HP Agile Manager

Software Version: 2.50

Installation and Administration Guide

Document Release Date: February 2016
Software Release Date: February 2016

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

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: https://softwaresupport.hp.com.

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to https://softwaresupport.hp.com and click **Register**.

Support

Visit the HP Software Support Online web site at: https://softwaresupport.hp.com

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: https://softwaresupport.hp.com and click **Register**.

To find more information about access levels, go to: https://softwaresupport.hp.com/web/softwaresupport/access-levels.

HP Software Solutions & Integrations and Best Practices

Visit **HP Software Solutions Now** at https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710 to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the **Cross Portfolio Best Practices Library** at https://hpln.hp.com/group/best-practices-hpsw to access a wide variety of best practice documents and materials.

Contents

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 the next page. Describes system components in basic and clustered configurations.
- "Linux prerequisites" on page 17. 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.
- "Installation and upgrade" on page 25. Describes detailed installation, upgrade, and uninstall procedures.
- "Start/Stop the Agile Manager service" on page 49. Lists commands for starting and stopping the Agile Manager service.
- "Log in to Agile Manager" on page 50. 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 51. Describes best practices and procedures for securing your Agile Manager system.
- "Manage the application server" on page 72. Describes optional procedures that are performed after installation to manage your Linux server.
- "Troubleshooting" on page 76. Describes the log files you should check if you encounter errors during your installation.
- "Agile Manager system administration" on page 78. 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 11
- "Clustered configuration example" on page 11
- "System requirements" on page 13

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	Stores the following Agile Manager schemas: • **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. The schemas reside on an Oracle server. For details, see "Oracle prerequisites" on page 19.
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 86.
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.

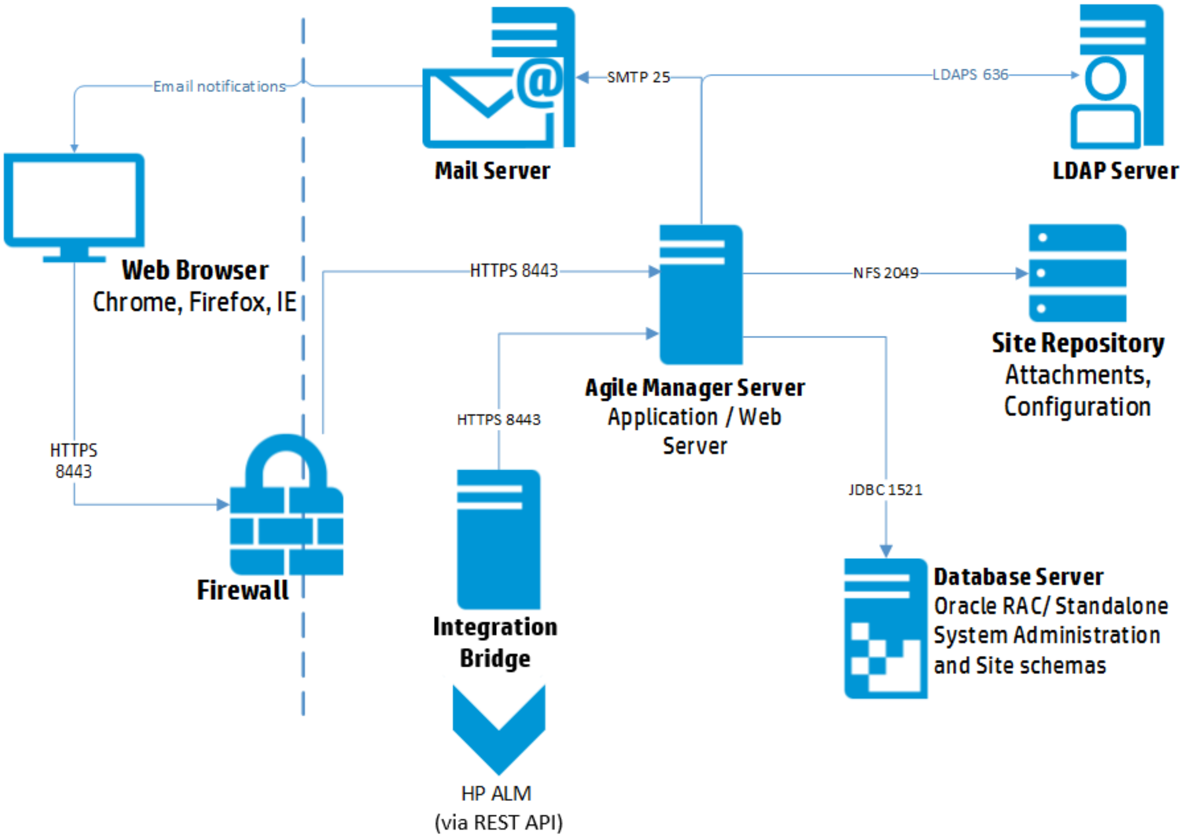
Component	Description
Site repository	Stores site files, such as attachments. By default, the repository is located on the same machine as the application server. This is useful for smaller setups. • **For larger organizations**, it is *advisable* to install the repository using a storage solution such as NAS (network-attached storage), SAN (storage area network), or a dedicated machine. • **In clustered configurations**, it is *required* to install the repository using a storage solution such as NAS, SAN, or a dedicated machine.
Integration Bridge	Optional. Used for NextGen Synchronizer. Communicates with ALM via the OTA API.
Tanuki wrapper	A Java service wrapper that allows Agile Manager to be installed and controlled. 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.



