14](#).

The **/<root>/opt/HP** directory requires at least enough free space to accommodate the size of Agile Manager after it has been installed, as well as any files created during operation. This directory should have approximately 5 GB of free space.

Verify disk space using the following command:

```
df -h
```


Linux server required permissions

You must have the following permissions to install Agile Manager on a Linux server machine:

Administrator user permissions

- You must be logged on as a local or domain user with administrator permissions.
- Your user name cannot include a pound sign (#) or accented characters (such as ä, ç, or ñ).
- By default, the Agile Manager installer requires a **root** user.

If you are unable to install Agile Manager using the **root** user for security reasons, speak to your system administrator about installing as a non-root user with sudo permissions. For more details, see ["Install as a non-root user" below](#).

Note: Some environments, such as by default in SUSE, you will still need to provide the **root** user password.

File directory permissions

You must have full read and write permissions for the `/opt/hp/agm` directory and all files and folders underneath it.

If the file repository is located on a remote machine:

- On the file server machine, share the file repository directory so that the user running the installation is the owner of the files.
- On the Agile Manager machine, or on each cluster node, create a mount directory that points to the file repository directory.

Install as a non-root user

By default, the Agile Manager installer requires a **root** user.

If you are unable to install Agile Manager using the **root** user for security reasons, speak to your system administrator about installing as a non-root user with sudo permissions.

Notes:

- The sudo package is included by default on some systems. These instructions assume that sudo is installed on the target machine. If sudo is not included by default, it can be downloaded and installed from <http://www.gratisoft.us/sudo/download.html>.
- Installing Agile Manager as a non-root user *without* sudo permissions is not supported and causes installation problems.
- Some environments, such as by default in SUSE, you will still need to provide the **root** user password.

1. Create a new user group: `groupadd agmadmins`
2. Create a new user: `useradd agmadmin`
3. Add the user to the group: `usermod -G agmadmins agmadmin`
To verify, run: `id agmadmin`
4. If required, change the new user's password: `passwd agmadmin`
5. Grant the new user root user permissions. Add the following line to the **sudoers** file: `agmadmin ALL=(ALL) ALL`
6. Continue with "[Install Agile Manager](#)" on page 36, running the rpm file as the sudo user.

See also:

- "[Install a clustered system](#)" on page 30
- "[Oracle prerequisites](#)" on the next page
- "[Pre-installation checklist](#)" on page 27

Oracle prerequisites

This chapter describes prerequisites required for your Oracle database server.

["Database requirements" below](#)

["Grant administrative user privileges" on page 21](#)

["Enable Oracle RAC Support" on page 24](#)

Use Oracle RAC when working with multiple Oracle instances to enhance Oracle database availability and scalability.

See also:

- ["System requirements" on page 14](#)
- ["Linux prerequisites" on page 16](#)
- ["Pre-installation checklist" on page 27](#)

When you're ready to install, continue with ["Install a clustered system" on page 30](#) or ["Install Agile Manager" on page 36](#).

Database requirements

Before connecting Agile Manager to an Oracle database server, verify the following:

Requirement	Description
Database connection	<ul style="list-style-type: none">• Connection to the database server• DNS resolution <p>Tip: Test the DNS resolution by pinging the database server.</p>

Requirement	Description
Database size	<ul style="list-style-type: none"> • Without ALI. 50 MB initial size; average projects may eventually reach 1 GB or more • With ALI. 5 GB initial size
Charset	<ul style="list-style-type: none"> • Set the database charset to AL32UTF8. • Set the following parameter value: NLS_LENGTH_SEMANTICS=CHAR
Database column length semantics	<p>Column length must be defined according to characters, and not according to bytes.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: Agile Manager uses the UNICODE character set, which sometimes requires more than 1 byte for each character. Define the column length by character to ensure that each column has the required length.</p> </div>
Tablespace name and size	<ul style="list-style-type: none"> • The tablespace names: <ul style="list-style-type: none"> Default. qc_data Temporary. temp • The minimum tablespace sizes for storing the System Administration database schema. Initial requirements are: <ul style="list-style-type: none"> qc_data. 20 MB temp. 50 MB • The tablespace must not be locked.

Requirement	Description
Clustered configuration or upgrade	<p>To install Agile Manager on a second node in a clustered configuration, or when upgrading:</p> <ul style="list-style-type: none">• The existing database schema name and permissions to connect Agile Manager to the database server.• Full read/write permissions on the existing repository.• Access to the previous system administration schema repository path. The Agile Manager user must have full read/write permissions to this path.• The confidential data passphrase that was used to create the existing schema.

Grant administrative user privileges

The installing database user must have sufficient permissions to perform certain administrative tasks in Oracle. For example, these tasks include creating the Agile Manager site user schema, copying data between projects, and checking that there is sufficient storage in a specific tablespace.

Note: If you are unable to use the Oracle system user due to security reasons, it is recommended that your database administrator create an Agile Manager administrator user, for example **agm_admin**, with the specific privileges required to install Agile Manager.

Run the following script on the Oracle database server, as the SYSDBA user, to grant the required database administrative user and role.

For details, see ["User privileges" on the next page](#).

```
--drop user agm_admin cascade;  
--drop role agm_admin_role;  
create user agm_admin identified by agm_admin
```

```

default tablespace qc_data
temporary tablespace temp
quota unlimited on qc_data;
grant CTXAPP to agm_admin WITH ADMIN OPTION;
create role agm_admin_role;
grant CREATE ANY SYNONYM to qc_admin_role;
grant agm_admin_role to agm_admin WITH ADMIN OPTION;
grant CREATE SESSION to agm_admin_role WITH ADMIN OPTION;
grant CREATE USER to agm_admin_role;
grant DROP USER to agm_admin_role;
grant CREATE TABLE to agm_admin_role WITH ADMIN OPTION;
grant CREATE VIEW to agm_admin_role WITH ADMIN OPTION;
grant CREATE TRIGGER to agm_admin_role WITH ADMIN OPTION;
grant CREATE SEQUENCE to agm_admin_role WITH ADMIN OPTION;
grant CREATE PROCEDURE to agm_admin_role WITH ADMIN OPTION;
grant SELECT ANY TABLE to agm_admin_role WITH ADMIN OPTION;
grant INSERT ANY TABLE to agm_admin_role;
grant SELECT ON DBA_FREE_SPACE to agm_admin_role;
grant SELECT ON SYS.DBA_TABLESPACES to agm_admin_role;
grant SELECT ON SYS.DBA_USERS to agm_admin_role;
grant SELECT ON SYS.DBA_REGISTRY to agm_admin_role;
grant SELECT ON SYS.DBA_ROLES to agm_admin_role;
  
```

User privileges	
CREATE ANY SYNONYM WITH ADMIN OPTION (1)	Required to view an object in a different schema without using the <owner.> prefix.

User privileges	
CREATE PROCEDURE WITH ADMIN OPTION (1)	Required to create stored packages for an Agile Manager site. Agile Manager uses packages to collect change history for specific tables.
CREATE SEQUENCE WITH ADMIN OPTION (1)	Required to create sequences for an Agile Manager project.
CREATE SESSION WITH ADMIN OPTION (1)	Required to connect to the database as the Agile Manager database administrative user.
CREATE TABLE WITH ADMIN OPTION (1)	Required to grant this permission to a newly created Agile Manager site user schema.
CREATE TRIGGER WITH ADMIN OPTION (1)	Required to create triggers for an Agile Manager project. Agile Manager uses database triggers to collect change history for specific tables.
CREATE USER	Required to create a new system user schema when creating a new Agile Manager site .
CREATE VIEW WITH ADMIN OPTION (1)	Required to create views for an Agile Manager site.
CTXAPP ROLE WITH ADMIN OPTION (1)	Enables Agile Manager to use the Oracle text searching feature. This role exists only if the Oracle text search component was installed and enabled on the database server.
DROP USER	Required to remove a System Administration database schema.
SELECT ANY TABLE WITH ADMIN OPTION (1) and INSERT ANY TABLE	Required to enhance performance when restoring a site.

User privileges	
SELECT ON DBA_FREE_SPACE (2)	Required to check free space on the database server prior to creating a new System Administration database schema or a new site.
SELECT ON SYS.DBA_REGISTRY (2)	Required to verify that the text search component is installed on the database server.
SELECT ON SYS.DBA_ROLES (2)	Required to verify that the text search role (CTXAPP) is installed on the database server.
SELECT ON SYS.DBA_TABLESPACES (2)	Required to collect a list of tablespaces that exist on the database server prior to creating a new System Administration database schema or a new site.
SELECT ON SYS.DBA_USERS (2)	Required to verify the existence of specific database site users. For example, you might want to verify the existence of an Oracle CTXSYS user before creating a new Agile Manager site.

Note:

- (1) The Agile Manager admin user must have privileges with **Admin Option**.
- (2) The **SELECT ON SYS.*** privileges can be given directly by the table owner, or through a database application role. To avoid giving these privileges each time, you can grant this role to the Agile Manager admin user. The recommended name for this role is **AGM_SELECT_ON_SYS_OBJECTS**.

Enable Oracle RAC Support

Use Oracle RAC to enhance Oracle database availability and scalability, allowing it to interact with more than one database instance.

Agile Manager RAC support includes load balancing between Oracle instances, and failover between all specified Oracle RAC nodes at the initial connection.

Note: TAF (Transparent Application Failover) is *not* supported.

A user failing to complete a request after an Oracle instance crash is required to perform the activity again with a working Oracle instance.