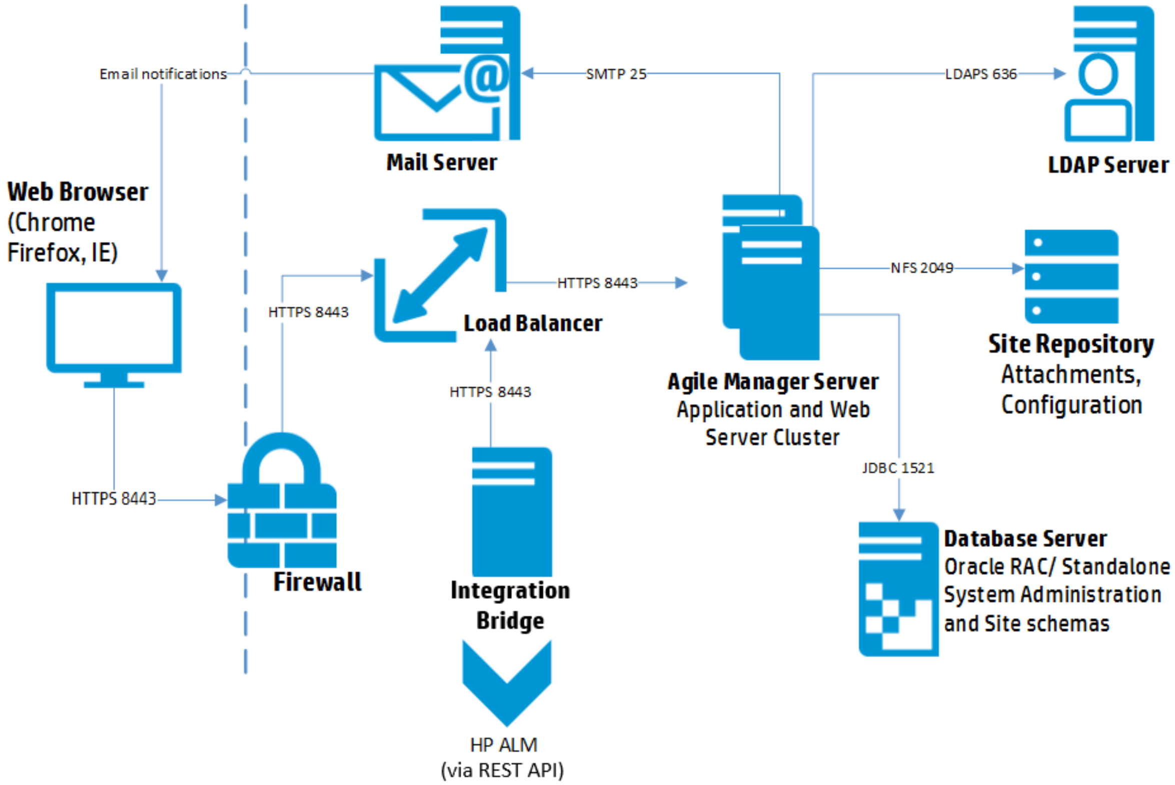
For more details, see "Agile Manager components" on page 9 and "Install Agile Manager" on page 27.