To enable Oracle RAC support:

1. Verify that the **tnsnames.ora** file is saved on your Agile Manager server.

This file should contain Oracle database addresses, similar to the examples below:

- ["RAC TNS Alias using all cluster nodes in the ADDRESS sub-section" below](#)
- ["RAC TNS Alias using Single Client Access Name \(SCAN\)" below](#)

2. Verify that you have the address of the TNS server to which Agile Manager should refer, for example, OrgRAC.

For details about connecting to Oracle RAC after installing Agile Manager, see ["Connect to Oracle RAC" on page 48](#).

Examples:

RAC TNS Alias using all cluster nodes in the ADDRESS sub-section

This example also utilizes the Load balance and Failover features.

```
OrgRAC =
(DESCRIPTION =
  (ADDRESS_LIST=
    (FAILOVER = on)
    (LOAD_BALANCE = on)
    (ADDRESS= (PROTOCOL = TCP)(HOST = server1)(PORT = 1521))
    (ADDRESS= (PROTOCOL = TCP)(HOST = server2)(PORT = 1521))
    (ADDRESS= (PROTOCOL = TCP)(HOST = server3)(PORT = 1521))
  )
  (CONNECT_DATA=
    (SERVICE_NAME = myrac.yourcompany.com)
  )
)
```

RAC TNS Alias using Single Client Access Name (SCAN)

This example enables Oracle 11gR2 clients to connect to the database with the ability to resolve multiple IP addresses, reflect multiple listeners in the cluster, and handle public client connections.

Installation and Administration Guide

Oracle prerequisites

```
OrgRAC_Scan =  
(DESCRIPTION =  
  (ADDRESS_LIST=  
    (FAILOVER = on)  
    (LOAD_BALANCE = on)  
    (ADDRESS= (PROTOCOL = TCP)(HOST = myrac-cluster-scan)(PORT = 1521))  
  )  
  (CONNECT_DATA=  
    (SERVICE_NAME = myrac.yourcompany.com)  
  )  
)
```

For more information on working with RAC SCAN, refer to the Oracle documentation.

Pre-installation checklist

Review and verify the following checklist before installing Agile Manager. This checklist outlines the information that you must have available during the installation process.

Caution: Always change default passwords to secure your system.

For a list of the supported system environments, see ["System requirements" on page 14](#). More details and optional pre-installation procedures are described in ["Linux prerequisites" on page 16](#) and ["Oracle prerequisites" on page 19](#).

Pre-installation checklist	
Clusters	Cluster host names Required only if you are using a clustered configuration.
Encryption passphrase	Confidential data passphrase Default. Seashells Grow Like Misty Tunas In a cluster, you will use the same passphrase on all nodes. Note: Make a note of the passphrase you use for support calls.
Database server	Database. Host name, port, system identifier (SID), and administrator user name and password. The Oracle SID identifies the specific Oracle instance on the Oracle server host machine. For Oracle RAC: The tnsnames.ora file with connection string, as well as database administrator username and password Tablespace. Default tablespace selection.

Pre-installation checklist	
System Administration	<p>System administration</p> <p>System administration password. The default password is empty. You can modify this password during installation.</p> <p>The default system administrator user name is sa. This cannot be changed. You can later define additional users as system administrators in the Agile Manager Administration site (Configuration > Users). For details, see "Define system administrators and reset user passwords" on page 90.</p> <p>System administration database schema</p> <p>System administration database schema user name and password.</p> <p>The default System Administration database schema name is agm_siteadmin_db, and the default password is tdtdtd. You can modify both of these defaults during installation.</p>
Site repository	<p>Repository path</p> <ul style="list-style-type: none">• By default, the repository is configured in the deployment folder. It is recommended to modify this default to a different location.• The user who installs Agile Manager must be the owner of the repository folder.

Installation types

This guide describes the following types of installation procedures:

- **Clustered installation.** When installing a clustered system, you'll need to install Agile Manager on each node in the cluster. Start with "[Install a clustered system](#)" on [the next page](#), and then continue in "[Install Agile Manager](#)" on [page 36](#) as directed for clustered installations.
- **Upgrading installation.** When upgrading your system, you'll need to follow steps and perform prerequisites specific to upgrades. Start with "[Upgrade your system](#)" on [page 32](#), and then continue in "[Install Agile Manager](#)" on [page 36](#) as directed for upgrades.
- **Standalone, first-time installation.** If you are installing Agile Manager on a standalone system for the first time, go directly to "[Install Agile Manager](#)" on [page 36](#).

Install a clustered system

This section describes the high-level steps in configuring a clustered Agile Manager system. Before starting, verify that your server nodes fulfill the Linux and Oracle server prerequisites. For details, see ["Linux prerequisites" on page 16](#) and ["Oracle prerequisites" on page 19](#).

1. Unpack the installation files on all nodes. For details, see the following steps:
 - ["Mount the site repository \(clusters only\)" on page 36](#)
 - ["Deploy the installation files" on page 36](#)
2. Create a shared folder, accessible for all nodes.
3. On one of the nodes, install Agile Manager. Continue the installation procedure on that node as described in the step entitled ["Open the directory in which the Agile Manager files are deployed" on page 37](#).

When defining the repository path, select the shared folder you created earlier.

4. After the wizard is complete, copy the `/opt/hp/agm/conf/qcConfigFile.properties` file from the server where you installed and configured Agile Manager to the same folder on all other nodes.
5. On each of the other nodes in the system, install Agile Manager. On each node, continue with the step entitled ["Open the directory in which the Agile Manager files are deployed" on page 37](#).

During installation, do not change any of the settings except for selecting the following options:

- **Keep all current settings.** For details, see ["Run the configuration wizard" on page 37](#)
 - **Connect to an existing schema/second node.** For details, see ["Select a database schema option" on page 40](#).
6. After completing the installation and configuration wizard on all nodes, access the Agile Manager Administration site. On the **Servers > Application** page, verify that

all of your application servers are displayed correctly.

For details, see ["Log in to Agile Manager" on page 52.](#)

Upgrade your system

Agile Manager includes several components, as described in "[System architecture](#)" on [page 10](#). When planning your installation and upgrade strategy, decide whether to install the new system on new components, or to reuse components from the existing system.

It is strongly recommended that you install the system on a set of completely new components, and restore your site to the updated system.

This produces two functioning Agile Manager systems: the original, which can open and work with an existing site, and the new system, to which existing projects will be upgraded. For details, see "[Recommended upgrade configuration](#)" on the [next page](#).

Installing the updated system on new components helps to avoid the following possible problems:

- **Unnecessary downtime** required to restore a backup if the site is corrupted before the upgrade is completed.
- **Repeated upgrades.** If you install the new version on the same server as the existing version, you must first uninstall the existing version. If you later discover a problem with the repository, you may require the original Agile Manager server to repair it.

This would require you to uninstall the new version and reinstall the old version in order to fix the problem, and then perform the upgrade again.

Continue with "[Upgrade Agile Manager](#)" on the [next page](#).

Note: If users are logged into Agile Manager during an upgrade, they may need to refresh their browsers to continue working after the upgrade is complete.

Recommended upgrade configuration

The following table lists recommendations for Agile Manager system components when installing the upgrade on a separate system, as recommended.

Agile Manager application server	Do not install the new version of the application server on the same machine where the existing application server is installed. Instead, install the updated version on a separate machine.
Database server	Install an updated version of the database schema on a separate machine, or create a new instance of the existing schema on the machine on which it is currently installed.
Site repository	Create a copy of the existing repository to be used by the new system.

Back up the database schema and site repository

We strongly recommend that you deactivate your site before backing it up. If you must back up while your site is still active, you must first back up the database, and only after back up the file system. We also recommend backing up the file system as soon as possible after backing up the database.

Upgrade Agile Manager

This section describes how to upgrade Agile Manager.

- 1. Copy the database schemas to the new system.**
 - a. Before installing the updated system on separate components as recommended, restore a backup or a copy of the following schemas to the new database schema or instance:

- System administration schema
- Site schema

For details about these schemas, see ["Agile Manager components" on page 10](#).
For assistance in copying the schemas, contact your database administrator.

b. Update the following columns in the PROJECTS table to their new values:

- PHYSICAL_DIRECTORY
- DBSERVER_NAME
- DB_CONNSTR_FORMAT
- DB_USER_PASS

Note:

- The database user must have the same permissions as the user installing Agile Manager.
- If you used a staging environment in the previous version, ensure that the existing site refers to the *production* site database and shared repository.

2. Verify the system requirements and server prerequisites.

Verify that your server nodes fulfill the Linux and Oracle server prerequisites in case of any changes since the previous version.

For details, see ["System requirements" on page 14](#), ["Linux prerequisites" on page 16](#), and ["Oracle prerequisites" on page 19](#).

3. Uninstall the previous version of Agile Manager.

For details, see ["Uninstall Agile Manager" on page 78](#).

After uninstalling, rename the **qcConfigFile.properties.rpmsave** file to **qcConfigFile.properties**. This enables you to use the same configuration settings as you used in the previous installation.

The **qcConfigFile.properties.rpmsave** file is located in the **/opt/hp/agm/conf/** directory.

4. Install and configure the new version of Agile Manager.

Go through the installation wizard, using the same configuration details as you used in the previous installation, except for the following:

In the **System Administration Database Schema** screen, select one of the following:

Option	Description
Upgrade a copy of the existing schema	Automatically connect to the existing Agile Manager site and start production work in the new version right away.
Upgrade a copy of the system administration schema for staging	Create a blank site in the new version to use as a staging environment. You will need to manually connect to the production environment later on. This option does not connect the original projects to the new environment. It only creates a new, upgraded environment that you can use for staging.


For details, see ["Install Agile Manager" on the next page](#).

5. **Move a production site to the upgraded environment.**

If you selected ["Upgrade a copy of the system administration schema for staging" above](#), do the following when you are ready to move your production site to the upgraded environment:

- a. Log in to the Agile Manager Administration system:

```
http://<serverName>:<port>/agm/admin
```

- b. Navigate to the **Servers > Database** page.
- c. Use the **Restore Site Schema**  option to connect to your production site. For details, see ["Restore a site schema" on page 84](#).

Install Agile Manager

This section describes how to install and configure Agile Manager.

- For high level instructions for installing a clustered system, see ["Install a clustered system" on page 30](#) and the considerations in ["Clustered configuration example" on page 13](#). For prerequisites and recommendations for upgrading, see ["Upgrade your system" on page 32](#).
- If you would like to install and connect to Oracle RAC to enhance Oracle database availability and scalability, see ["Connect to Oracle RAC" on page 48](#).
- If you encounter problems during the installation process, see ["Troubleshooting" on page 79](#) for suggestions.

Note: If you have uninstalled Agile Manager and want to reinstall using the same settings you used before, be sure to rename the `qcConfigFile.properties.rpmsave` file to `qcConfigFiles.properties`. For details, see ["Uninstall Agile Manager" on page 78](#).

1. Mount the site repository (clusters only)

In a clustered configuration, mount the site repository before installing. The mount should not use any cache mechanisms. For details, contact your network administrator.

All nodes must mount the shared file server with the same mount name. For example, if the file server is `some.server.org`, and it is mounted on `/mnt/some_server` on the first node, it should be mounted with `/mnt/some_server` on all nodes.

2. Deploy the installation files

Copy the rpm and `hpPublicKey2048.pub` files provided in the installation package to the `tmp` folder, or any other accessible folder.

Navigate to the directory where the rpm file is stored and run one of the following:

As root user	<pre>rpm --import hpPublicKey2048.pub rpm -i AGM-ONPREM<version number>.rpm</pre>
As sudo user	<pre>sudo rpm --import hpPublicKey2048.pub sudo rpm -i AGM-ONPREM<version number>.rpm</pre>

The installation files are deployed under **/opt/hp/agm**.

3. Open the directory in which the Agile Manager files are deployed

```
cd /opt/hp/agm
```

4. Run the configuration wizard

As root user	<pre>./run_config.sh</pre>
As sudo user	<pre>sudo ./run_config.sh</pre>

Note: If you are installing Agile Manager on a secondary node of a cluster, some of the steps relevant only to a primary node or a first time configuration are not displayed.

The Agile Manager configuration wizard opens.

```
Welcome  
  
Welcome to the HP Agile Manager Server Configuration Wizard.  
  
The wizard will guide you through the steps of installing HP Agile Manager  
on your computer.  
  
Throughout the wizard, press Enter to accept the default selection, or type  
your new selection. To exit the wizard, click Ctrl+C.
```

5. Accept the EULA

The Agile Manager EULA is displayed. Read through the EULA and accept its terms to continue.

```
-----  
End User License Agreement  
  
HP End User License Agreement - Enterprise Version  
  
1. Applicability. This end user license agreement (the "Agreement") governs the  
use of accompanying software, unless it is subject to a separate agreement  
between you and Hewlett-Packard Company and its subsidiaries ("HP"). By  
downloading, copying, or using the software you agree to this Agreement. HP  
provides translations of this Agreement in certain languages other than  
English, which may be found at: http://www.hp.com/go/SWlicensing.
```

6. Reuse detected settings

If you previously configured Agile Manager, you can save detected settings from the previous configuration.

```
Current Settings  
  
The wizard has detected existing configuration settings on this computer.  
Do you want to keep all current configuration settings?  
  
[X] 1 - Yes, I want to keep all current settings  
[ ] 2 - No, I want to reconfigure server settings  
  
Press Enter to keep the current selection, or type selection number: █
```

Note: This step is displayed only if the `qcConfigFiles.properties` file exists in the `/opt/hp/agm/conf/` directory.

- If you are installing a cluster, you must copy this file from a previous installation before you begin. For details, see ["Install a clustered system" on page 30](#).
- If you are upgrading a system, you must have uninstalled the previous version of Agile Manager and renamed this file. For details, see ["Upgrade Agile Manager" on page 33](#).

Select whether to keep or clear the existing settings. If you select **Yes**, existing settings are used as defaults in subsequent wizard parameters. You can make changes to any of the settings.

7. Enter database parameters

```
Database Server  
  
DB host name:
```

Specify the following. Press **ENTER** after each entry.

Parameter	Description
DB host name	The database server name.
DB port number	The database server port number. You can accept the default port number.
Oracle SID	The Oracle system identifier.

8. Enter database administrator login information

```
Database Administrator Login  
  
DB admin user name:
```

Specify the following. Press **ENTER** after each entry.

Note: If you are performing an upgrade and specified your previous Agile Manager database, or a copy of your previous database, many parameters in the rest of the configuration tool are provided for you.

Parameter	Description
DB admin user name	The name of the user with the administrative permissions required to connect Agile Manager to the database server.
DB admin password	The database administrator password.

9. Select a database schema option

```
System Administration Database Schema

Select an option

[X] 1 - Create a new schema
[ ] 2 - Upgrade a copy of the existing schema
[ ] 3 - Connect to existing schema/second node
[ ] 4 - Upgrade a copy of the System administration schema for staging

Type a number to change the selection or press Enter to continue:
```

Select one of the following:

Option	Description
Create a new schema	Creates a new System Administration database schema. Note: The following warning can be ignored: Schema differences were found This warning is generated as part of the schema extension and upgrade mechanisms.

Option	Description
Upgrade a copy of the existing schema	<p>Creates a copy of the existing system administration database schema and upgrades the copy.</p> <p>This option also automatically connects to the existing Agile Manager site.</p> <p>This option is relevant for upgrades only, and enables you to work with both versions of Agile Manager simultaneously.</p> <p>When prompted:</p> <ol style="list-style-type: none">Enter or accept the provided values for the old schema name and password.Enter a name for the new schema.
Connect to existing schema / second node	<p>Enables you to connect to an existing System Administration database schema.</p> <p>This option is mainly relevant when you are configuring a second node in a cluster. In such cases, this option is valid only when all nodes are installed with the same version.</p> <div data-bbox="553 1209 1369 1451" style="background-color: #f0f0f0; padding: 10px;"><p>Note: Selecting this option uses existing data throughout the rest of the wizard, except for defining the confidential data passphrase. Continue with "Enter a confidential data passphrase" on page 44 and then "Review the settings" on page 46.</p></div>

Option	Description
Upgrade a copy of the system administration schema for staging	<p>Creates a copy of the existing system administration database schema and upgrades the copy.</p> <p>This option creates a blank site that you can use as a staging environment before upgrading your production environment.</p> <p>When prompted:</p> <ol style="list-style-type: none">Enter or accept the provided values for the old schema name and password.Enter a name for the new schema. <p>Note: Selecting this option uses existing data throughout the rest of the wizard, except for defining the confidential data passphrase. Continue with "Enter a confidential data passphrase" on page 44 and then "Review the settings" on page 46.</p>

10. Enter Oracle temporary tablespace information

The temporary tablespace is the location on the database where temporary tables are created to facilitate internal database functionality, such as large sorting tasks.

```
Oracle Tablespaces

Select the default and temporary tablespaces that will be used to store the
Agile Manager Server Site Administration database schema.

Temporary Tablespace:

[X] 1 - TEMP
```

Press **ENTER** to select the default **TEMP** directory.

11. Enter Oracle default tablespace information

The Default Tablespace is the location on the database where database objects will be created.

Note: If you are installing Agile Manager on a secondary node or if the System Administration database already exists, the new System Administration database schema is created in the same tablespace as the existing schema. In such cases, continue with ["Enter system administrator login information" on page 45](#).

```
Default Tablespace:
[X] 1 - QC_DATA 7543MB
[ ] 2 - TDDATA 1654MB
[ ] 3 - TD 2778MB
[ ] 4 - USERS 8595MB

Type a number to change the selection, or click Enter to continue:
```

Select a default tablespace.

12. Enter system administration database schema details

```
SA Schema Details

Schema name: [agm_siteadmin_db]
```

- a. Enter a name for the System Administration database schema, or accept the default.

If you selected **Upgrade a copy of the existing schema** above, the **New Schema Name** option appears. Type a name for the upgraded copy of the System Administration database schema.

- b. The wizard prompts you to enter a password, and provides a default of **tdtdtd** (encrypted). Accept the default password, or enter a new one to change it. The wizard validates your settings.

Caution: Using the default value is not secure and is not recommended. It

can cause encrypted information to be more vulnerable to unauthorized access.

Note: When upgrading an existing System Administration database schema to work in Agile Manager, you must use the same name that you used before the upgrade.

13. Enter a confidential data passphrase

```
Security

Agile Manager Server encrypts confidential data, such as passwords to external
systems (DB, LDAP), and secures communication with other HP BTO applications.

Confidential Data Encryption

Enter a passphrase with at least 12 characters for secure storage of
confidential data.
Important: If you are installing a cluster of servers, make sure you enter the
same passphrase on all nodes.

Confidential data passphrase: [*****]
```

Agile Manager uses this passphrase when encrypting and decrypting confidential data, such as passwords to external (DB, LDAP) systems. Therefore, if you are configuring a clustered system, you must use the same passphrase on both nodes.