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 an large number of users.

The following diagram illustrates a clustered Agile Manager system configuration.


Email notifications
Mail Server
SMTP 25
LDAPS 636
LDAP Server
Web Browser (Chrome Firefox, IE)
HTTPS 8443
Load Balancer
HTTPS 8443
NFS 2049
Site Repository Attachments, Configuration
Agile Manager Server Application and Web Server Cluster
HTTPS 8443
HTTPS 8443
JDBC 1521
Firewall
Integration Bridge
Database Server Oracle RAC/ Standalone System Administration and Site schemas
HP ALM (via REST API)

For more details, see "Agile Manager components" on page 9 and "Install a clustered system" on page 38.

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.

Cluster considerations	
Shared resources	All nodes must have access to: - All database servers - The System Administration database schema - The site repository 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.

System requirements

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

This section includes details about the following:

Minimum hardware requirements

> **Note:** Minimum requirements are defined for basic systems and usage, without synchronization or ALI configured.
>
> For details about other configurations, see "Recommended hardware requirements" on the next page.

Component	Minimum requirements
Application server	- Dual Core CPU - 4 GB Memory (RAM) - Maximum 2 GB heap - Free disk space: 16 GB minimum

Database server	- Dual Core CPU - 4 GB Memory (RAM)

Recommended hardware requirements

Recommended hardware requirements are defined separately for the following system configurations:

- "Basic Agile Manager, without NextGen Synchronizer" below
- "Basic Agile Manager, with NextGen Synchronizer" below
- "Clustered Agile Manager, with NextGen Synchronizer" below

Basic Agile Manager, without NextGen Synchronizer

Component	Minimum requirements
Application server	- Quad Core CPU - 8 GB Memory (RAM) - Maximum 4 GB heap - Free disk space: 16 GB minimum
Database server	- 8 Core CPU - 16 GB Memory (RAM)

Basic Agile Manager, with NextGen Synchronizer

Component	Minimum requirements
Application server	- 16 Core CPU - 16 GB Memory (RAM) - Maximum 10 GB heap - Free disk space: 16 GB minimum
Database server	- 12 Core CPU - 32 GB Memory (RAM)

Clustered Agile Manager, with NextGen Synchronizer

Component	Minimum requirements

Application server	4 nodes, clustered. Each node has: • 8 Core CPU • 12 GB Memory (RAM) • Maximum 8 GB heap • Free disk space: 16 GB minimum
Database server	• 16 Core CPU • 64 GB Memory (RAM)

Additional system requirements

Agile Manager systems require the following, regardless of system configuration:

- "Application server TCP port requirements" below
- "Database size requirements" below
- "Supported environments" on the next page
- "Client machine requirements" on the next page

Application server TCP port requirements

8080 and 8443 are the default ports used for HTTP and HTTPS access.

> **Note:** Linux requires secure processes to use port numbers above 1024.
>
> Contact your system administrator to modify the process permissions and use lower ports.

Database size requirements

Configure your database server with a database sized as follows:

Configuration	Requirements
Without ALI	50 MB initial size; average projects may eventually reach 1 GB or more
With ALI	5 GB initial size

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.

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.

Supported environments

Operating system	Red Hat Enterprise Linux 6.2, 6.3, 6.4, or 6.5 (64 Bit) SUSE Linux Enterprise 11 Service Pack 3
Database	Oracle Database 11.2.0.4, Standard and Enterprise Editions. Oracle Database 12.1.0.1, Enterprise Edition. **Note:** PDB is not supported.

Client machine requirements

Supported browsers	Chrome 23 and above Firefox 16 and above Internet Explorer 10 and 11 **Note:** When working in Internet Explorer, make sure that the Chrome Frame plug-in is disabled.
Screen resolution	1920x1080 (recommended); 1680x1050 (supported)

Linux prerequisites

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

"Linux disk space requirements" below

"Linux server required permissions" below

> **See also:**
>
> - "System requirements" on page 13
> - "Oracle prerequisites" on page 19

Linux disk space requirements

Verify that your server machine meets the Agile Manager disk space requirements listed in "System requirements" on page 13.

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.

This user must have permissions to do the following:

- Run an RPM package installation
- Create local users (Optional. By default, the installation process creates a user who then runs the Agile Manager service. If necessary, you can prevent this creation. For more detail, see "Run the configuration wizard" on page 28.)
- Run the **su** command to switch users
- Register HPALM as a service in the Linux init system

> **Note:** In 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 who runs the Agile Manager service is the owner of the files. By default, this is **agml-user**. For more detail, see "Change the name of the service user (optional)" on page 28.
- On the Agile Manager machine, or on each cluster node, create a mount directory that points to the file repository directory.

Oracle prerequisites

This chapter describes prerequisites required for your Oracle database server.

"Database requirements" below

"Grant administrative user privileges" on the next page

"Enable Oracle RAC Support" on page 23

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

> **See also:**
>
> - "System requirements" on page 13
> - "Linux prerequisites" on page 17

Database requirements

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

Requirement	Description
Database connection	• Connection to the database server For details on securing the connection between Agile Manager and the database, see "Use SSL/TLS between system components" on page 56. • DNS resolution **Tip:** Test the DNS resolution by pinging the database server.
Database size	• **Without ALI.** 50 MB initial size; average projects may eventually reach 1 GB or more • **With ALI.** 5 GB initial size
Charset	• Set the database charset to **AL32UTF8**. • Set the following parameter value: **NLS_LENGTH_SEMANTICS=CHAR**

Requirement	Description
Database column length semantics	Column length must be defined according to characters, and not according to bytes. **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.
Tablespace name and size	• The tablespace names: **Default.** `qc_data` **Temporary.** `temp` • The minimum tablespace sizes for storing the System Administration database schema. Initial requirements are: **`qc_data.`** 20 MB **`temp.`** 50 MB • The tablespace must not be locked.
Clustered configuration or upgrade	To install Agile Manager on a second node in a clustered configuration, or when upgrading: • 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, we recommend that your database administrator create an Agile Manager administrator user, for example **agm_admin**, with the specific privileges required to install Agile Manager. If you need to install

> Agile Manager with lesser privileges, contact HP Customer Support.

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 agm_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.
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.

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.

User privileges	
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**.

User privileges after completing maintenance

- We recommend leaving permissions in place after completing installation, upgrade, or other maintenance procedures. ADMIN options can be removed.
- The CREATE SESSION permission is *required* for Agile Manager day-to-day functionality, although you can remove the ADMIN option for this permission as well.
- To perform any subsequent upgrades or other maintenance procedures, be sure to return any permissions and ADMIN options you have removed.

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.