Keep a record of the passphrase you choose.

You can also select to use the default value of Seashells Grow Like Misty Tunas.

Caution: Using the default value is not secure and is not recommended. It can cause encrypted information to be more vulnerable to unauthorized access.

Considerations when selecting a Confidential Data Passphrase

Consideration	Details
Password is constant	You cannot change or reset a confidential data encryption passphrase after the configuration wizard is complete.
Password syntax	The passphrase is case-sensitive. The passphrase must not have empty spaces before or after the passphrase. The passphrase may contain only alphanumeric characters.
When upgrading	When upgrading the version of the System Administration database schema, you must enter the same passphrase that was used for the previous installation. By default, the wizard supplies the encrypted password.
Installing on a cluster	If you are installing Agile Manager on a cluster, you must use the same passphrase for all nodes.

14. Enter system administrator login information

```
Site Administrator User

Type the password to be used when logging in to Agile Manager Administration.
Note: The default administrator user name is 'sa'. To add or change
administrators, after the configuration is complete, log in to the Agile
Manager Administration.

Password:
```

Define the password the **sa** user will use to log in to the Agile Manager Administration site. The wizard prompts you to retype the password.

Caution: Using the default password value is not secure and is not

recommended. It can cause encrypted information to be more vulnerable to unauthorized access.

Note: The default administrator user name is **sa**. You cannot change this value.

15. Enter the file repository path

```
File Repository Path  
  
File repository path: [/opt/hp/agm/repository]
```

Accept the default path or enter a new path.

Tip: See "[Site repository](#)" on page 28 for guidelines about defining this path.

16. Verify that the application server port 8080 is free

```
Application Server  
  
Advanced Options  
  
Server HTTP Port: [8080]
```

Note: You can change the default port after configuration is complete. For details, see "[Change the application server port number](#)" on page 75.

17. Review the settings

```
Installation Summary  
  
To confirm the following configuration, Select "Continue". To modify any of the  
settings, Select "Back"
```

Review the information displayed. Select **Continue** to apply the settings.

18. Complete the configuration

```
Finish

The wizard settings were successfully set.

Select "Start server now" to start Agile Manager server now.
To start the server later, run "/opt/hp/agm/wrapper/HPALM start".
To always start the server at boot time, run: "/opt/hp/agm/wrapper/HPALM install".

[X] 1 - Start server now
[ ] 2 - Start server later

Type a number to change the selection or press Enter to continue: █
```

Select whether you want to start the Agile Manager service now or later. If you select to start the service later, see ["Start/Stop the Agile Manager service" on page 50](#) for details.

Note: If you would like to connect to Oracle RAC, do not start the server. Instead, continue with ["Connect to Oracle RAC" on the next page](#).

When the service is up, continue with ["Log in to Agile Manager" on page 52](#). For security best practices and procedures, see ["Secure your system" on page 53](#). For other server and system management details, see ["Manage the application server" on page 74](#) and ["Agile Manager system administration" on page 81](#).

Notes after installing:

- Do not move the following files created by the configuration wizard:

`/opt/hp/agm/repository/qc/repid.txt`

`/opt/hp/agm/conf/qcConfigFile.properties`

- Some configuration settings can be modified after running the wizard. For details, see ["Manage the application server" on page 74](#).

Connect to Oracle RAC

This section describes how to connect your Agile Manager system to Oracle RAC.

Oracle RAC enables you to enhance Oracle database availability and scalability, allowing it to interact with more than one database instance. Agile Manager RAC support includes load balancing between Oracle instances, and failover between all specified Oracle RAC nodes at the initial connection.

1. Perform the steps in ["Enable Oracle RAC Support" on page 24](#).
2. Install Agile Manager as described in ["Install Agile Manager" on page 36](#).

Note: At the end of the procedure, do *not* start the server.

3. On the application server, browse to the `/opt/hp/agm/conf` directory, and open the `qcConfigFile.properties` file for editing.
4. Modify the following parameters:

Parameter name	Description
dbConnectionString	The string used to connect to the database. For example: <pre>dbConnectionString= jdbc\:mercury\:oracle\:TNSNamesFile\=/opt/hp/a gm/conf/tnsnames.ora;TNSServerName\=ALMP</pre>
dbSchemaName	Name of the system administration schema
dbServerName	Name of the database host server (<code>sa_db_host</code>).

The following password parameters can be set in plain text for configuration. After configuration, the passwords are automatically encrypted.

Parameter name	Description
dbaPassword	Password of the user used for installation.
DefaultUserPassword	System administration database schema password Default = tdtdtd . Change this password to protect your system.
windowsUserPassword	Not in use.
siteAdminPassword	Password of the Agile Manager default sa user. Default is blank. Change this password to protect your system.

Note: Do *not* modify the following parameters:

- communicationSecurityPassphrase.
- initString.
- siteAdminUserName. Keep this defined as **sa**.

5. On the application server, place the relevant **tnsnames.ora** file in the **/opt/hp/agm/conf** directory, as defined in the **dbConnectionString** parameter.
6. Run the configuration wizard silently:

As root user	<code>./run_config.sh -nonInteractive</code>
As sudo user	<code>sudo ./run_config.sh -nonInteractive</code>

7. Start the server. For details, see ["Start/Stop the Agile Manager service" on the next page](#).

Start/Stop the Agile Manager service

Action	Command
Start the service	<code>/opt/hp/agm/wrapper/HPALM start</code>
Stop the service	<code>/opt/hp/agm/wrapper/HPALM stop</code>
Restart the service	<code>/opt/hp/agm/wrapper/HPALM restart</code>

Start the Agile Manager service after reboot

By default, Agile Manager does not start when the system boots. To register the Agile Manager service to start when the system boots, run: `/opt/hp/agm/wrapper/HPALM install`

To remove this registration, run: `/opt/hp/agm/wrapper/HPALM remove`

Run Agile Manager as a simple user

Depending on your security requirements, you may need to run Agile Manager as a simple user, with no special permissions. To do this:

1. Create a new simple user: `useradd agmuser`
2. Set the new user as the owner of the Agile Manager installation folder: `chown agmuser:agmuser /opt/hp/agm -R`

Note: In a clustered environment, this user must also be the owner of the shared repository directory. Therefore, this user must be a network user, and not a local user.


3. Edit the **agm/wrapper/HPALM** script, and search for the following text: RUN_AS_USER
4. Un-comment the following line: #RUN_AS_USER=agmuser
5. Set the Agile Manager service to run after rebooting:
/opt/hp/ag/wrapper/HPALM install
6. Start the Agile Manager server: /opt/hp/ag/wrapper/HPALM start


Log in to Agile Manager

After installing, manage your Agile Manager system using the Agile Manager Administration site. Manage your site and users directly in Agile Manager.

Agile Manager	http://<server>:<port>/agm/login
Agile Manager Administration site	http://<serverName>:<port>/agm/admin

The default user installed with Agile Manager is the **sa** user. You defined the **sa** user password during installation (see "[Enter system administrator login information](#)" on [page 45](#)).

To fully benefit from Agile Manager's rich feature set, access the *Help Center* (in the header, click ) or join the discussion at [HP Communities](#).

Note: The *Agile Manager Help Center* is installed together with Agile Manager. Access the help from within Agile Manager using the Help  menu, or open it at this path:

http://<server>:<port>/agm/agmdocs/Default.htm.

Secure your system

The Agile Manager platform is designed to be part of a secure architecture, and can meet the challenge of dealing with the security threats to which it could potentially be exposed.

This chapter describes best practices and recommended procedures to enhance the security of your Agile Manager deployment.

Note: Enterprise security requirements are constantly evolving. If there are additional security requirements that are not covered by this chapter, [contact us](#) about adding them in future versions of this guide.

Report security issues: <https://h41268.www4.hp.com/live/index.aspx?qid=11503>

Access latest Agile Manager security information/register for security alerts:
<https://h20566.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive?ac.admitted=1389784040189.876444892.199480143>

This chapter includes:

- "Secure deployment" on the next page
- "Secure the application server" on page 55
- "Secure system administration" on page 60
- "Secure user authorization" on page 61
- "Data encryption" on page 63
- "Configure an SSL connection" on page 67
- "Secure attachment files" on page 55
- "Secure the network and communication" on page 57
- "Secure user authentication" on page 60
- "Data integrity" on page 62
- "Data logging" on page 65
- "Integrate an Apache web server (example)" on page 71

Secure deployment

Agile Manager is an enterprise-wide application based on Java 2 Enterprise Edition (J2EE) technology. J2EE technology provides a component-based approach to the design, development, assembly, and deployment of enterprise applications.

Agile Manager can be configured in a basic configuration or a clustered configuration. Use any of the following methods to enhance security in either configuration:

Secure deployment methods	
SSL	<p>Basic configuration. Enable SSL on the Agile Manager Jetty and make it required.</p> <p>Clustered configuration. Require SSL for the Agile Manager virtual IP on the load balancer.</p> <p>For details, see "Configure an SSL connection" on page 67.</p>
Reverse proxy	<p>Install a reverse proxy in front of the Agile Manager server, and then configure SSL on the reverse proxy server.</p> <p>For details, see "Reverse proxy architecture" on page 58 and "Integrate an Apache web server (example)" on page 71.</p> <p>For details about enabling SSL for all interactions with Apache, see http://httpd.apache.org/docs/current/ssl/ssl_howto.html.</p>
Firewall	<p>Use a firewall between the client and the other Agile Manager components.</p> <p>Block access to all incoming traffic except for the http port (8080) or https port (8443) used by Agile Manager.</p>

See also: ["Secure the network and communication" on page 57](#)

Common considerations and best practices

- Thoroughly review the trust boundaries between application, exchange, database, and LDAP servers to minimize the number of hops between the components. Additionally, it is recommended to use SSL to secure access to servers located

across such boundaries.