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.

```
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.

Installation and upgrade

> **Note:** Before you start any installation or upgrade procedure, use the "Pre-installation checklist" on the next page to verify that you have all the details you need.

This guide describes the following types of installation procedures:

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 27.
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 page 38.
Upgrade a clustered production system	When upgrading a clustered production system, you'll need to upgrade Agile Manager on each node in the cluster. Start with "Upgrade a clustered system" on page 40.
Upgrade a basic production system	When upgrading your production system directly (without using a staging system), you'll need to follow steps and perform prerequisites specific to upgrades. Start with "Upgrade a basic production system" on page 44
Upgrade by first creating a staging system	When upgrading using a staging system, you'll need to manually copy files before and during the upgrade, and manually connect your staging system to those files. Start with "Upgrade Agile Manager using a staging environment" on page 47.

See also: "Uninstall Agile Manager" on page 39

Security enhancements for upgrades

To run Agile Manager as a simple user, with no special permissions, previous versions of Agile Manager required you to create an additional user for this purpose, named **agmuser**.

If you did this, and are now upgrading, you can delete this **agmuser** user as instructed during the upgrade.

Our upgraded installation process now creates its own non-root user, named **agml-user**. This user has limited privileges and is responsible for running the Agile Manager service.

- If you have a clustered configuration, you will need to create a network user with this name, and change the owner of the shared repository folder to this user, as instructed during the upgrade.
- To use a username other than **agml-user**, modify installation and configuration files after deploying. For details, see "Change the name of the service user (optional)" on page 28.

> **Note:** Upgrades support a user named **agml-user** only. If you modify this name, you will need to perform these steps again during any subsequent upgrades.

> **Caution:** The **agml-user** user is internal and should not be used explicitly, such as for login or running scripts of any kind.

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 13.

More details and optional pre-installation procedures are described in "Linux prerequisites" on page 17 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.

Pre-installation checklist	
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. **Tablespace.** Default tablespace selection.
System Administration	**System administration** System administration password. The default password is empty. You can modify this password during installation. 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 91. **System administration database schema** System administration database schema user name and password. 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.
File repository	Repository path • By default, the repository is configured in the deployment folder. • The user who runs Agile Manager must be the owner of the repository folder. In clustered configurations, we recommend you create a network user named **agml-user** to be the owner of this folder and to run the Agile Manager service. For details, see "Install a clustered system" on page 38.

Install Agile Manager

This section describes how to install and configure Agile Manager.

If you are installing a clustered system or upgrading, first see:

- "Install a clustered system" on page 38
- "Upgrade a basic production system" on page 44
- "Upgrade Agile Manager using a staging environment" on page 47
- "Upgrade a clustered system" on page 40

If you are installing Agile Manager as a non-root, sudo user, first see "Linux server required permissions" on page 17.

If you encounter problems during the installation process, see "Troubleshooting" on page 76 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 39.

1. **Deploy the installation files**

   Navigate to the directory where the rpm file is stored (for example, `cd /home`), and run one of the following:

As root user	`rpm --import keys/*.pub`
	`rpm -i Agile-Manager-ONPREM-<version number>.rpm`

As sudo user	`sudo rpm --import keys/*.pub`
	`sudo rpm -i Agile-Manager-ONPREM-<version number>.rpm`
	Note: For details about Agile Manager and sudo permissions, see "Linux server required permissions" on page 17.

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

2. **Change the name of the service user** (optional)

   By default, Agile Manager creates a user with limited permissions to run Agile Manager. This user is named **agml-user**.

   If you would like to modify this username, do the following:

   a. Browse to, and open the **/opt/hp/agm/conf/wrapper-user.conf** file for editing.

   b. Replace the string `agml-user` with the name of your service user. This can be a local user or an LDAP user.

      Agile Manager creates a user by this name. To instruct Agile Manager to use an existing user by this name and not create it, see step #3.

      > **Caution:** Do not enter `root` as the user name.

3. **Run the configuration wizard**

   Open the directory in which the Agile Manager files are deployed

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

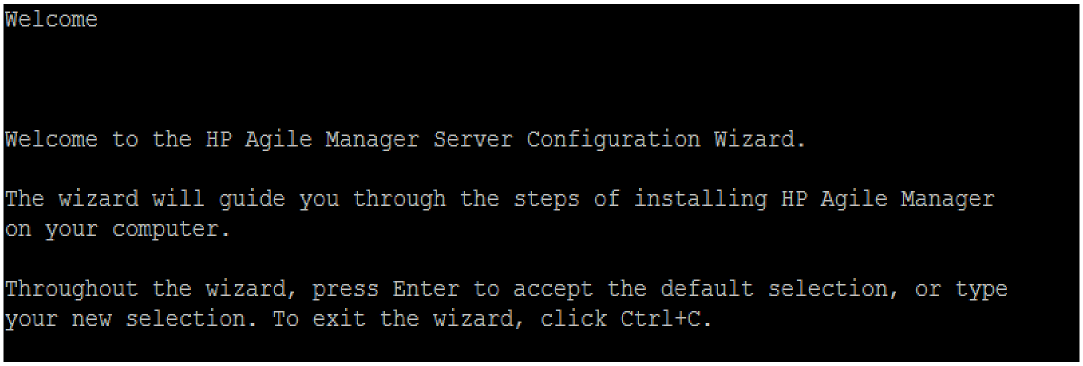
Run one of the following commands:

As root user	`./run_config.sh`
As sudo user	`sudo ./run_config.sh`

Note:

- To instruct Agile Manager to use an existing user to run the service instead of creating a new user, use the **-noUserCreation** flag:
  `./run_config.sh -noUserCreation`
  Agile Manager uses the user that you defined in the **/opt/hp/agm/conf/wrapper-user.conf** file.
- 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.

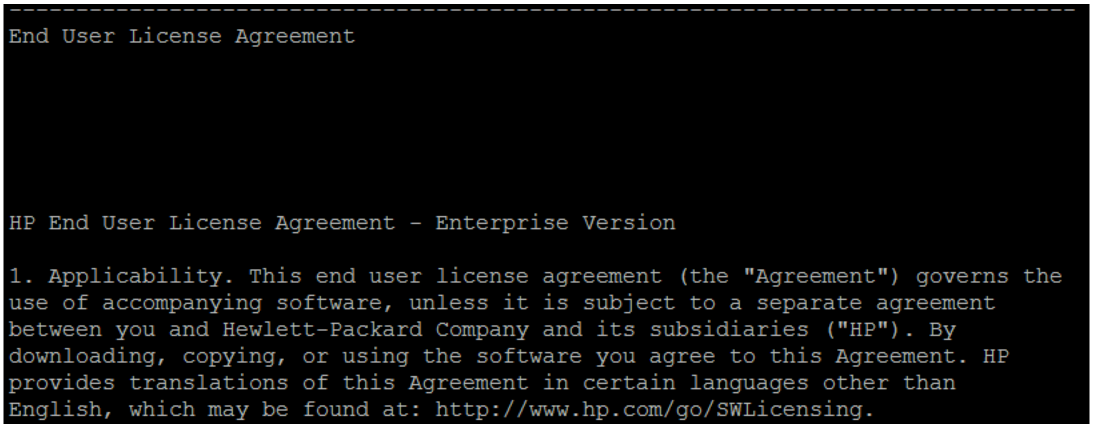
The Agile Manager configuration wizard opens.



```
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.
```

4. **Accept the EULA**

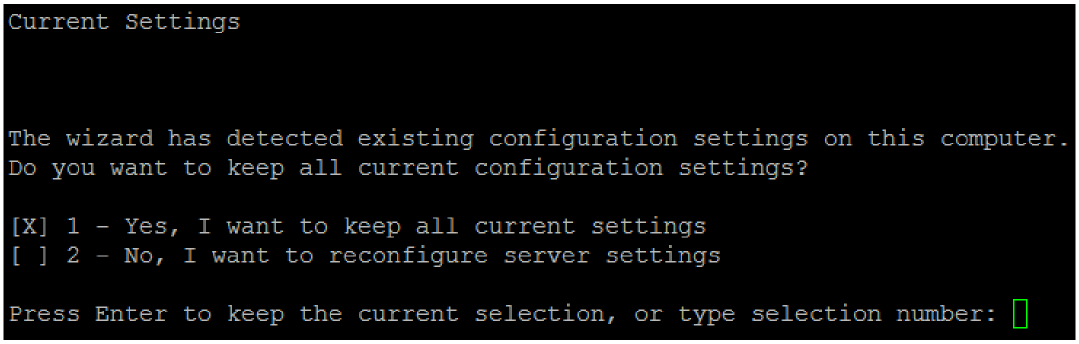
   The Agile Manager EULA is displayed. Read through the EULA and accept its terms to continue.