- When there is a firewall between any Agile Manager deployment components, ensure the proper configuration according to the vendor recommendation.
- Run periodic trusted root Certificate Authority certificate updates on your clients and servers to ensure that the publisher certificates used in digital code signing are trusted.

Note: By default, the Agile Manager application server does not have SSL enabled. It is expected and recommended that the front end server, either the load balancer or the reverse proxy, will be configured to require SSL.

Currently, a secure channel to the database server from Agile Manager is not supported.

Secure attachment files

Use the Agile Manager Administration site to limit the types of files and file sizes the users can upload as entity attachments. In the Administration site, browse to the **Configuration > General** page, and define the following options:

- **Maximum upload file size (MB)**
- **Blocked file extensions files types**

For details, see "[Define repository attachment settings](#)" on page 86.

Note: Attachment files can still contain dangerous content, and must be downloaded and opened with caution. It is strongly recommended to implement proper anti-virus protection for the file storage allocated for the Agile Manager repository.

Secure the application server

Perform any of the following additional steps to secure your application server:

- Always use the minimal possible permissions when installing and running Agile Manager. For example, install Agile Manager using sudo permissions, and run Agile Manager as a simple user with no special permissions. For details, see "[Install as a non-root user](#)" on page 17 and "[Run Agile Manager as a simple user](#)" on page 50.
- When configuring SSL on the Agile Manager application server, keep your keystore in a private directory with restricted access. Although the Java keystore is password protected, it is vulnerable as long as the password was not changed from its default value of **changeit**. For details, see "[Configure an SSL connection](#)" on page 67.
- Always obfuscate passwords entered into the **jetty.xml** file. For details, see <http://www.eclipse.org/jetty/documentation/current/configuring-security-secure-passwords.html>.
- Always modify the default passwords when prompted, such as the default **sa** user password, or the confidential data passphrase.

Application server security FAQs

Question	Answer
Are application resources protected with permission sets that allow only an application administrator to modify application resource configuration files?	Yes. Only the user with permission to access specific directories on the Agile Manager application server machine can modify Agile Manager configuration files.
Does Agile Manager ensure that configuration files are not stored in the same directory as user data?	<p>Administrators can use the Agile Manager Administration site to change the location of the repository and log files to avoid mixing user data with configuration files.</p> <p>Change the repository path on the Servers > Database page, and the log file path on the Servers > Application page.</p> <p>For details, see "Configure database settings" on page 84 and "Configure application logs" on page 82.</p>

Question	Answer
Does Agile Manager execute with no more privileges than necessary for proper operation?	Yes. The permissions model is constantly reviewed and only necessary permissions are required.

Secure the network and communication

The following measures are recommended to secure the communication between Agile Manager system components:

- ["Separate and secure system components" below](#)
- ["DMZ architecture using a firewall" on the next page](#)
- ["Benefits to using a reverse proxy:" on the next page](#)
- ["Use SSL between system components" below](#)
- ["Reverse proxy architecture" on the next page](#)
- ["Secure communication channels" on page 59](#)

Separate and secure system components

- Separate your web servers, application servers, load balancers, and database servers.
- Follow security guidelines for LDAP servers and Oracle databases.
- Run SNMP and SMTP servers with low permissions.

Use SSL between system components

The SSL protocol secures the connection between the client and the server. URLs that require a secure connection start with HTTPS instead of HTTP. Agile Manager supports SSLv3 and TLSv1.

For details, see ["Configure an SSL connection" on page 67](#).

Note: By default, the Agile Manager application server does not have SSL enabled. It is expected and recommended that the front-end server, either a load balancer or a reverse proxy, is configured to require SSL.

DMZ architecture using a firewall

In a DMZ architecture, an additional network is added to the system, enabling you to isolate the internal network from the external network. Use a firewall to create a complete separation, and to avoid direct access, between the Agile Manager clients and servers.

There are a few common DMZ implementations. This guide discusses implementing a DMZ and reverse proxy in a back-to-back topology environment.

Note: When using a firewall, you must leave the port designated for incoming traffic (the jetty port) open. By default, this is port **8080**, or **8443** if you are using a secure connection.

Reverse proxy architecture

Agile Manager fully supports reverse proxy and secure reverse proxy architecture.

A reverse proxy is a server positioned between the client and the web servers. To the client machine, the reverse proxy looks just like a standard web server that serves the client's HTTP(S) requests, with no additional configuration required.

The client sends web content requests to the reverse proxy, which then forwards it on to a web server. The web server responds in turn, via the reverse proxy. However, the response appears to the client as if it was sent by the reverse proxy instead of the web server.

The reverse proxy functions as a bastion host through all communication with external clients, and is the only machine addressed by external clients, and obscures the rest of the internal network.

For example of how to configure a reverse proxy, see ["Integrate an Apache web server \(example\)" on page 71](#).

Benefits to using a reverse proxy:

- Ability to place the application server on a separate machine in the internal network.
- No DMZ protocol translation. Incoming and outgoing protocol are identical. Only header changes occur.

- Only http(s) access to the reverse proxy is allowed. This enables improved communication protection by stateful packet inspection firewalls.
- Access to most web server security features, such as authentication methods and encryption.
- NAT firewall support.
- Ease of maintenance. You can add patches to your reverse proxy as needed.
- The reverse proxy provides good performance compared to other bastion solutions.
- Ability to define a static and restricted set of redirect requests on the reverse proxy.
- Screening of server IP addresses, as well as internal network architecture.
- A minimal number of required open ports in the firewall.
- The only accessible client of the web server is the reverse proxy.

Secure communication channels

Agile Manager supports the following secure channels:

- **Client / Application server.** In general, trust is only needed on the client. This is a trust to the authority that issued the server certificate for the Agile Manager application server.
- **Application server / LDAP server.** Configure LDAP settings in the **Users > Settings** page in the Agile Manager Administration site. For details, see "[LDAP](#)" on page 88.
- **Application server / Mail server.** Specify a secure port when defining the mail server.
- **Reverse proxy or load balancer / Application server.** Configure the Agile Manager application server with SSL.

On the reverse proxy or load balancer, use a secure connection to the Agile Manager server, such as **https://<server>:8443/agm**

Secure system administration

Your Agile Manager site is managed using the Agile Manager Administration site.

- Secure the Administration site by changing the system administrator password during the initial setup (see ["Enter system administrator login information" on page 45](#)), or later in the Agile Manager Administration site. Use the Administration site to designate other system administrators.

To manage system administrators and passwords, see the **Users > User Management** administration page. Use a strong password for the system administrator.

- Restrict site customization by modifying user permissions in the Agile Manager configuration area (**Site > Site Users**).
- To debug user actions, set the log level to **Debug** in the Agile Manager Administration site (**Servers > Application**). Be sure to revert the log level back to the previous value when you are finished debugging.
- After updating your licenses, store the license file in a secure location to prevent unauthorized access.

For details see ["Log in to Agile Manager" on page 52](#) and ["Agile Manager system administration" on page 81](#).

Secure user authentication

Agile Manager supports the following authentication methods:

- **Create users directly in Agile Manager.** This option is not secured. For secure access, use external LDAP authentication.
- **LDAP authentication.** Import users from any LDAP provider that supports LDAP3.

Authentication is configured in the Agile Manager Administration site (**Users > Settings**). Users are added or imported by site administrators in the Agile Manager configuration area (**Site > Site Users**).

For details see "[Log in to Agile Manager](#)" on page 52, "[Configure user authentication](#)" on page 88, and the *Agile Manager Help Center*.

Secure authentication FAQs

Question	Answer
Can Agile Manager require account passwords that conform to corporate policy?	LDAP authentication is the recommended solution for ensuring password policy support.
Which LDAP providers does Agile Manager support?	Agile Manager works with any LDAP provider that supports the LDAP3 protocol.
Describe the session management and session lockout mechanisms. How does Agile Manager respond if verification fails? Is the user locked out? Can it be configured?	Agile Manager manages sessions at the user level. Inactivity timeouts can be configured by system administrators using the Agile Manager Administration site (Site Configuration > General). LDAP configuration only: Users who attempt a series of incorrect logins are locked out of Agile Manager for 30 minutes.

Secure user authorization

User access to Agile Manager resources is authorized based on the user's role and permissions.

Before accessing Agile Manager, users must be added or imported in Agile Manager and activated. Users are automatically activated as long as you have available licenses.

Users can have any of the following roles:

Role	Description	Location defined
System administrator	Authorized to access the Agile Manager Administration site and modify system administration values.	Agile Manager Administration site (Configuration > Users)
Site administrator	Has full permission in the Agile Manager application and configuration areas for all products. Site administrators can restrict the workspaces that site users have access to.	Agile Manager configuration area (Site > Site Users)
Workspace administrator	Has full permission in the Agile Manager application and configuration areas for a specific Agile Manager workspace. Workspace administrators can restrict the applications that workspace users have access to.	Agile Manager configuration area (Workspace > Workspace Users)
Team member	Has full permissions in the application area and read-only access to the configuration area. Users can view only items associated with the applications to which they have access.	Agile Manager configuration area (Workspace > Workspace Users)

For details, see "[Define system administrators and reset user passwords](#)" on page 90 and the *Agile Manager Help Center*.

Data integrity

Data integrity is a critical security requirement, and the data backup procedure is an integral part of this requirement. Agile Manager does not provide backup capabilities. Backup is the responsibility of the Oracle database administrator.

Consider the following when backing up your system:

- Backup is especially important before critical actions such as upgrade.

You can restore your site to a specific backup file using the Agile Manager Administration site (**Servers > Database Server**). For details, see "[Configure database settings](#)" on page 84.

- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Data backup consumes a lot of resources. It is strongly recommended to avoid running backups during peak demand times.

Note: When backing up the database, ensure that the file repository is backed up at the same time to reflect the same system state.

Data encryption

Agile Manager supports the following types of encryption:

- **Agile Manager encryption.** Agile Manager stores sensitive credentials, encrypted, in the database.

Examples of sensitive data include credentials to the database server used by Agile Manager, credentials to the LDAP and SMTP servers that Agile Manager integrates with, and credentials for machines that contain user data.

Agile Manager uses the following security configuration:

JCE crypto source, Symmetric block cipher, 3DES engine, 192 key size

LW crypto source, Symmetric block cipher, AES engine, 256 key size

- **Password encryption.** User passwords are never stored. Only the hash versions of passwords are stored.
- **Transparent Data Encryption (TDE).** Agile Manager is certified to work with TDE for Oracle databases.

- **Full Disk Encryption (FDE).** FDE is supported for all system components, including database, server, repository server, and client machines.

Caution: Implementing TDE or FDE can impact system performance. For details, contact the vendor providing your encryption.

Encryption FAQs

Question	Answer
Does Agile Manager transmit account passwords in an approved encrypted format?	It is strongly recommended to enable SSL on the Agile Manager and LDAP servers to ensure secure account password transmission. For details, see "Uninstall Agile Manager" on page 78 and "LDAP" on page 88 .
Does Agile Manager store account passwords in approved encrypted format?	User passwords are not stored at all, only the hash versions. Internal system passwords are stored in AES 256.
Does Agile Manager use the Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules and random number generator to implement encryption, key exchange, digital signature, and hash functionality?	The cryptography provider used by Agile Manager is not FIPS validated.

Question	Answer
What base product and service authentication methods are provided?	Agile Manager can be configured to support the following authentication methods: <ul style="list-style-type: none">• Username/password• LDAP authentication For details, see " Secure user authentication " on page 60.
Are there any default vendor-supplied passwords or other security parameters embedded in Agile Manager?	Yes. Default passwords can be replaced during installation and configuration. Installation and configuration is described in " Install Agile Manager " on page 36.

Data logging

Agile Manager provides the following types of logs:

["Application logs"](#) below

["Entity logs"](#) on the next page

Application logs

Application log files can report all system events, depending on the log level configured in the Agile Manager Administration site (**Servers > Application**). The period of time that log data is kept is configurable, and the default is unlimited.

The **wrapper.log** is configurable in the **wrapper.conf** file.

Recommendations:

- Pay attention to the log level and do not leave the log level at **Debug**.
- Pay attention to log rotation.
- Restrict access to the log directory.
- If log archiving is required, create your own archiving policy.

Log levels and log rotations are set using the Agile Manager Administration site (**Servers > Application**). For details, see "[Configure application logs](#)" on page 82.

Entity logs

Changes to existing entities, such as defects and user stories, are stored in the database as entity history. You can view entity history from the **Details** page in Agile Manager.

Entity history is kept as long as the entity itself is not deleted. For this reason, we recommend assigning backlog items to a dedicated release, feature, or theme as an alternative to permanent deletion. Administrators can also archive themes and features to remove them from backlog grids and graphs.

For details, see the *Agile Manager Help Center*.

Note: It is the user's responsibility not to insert unprotected and sensitive data into regular Agile Manager entity fields.

Log file FAQs

Question	Answer
Does Agile Manager audit access to need-to-know information and key application events?	The information can be obtained from the application log files or the Agile Manager entity history.
Does Agile Manager display the user's time and date of the last change in data content?	This information is available in Agile Manager entity history.
Does Agile Manager support the creation of transaction logs for access and change to the data?	This information can be found in the application logs, depending on log level.

Configure an SSL connection

The following procedure describes how to configure a Secure Socket Layer (SSL) connection to Agile Manager.

Caution: This procedure must be performed only after installing Agile Manager. For details, see ["Install Agile Manager" on page 36](#).

1. Obtain the server certificate issued to the name of this server in java keystore format. It must contain a private key and the certificate authority that issued it.

For example, you can create this certificate by yourself as follows:

- a. Log in to the server as user **root**, and navigate to the home folder.
- b. Run the following commands one by one:

```
cd /root

export SERVER_DN="CN=< server machine
name>,OU=X,O=Y,L=Z,S=XY,C=YZ"

export KSDEFAULTS="-storepass changeit"

export KEYINFO="-keyalg RSA"

keytool -genkey -alias tomcat -dname $SERVER_DN $KSDEFAULTS -
keystore server.keystore $KEYINFO -keypass changeit

keytool -export -alias tomcat -file temp_server.cer $KSDEFAULTS
-keystore server.keystore

keytool -import -v -trustcacerts -alias tomcat -file temp_
server.cer $KSDEFAULTS -keystore client.keystore.trust -keypass
changeit
```

2. Install the certificate in the Java home as follows:

- a. Navigate to the Agile Manager Java home, and backup the **cacerts** file:

```
cd /opt/hp/agm/java/jre/lib/security
cp cacerts cacerts.backup
```

- b. Replace the original **cacerts** file with the **client.keystore.trust** file, renaming it to **cacerts**:

```
cp ~/client.keystore.trust ./cacerts
```

3. Verify that all users have logged out of Agile Manager, and stop the Agile Manager service: `/opt/hp/agm/wrapper/HPALM stop`
4. Navigate to the **/opt/hp/agm/server/conf/** directory and make a backup of the **jetty.xml** file:

```
cp /opt/hp/agm/server/conf/jetty.xml
/opt/hp/agm/server/conf/jetty.xml.backup
```

5. Open the **jetty.xml** file and add the following section under the **Configure** element:

```
<Call name="addConnector">
<Arg>
<New class="org.eclipse.jetty.server.ssl.SslSocketConnector">
<Set name="host"><Property name="jetty.host" /></Set>
<Set name="Port">8443</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="keystore">/home/admin/Downloads/server.keystore</Set>
<Set name="password">changeit</Set>
<Set name="keyPassword">changeit</Set>
<Set name="truststore">/home/admin/Downloads/server.keystore</Set>
<Set name="trustPassword">changeit</Set>
```

```
</New>  
</Arg>  
</Call>
```

6. In the added section, do the following:
 - Replace the **/home/admin/Downloads** path with the location of your keystore file.
 - If you want to change the port number, replace **8443** with the new port number.
 - If you have changed the default keystore password, replace **changeit** with the new password.

7. (Optional) To encrypt the password, perform the following steps:

- a. Run: `./java -cp " ./opt/hp/agm/lib/*:/opt/hp/agm/lib/ext/" org.eclipse.jetty.http.security.Password <password>`

For example, if you run the following command:

```
./java -cp " ./opt/hp/agm/lib/*:/opt/hp/agm/lib/ext/"  
org.eclipse.jetty.http.security.Password changeit
```

The output will appear as follows:

```
changeit  
OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0  
MD5:b91cd1a54781790beaa2baf741fa6789
```

- b. In the **jetty.xml** file, replace the plain text password with the encrypted output, including the **OBF** and **MD5** prefix.
8. After ensuring that the SSL connection works, disable non-HTTP access to the Agile Manager application server. In the **jetty.xml** file, locate the following section and comment it out by placing **<!--** at the beginning of the section, and **-->** at the end.

For example:

```
<!--  
<Call name="addConnector">  
<Arg>  
<New class="org.eclipse.jetty.server.nio.SelectChannelConnector">  
<Set name="host"><Property name="jetty.host" /></Set>  
<Set name="port"><Property name="jetty.port"  
default="8080"/></Set>  
<Set name="maxIdleTime">300000</Set>  
<Set name="Acceptors">2</Set>  
<Set name="statsOn">>false</Set>  
<Set name="confidentialPort">8443</Set>  
<Set name="lowResourcesConnections">20000</Set>  
<Set name="lowResourcesMaxIdleTime">5000</Set>  
</New>  
</Arg>  
</Call>  
-->
```

Note: It is possible that this section in your **jetty.xml** file is slightly different.

9. Save the **jetty.xml** file.
10. Restart the Agile Manager service: `/opt/hp/agm/wrapper/HPALM restart`
11. Connect to Agile Manager using port 8443, or the number of the new port if you changed it above. Connect to Agile Manager as described in using the following URLs:

Agile Manager	<code>https://<server>:<port>/agm/login</code>
----------------------	--

Agile Manager Administration site	<code>http://<serverName>:<port>/agm/admin</code>
--	---

Integrate an Apache web server (example)

To support external authentication or to increase security, place the Agile Manager application server behind a secure reverse proxy. For details, see ["Reverse proxy architecture" on page 58](#).

This section describes one way to do this, by configuring the Apache Web server to redirect requests to the Agile Manager application server.