```
-------------------------------------------------------------------------------
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.
```

5. **Reuse detected settings**

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



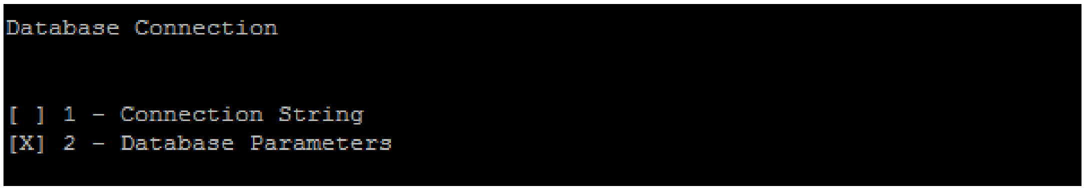
```
Current Settings


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 38.
> - If you are upgrading a system, you must have uninstalled the previous version of Agile Manager and renamed this file. For details, see "Upgrade a basic production system" on page 44.

   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.

6. **Enter database parameters**

   Select whether you want to enter your database parameters as a connection string, or individually. To configure SSL, as described below, select Connection String.



```
Database Connection


[ ] 1 - Connection String
[X] 2 - Database Parameters
```

   Then enter the connection data, as a string, or as prompted.

   When entering data as parameters, press **ENTER** after entering each of the following:

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

If you use an ORA configuration file to define your database addresses, use a connection string for this step.

> The following is an example of a connection string built from an ORA file and service name:
>
> ```
> jdbc:mercury:oracle:TNSNamesFile=/<path>;TNSServerName=<name>
> ```
>
> where:
>
> - `jdbc:mercury:oracle` is required
> - `<path>` = the path to the tnsnames.ora file
> - `<name>` = the name of the TNS server

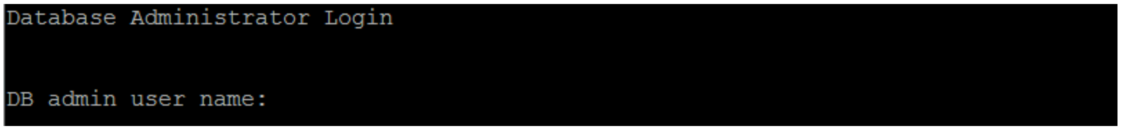
You can configure a secured connection between Agile Manager and the Oracle database. For details, see "Use SSL/TLS between system components" on page 56.

In this case, use a connection string for this step, and add the following parameters:

Parameter	Description
EncryptionMethod	SSL
TrustStore	The full path to the client certificate (wallet) file. For example: `/Wallets/client_wallet/ewallet.p12`.
TrustStorePassword	The password used to protect the certificate.