Note: Configure the Apache Web server to work in proxy HTTP mode. It is recommended that you use Apache HTTP Server version 2.4.

1. Verify that the Apache Web server is stopped.
2. Navigate to the **<Apache Home directory>\conf** directory.
3. Open the **httpd.conf** file.
4. Uncomment or add the following load module commands:

```
LoadModule proxy_module modules/mod_proxy.so  
LoadModule proxy_http_module modules/mod_proxy_http.so
```

Note: Make sure that both modules exist in your Apache installation.

5. Add the following section to the end of the file:

Note: If you are connecting to Agile Manager from a local machine, replace **<Agile Manager server name>** with the **localhost**.

```
# Turn off support for true Proxy behavior as we are acting as
# a reverse proxy
ProxyRequests Off

# Turn off VIA header as we know where the requests are proxied
ProxyVia Off

# Set the permissions for the proxy
<Proxy *>
AddDefaultCharset off
Order deny,allow
Allow from all
</Proxy>

# Turn on Proxy status reporting at /status
# This should be better protected than: Allow from all
ProxyStatus On
<Location /status>
SetHandler server-status
Order Deny,Allow
Allow from all
</Location>

# Configuring mod_proxy_http
# To connect to servlet container with HTTP protocol, the
# ProxyPass directive can be used to send requests received on a
# particular URL to a Jetty instance.
ProxyPreserveHost off
ProxyPass /qcbn http://localhost:8080/qcbn
ProxyPassReverse /qcbn http://localhost:8080/qcbn
```



```
ProxyPass /agm http://localhost:8080/agm
ProxyPassReverse /agm http://localhost:8080/agm

# Rewrite rule trailing slash must be used in the VirtualHost
# sectionLoadModule rewrite_module modules/mod_rewrite.so
RewriteEngine On
```

6. Save the changes to the file.
7. Restart the Apache Web server.

Connect to Agile Manager using the URLs listed in "[Log in to Agile Manager](#)" on [page 52](#), using the apache port in the URL.

Manage the application server

This chapter contains information relating to managing the Agile Manager application server, as well as information regarding general Java management tools.

["Change the heap memory size" below](#)

["Change the application server port number" on the next page](#)

["Application server management tools" on page 76](#)

Note: You may also need to move the repository. If you do this, you must also modify the repository path configured in Agile Manager. Use the **Restore Site Schema** option in the Agile Manager Administration site (**Servers > Database**). For details, see ["Restore a site schema" on page 84](#).

Change the heap memory size

After you install Agile Manager, you may need to change the heap memory values. For example, you may want to increase the heap size if there is an increase in the number of concurrent user sessions.

Note:

- The maximum heap value cannot exceed your maximum memory (RAM) size.
- On a machine running on a 32-bit operating system, the heap memory size should not exceed 1024 MB.

1. Verify that all users have logged out of Agile Manager and stop the Agile Manager service: `/opt/hp/agm/wrapper/HPALM stop`
2. In the Agile Manager deployment path, open the **wrapper.conf** file.
3. Change the **wrapper.java.maxmemory** value as necessary.
4. Restart the Agile Manager service: `/opt/hp/agm/wrapper/HPALM restart`

Change the application server port number

After you install Agile Manager, you may need to change the application server port number.

It is possible that the default application server port may be in use by another application that is running on the same machine. In this case, you can either locate the application that is using the port and stop it, or you can change the Agile Manager server port.

The default port is **8080** or **8443** for secure connections.

1. Verify that all users have logged out of Agile Manager and stop the Agile Manager service: `/opt/hp/agm/wrapper/HPALM stop`
2. Navigate to the `/opt/hp/agm/server/conf/jetty.xml` file.
3. Change the **jetty.port** value.
4. Restart the Agile Manager service: `/opt/hp/agm/wrapper/HPALM restart`

Change the system administration schema password

Change the system administration schema password routinely to maintain system security.

1. Verify that all users have logged out of Agile Manager, and stop the Agile Manager service: `/opt/hp/agm/wrapper/HPALM stop`
2. Run the configuration wizard again, as described in ["Install Agile Manager" on page 36](#).

During installation, keep all current settings and make only the following modifications:

Wizard page	Selection option
Current Settings	Select Keep all current settings . Example
System Administration Database Schema	Select Connect to existing schema/second node . Details
SA Schema details	Enter the new password when prompted. Details

3. Select whether you want to start the Agile Manager service now or later. If you select to start the service later, see ["Start/Stop the Agile Manager service" on page 50](#) for details.
4. When the service is up, continue with ["Log in to Agile Manager" on page 52](#).

Application server management tools

The Agile Manager application server is Java-based. We recommend the following Java tools for effectively managing your Agile Manager server:

Tool	Address
jconsole	http://java.sun.com/developer/technicalArticles/J2SE/jconsole.html <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note: To connect to jconsole using a remote process, use the following URL syntax:</p> <pre>service:jmx:rmi://<server>:29601/jndi/rmi://<server>:9999/server</pre> <p>If you do not want to expose this console, you must close the relevant ports (29601 and 9999) on your server.</p> </div>
jstack	http://download.oracle.com/javase/1.5.0/docs/tooldocs/share/jstack.html

Tool	Address
jmap	http://download.oracle.com/javase/1.5.0/docs/tooldocs/share/jmap.html
jvisualvm	http://download.oracle.com/javase/6/docs/technotes/tools/share/jvisualvm.html

Uninstall Agile Manager

1. Log in to the server machine as the same user who installed Agile Manager (either **root** or the **agmadmin** sudo user).
2. Remove the Agile Manager service from the items that start when the system boots: `/opt/hp/agm/wrapper/HPALM remove`
3. Uninstall Agile Manager: `rpm -e Agile-Manager`

Note: By default, the **conf**, **log**, and **repository** directories are not deleted from your machine.

When you uninstall Agile Manager, the **qcConfigFile.properties** file is renamed to **qcConfigFile.properties.rpmsave**. This file stores the values you defined the last time you ran the configuration wizard.

If you want to reinstall Agile Manager using the same values as you used before, you must rename this file to **qcConfigFile.properties** before reinstalling.

4. (Optional) To remove all traces of Agile Manager from the machine, delete all remaining files in the installation directory as well as the deployment path.
 - Removing the **conf** directory will require you to manually add values the next time you run the configuration wizard.
 - Removing the **repository** directory also removes all site repositories. The database is still retained unless it is specifically deleted.

Troubleshooting

If you encounter problems installing Agile Manager, check for errors in the following log files:

Log	Path
Installation and configuration	/opt/hp/agm/log/InstallationLog_<date and time>.html
System administration database schema creation	/opt/hp/agm/log/sa

Error: An Agile Manager installation already exists

Uninstall the existing Agile Manager installation and remove all traces of it from the server machine. Then try installing Agile Manager again.

Caution: If a log file is deleted while the Agile Manager server is running, it is not recreated until the server is restarted.

For details, see ["Uninstall Agile Manager" on the previous page](#).

Error: Agile Manager server isn't started because RMI port is in use

In such cases, an error will appear in the **wrapper.log** file. For example:

```
INFO | jvm 5 | 2014/07/15 14:00:09.497 | WrapperSimpleApp Error:  
Caused by: java.rmi.server.ExportException: Port already in use:  
29601; nested exception is:  
  
INFO | jvm 5 | 2014/07/15 14:00:09.497 |  
java.net.BindException: Address already in use
```

Workaround: Do one of the following:


- Release the Linux process that is using the port.
- Change the RMI port used by Agile Manager. Do the following:
 - a. Verify that all users have logged out of Agile Manager and stop the Agile Manager service: `/opt/hp/agm/wrapper/HPALM stop`
 - b. Navigate to the `/opt/hp/agm/conf/jetty-jmx.xml` file and modify the **jetty.port** value.
 - c. Restart the Agile Manager service: `/opt/hp/agm/wrapper/HPALM restart`

Agile Manager system administration

This section of the Agile Manager Installation and Administration Guide is intended for system administrators who need to configure servers, users, and other system settings.

Note: The functions described in this section are only available from the Agile Manager Administration site.

You must be defined as an Agile Manager system administrator to access the Administration site. For access details, see ["Log in to Agile Manager" on page 52](#).

Each page in the Administration site enables you to save your changes, or undo changes since the last save. Hover over tooltips  to display additional details about each field.

Configure the following:

Server settings	81
System and user settings	85

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Server settings

Configure application logs	82
Configure database settings	84
Configure an email notification server	85

Configure application logs

Tab: Servers > Application

If you are working in a clustered environment, select a server name from the list on the left.

The following standard log4j files are generated by Agile Manager and stored on the application server:

- **agm.logger.txt.** Records events that occur in the Agile Manager application. Stored in the `/opt/hp/agm/log/qc` directory.
- **sa.logger.txt.** Records events that occur in the Administration site. Stored in the `/opt/hp/agm/log/sa` directory.

Default values

- Log levels for both files are set to WARN.
- Log files are limited to 10000 KB, after which the current log entries are copied to a different file, which is appended with a sequential number. This sequential number is updated each time a new log file is created, until the defined maximum number of files is reached.
- 10 log files are kept at a time, including one current log file, and nine log files with earlier entries.

Configure log settings

You can configure the log settings using the `log4j.properties` file. This file is located on the application server, in the `/opt/hp/agm/webapps/qcbin/WEB-INF/classes` directory.

Changes to the log settings do not require you to restart the server.

Configure the following log values:

Parameter	Description
Log level	<p>Defined in the first line of the file. Default. WARN</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: If you change the log level to Debug, make sure to change it back when you are finished debugging.</p> </div>
FileAppender	<p>Defines the appender added to each file name when the log file reaches the maximum configured size. Default. RollingFileAppender (standard log4j value)</p>
FileAppender.File	<p>Defines the location and name of the log file. Default. \${log.folder}qc/agm.logger.txt</p>
FileAppender.MaxFileSize	<p>Defines the maximum size of the log file. Default. 10000 KB</p>
FileAppender.MaxBackupIndex	<p>Defines the maximum number of log files retained, including files with previous entries. After this maximum is reached, the oldest entries are deleted from the system. Default. 10 files</p>
FileAppender.layout	<p>Defines the log files layout and organization. Default. PatternLayout (standard log4j value)</p>
FileAppender.layout.ConversionPattern	<p>Defines the data displayed in the log files. Default. Standard log4j values, as well as the following custom attributes:</p> <ul style="list-style-type: none"> • file. The file that contains the event. • class. The event class. • method. The event method. • build. The build where the event occurred.

Configure database settings

Tab: Servers > Database

Caution: Do not perform any actions on this page while users are currently connected to Agile Manager.

Database server details are configured during Agile Manager installation and configuration. For details, see ["Enter database parameters" on page 39](#).

The Administration site enables you to do the following:

- ["Edit the Agile Manager database user password" below](#)
- ["Restore a site schema" below](#)

[Edit the Agile Manager database user password](#)

If you update your database password, you will also need to edit the password configured in Agile Manager accordingly.

Click **Edit Password**. Enter the new password, and then enter it again to confirm.

Caution: Your site is temporarily deactivated while you are editing the password.

[Restore a site schema](#)

Restore a site to a previous state using an older version of your database and repository. This action replaces the database currently configured for Agile Manager (and displayed on the **Servers > Database** page).

After you restore a site, all data currently displayed in Agile Manager will be inaccessible from Agile Manager.

Additionally, restore a site schema when upgrading Agile Manager using separate system components, as recommended. For details, see ["Upgrade your system" on page 32](#).


Click **Restore Site Schema**, and enter the site schema and repository information for the site you want to restore.

Caution: You must use a schema hosted on the same database server, with identical credentials to the ones defined in the current version.

Configure an email notification server

You must configure an SMTP mail server to enable Agile Manager to send notifications to users.

Tab: Servers > Mail

1. Define the server name and server port number.
2. If your mail server requires SMTP authentication, select **Enable connection to an SMTP server that requires authentication**, and enter the authentication details.
3. Save your changes and click **Test Send Mail**  to send a test email using the settings you configured.

Enter the source and target email addresses, and click **Test**.

System and user settings

Configure miscellaneous system settings	85
Update user licenses	87
Configure user authentication	88
Define system administrators and reset user passwords	90
Configure advanced parameters	91

Configure miscellaneous system settings

Tab: Configuration > General

Define security settings

Under **Security**, define the following:

- **The inactivity timeout.** Modifying this option requires users to log out and log in again for the changes to take effect.
- **'sa' user login permissions.** Whether the default **sa** user is allowed to log in using Agile Manager credentials, regardless of LDAP configuration

This setting is relevant when LDAP authentication is configured, and the **sa** user does not exist in the LDAP system.

Caution:

- If you have system administrators other than the **sa** user, and you disable this option, you cannot enable it again.
- You cannot disable this option if the **sa** user is the only system administrator or the only site administrator.

System administrators are configured on the **Users** administration site page. For details, see ["Define system administrators and reset user passwords" on page 90](#).

Site Administrators are configured in the Agile Manager configuration area (**Site > Site Users**). For details, see the *Agile Manager User Guide*.

Define repository attachment settings

Define limitations for the types of files that can be uploaded as attachments, including:

- Maximum file size
- File extension types

Define report settings

Define when Agile Manager aggregates daily data for dashboard graphs over time. Modifying this option requires you to restart the server to take effect.

Update user licenses

Tab: Configuration > Licenses

Agile Manager is installed with a default "Instant On" below license, which supports 100 users for 30 days. Purchase additional licenses to add more users, or to access Agile Manager after the initial 30 days.

Add additional licenses by updating your system with a **.dat** license file provided by HP. After updating your licenses, store the license file in a secure location to prevent unauthorized access.

1. Click **Update Licenses**.
2. Browse to, and select the **.dat** file you want to upload.
3. Click **Refresh** to view the updated number of licenses in the table.

Note:

- Adding or importing more users than your licenses support will cause those users to be added as Inactive. Activate or deactivate users in the Agile Manager configuration area (**Site > Site Users**).

For details, see the *Agile Manager User Guide*.

- If you are working in a clustered configuration, installing a license on one node will not always automatically install the license on the other node(s).

In such cases, access the Agile Manager Administration site directly from the other node (and not through the load balancer), and update the license there as well. Restart the other node for your license to take effect.

License types

Instant On	Initial license provided with a trial download of Agile Manager. Supports 100 users for 30 days.
-------------------	--

Evaluation	<p>Purchased license that supports a specific number of named users, for a limited period of time.</p> <p>Used to replace the default Instant On license in case you need more time to evaluate Agile Manager.</p>
Perpetual	<p>Purchased license that supports a specific number of unnamed users for an indefinite period of time. Purchase additional licenses to add more users.</p>
Term	<p>Purchased license that supports a specific number of named users, for a limited period of time.</p> <p>Additional licenses must be purchased to continue using Agile Manager after this time period is complete, or to add additional users.</p> <p>Available only if you already have a Perpetual license. Use this if you need to add more users for a short period of time only.</p>

Configure user authentication

Tab: Configuration > Authentication

Agile Manager supports the following types of authentication:

Agile Manager

Users are added to and authenticated directly by Agile Manager.

Select **Agile Manager**, and continue directly to the Agile Manager configuration area to add individual users.

LDAP

Users are imported from and authenticated by your company's LDAP system.

LDAP users log in to Agile Manager using the email address configured in their system profile, and their computer password.


Note: Agile Manager also supports LDAP communication transfer over secure

sockets (SSL). This ensures that users' credentials (passwords) are not sent over the network in an unsecured way.

To use LDAP over SSL, you must configure the following:


LDAP server configuration	<p>Pre-configure the following on the LDAP server:</p> <ul style="list-style-type: none">• Enable SSL.• Define a secure port. Agile Manager uses port 636 by default.• Install a server certificate. <p>Additionally, obtain a root certificate (and any intermediate) from the certificate authority (CA) that issued the LDAP certificate.</p>
Agile Manager server configuration	<p>Pre-configure a certificate trust store on the Agile Manager application server.</p> <p>In most cases, the default trust store is used. The default trust store is <code><JAVA_HOME>/jre/lib/security/cacerts</code> (the default password is changeit), where <code><JAVA_HOME></code> is the installation location for the JDK that comes with Agile Manager (for example, <code>/opt/hp/agm/java/jre</code>).</p> <p>To establish trust to the CA that issued the LDAP server certificate, import the root CA certificate into the Java trust store using the <code>keytool</code> utility.</p> <p>Note: The <code>keytool</code> utility is located in the <code>bin</code> folder of the <code>JAVA_HOME</code> (for example, <code>/opt/hp/agm/java/jre/bin</code>).</p> <p>For example: <code>keytool -import -alias <your LDAP CA> -trustcacerts -file <LDAP CA cert> -keystore <JAVA_HOME>/jre/lib/security/cacerts</code></p> <p>If there are any intermediate Certificate Authorities, import their certificates as well.</p>

To configure LDAP authentication:

1. On the Authentication page, select **LDAP**, and configure Agile Manager to connect to your LDAP system using the fields below. Hover over tooltips  if you need additional clarifications about a specific field.
 - When setting the **Directory Provider URL** field for SSL, use the following syntax:
`ldaps://<server name>`.
 - Set the **Result record limit** value to the number of users you want to import into Agile Manager at a time.

Importing large numbers of users simultaneously may take a few moments.

Tip: If your organization prefers to use login identifications other than the email address, enter the relevant LDAP field in the **Alternative Login ID** field.

2. Click **Test connection** to test the connection with the LDAP server. To verify both authentication and import settings, click **Test LDAP Settings** .
3. After the LDAP settings are defined, continue to the Agile Manager configuration area to import users (**Site > Site Users**). For details, see the *Agile Manager User Guide*.

Define system administrators and reset user passwords

Tab: Configuration > Users

System administrators

After adding individual users to your site, or importing them from an LDAP system, define specific users as additional system administrators.

System administrators have read and write access to the Agile Manager Administration site. In the Agile Manager application, system administrators have no default special privileges.

- To define a user as a system administrator, select the user row and click **Set as System Administrator**.

- To remove the system administrator role from a specific user, select the user row and click **Remove from System Administrators**.
- Find a specific user by entering all or part of a full or login name, or a phone number, in the **Filter** box.

User passwords

Use this page to reset passwords for users not managed in an LDAP system.

1. Select the user row and click **Reset User Password**.
2. Enter the new password and confirm it.

Configure advanced parameters

Tab: Configuration > Advanced Parameters

Note: Advanced parameters are system parameters that are defined together with HP customer support.

- Click **Add Parameter**, and enter the parameter's name and value.
- Sort parameters by column, or filter parameters by any matching text in the parameter's name, value, or description.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation and Administration Guide (Agile Manager 2.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-doc@hp.com.

We appreciate your feedback!