> The following is an example of a connection string used for an SSL connection with the database:
>
> ```
> jdbc:mercury:oracle://<DBHostname>:2484;sid=<SID>;EncryptionMethod=SSL;TrustStore=<certificate_folder>/ewallet.p12;TrustStorePassword=<password>
> ```
>
> where:
>
> - `jdbc:mercury:oracle` is required
> - `<DBHostname>` = the database server host name
> - `<SID>` = the Oracle system identifier
> - `certificate_folder` = the folder containing the certificate file
> - `<password>` = the key-store password for the certificate file

7. **Enter database administrator login information**

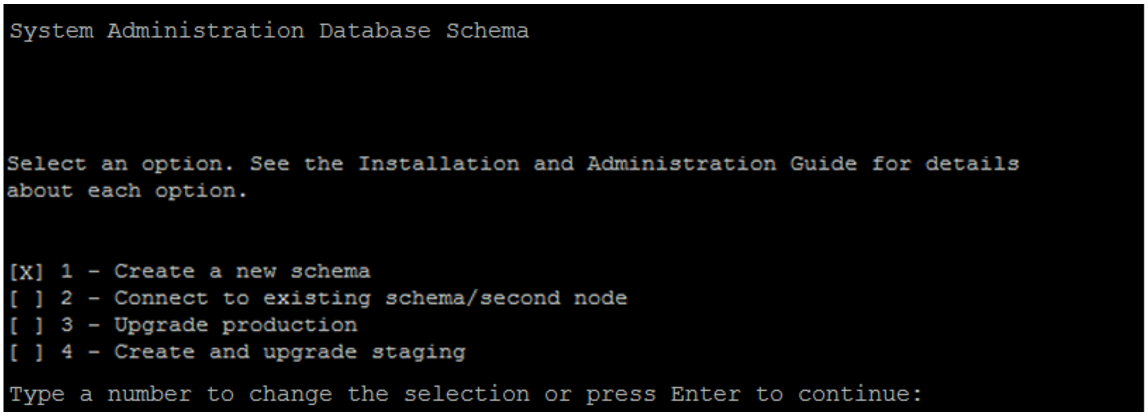


```
Database Administrator Login


DB admin user name:
```

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

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.

8. **Select a database schema option**



```
System Administration Database Schema



Select an option. See the Installation and Administration Guide for details
about each option.


[X] 1 - Create a new schema
[ ] 2 - Connect to existing schema/second node
[ ] 3 - Upgrade production
[ ] 4 - Create and upgrade staging
Type a number to change the selection or press Enter to continue:
```

Select one of the options displayed. Click the relevant link below to jump to more details about each option.

- "Create a new schema" below
- "Connect to existing schema / second node" below
- "Upgrade production" on the next page
- "Create and upgrade staging" on the next page
- **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.

- **Connect to existing schema / second node**

  Enables you to connect to an existing System Administration database schema.

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.

> **Caution:** If you are installing or upgrading a cluster, first see "Install a clustered system" on page 38 or "Upgrade a clustered system" on page 40.

In the rest of the configuration wizard, continue to use the existing data, except when defining the confidential data passphrase. Continue with "Enter a confidential data passphrase" on page 35 and then "Review the settings" on page 37.

- **Upgrade production**

  Creates a copy of the existing system administration database schema and upgrades the copy, and automatically connects to the existing Agile Manager site.

  > **Caution:** This option is relevant for upgrades to production systems only.
  >
  > Do *not* select this option if you would like to test the upgrades on a separate system before upgrading your production system.
  >
  > If you are performing "Upgrade Agile Manager using a staging environment" on page 47, select "Create and upgrade staging" below instead.

  After selecting **Upgrade production**, do the following when prompted:

  i. Enter or accept the provided values for the old system administration schema name and password.

  ii. Enter a name for the new system administration schema.

  In the rest of the configuration wizard, continue to use the existing data, except when defining the confidential data passphrase. Continue with "Enter a confidential data passphrase" on page 35 and then "Review the settings" on page 37.

- **Create and upgrade staging**

  Creates a copy of the existing system administration database schema and upgrades the copy, but does not connect to any Agile Manager site.

  Instead, this option creates a blank system that you can use as a staging environment before upgrading your production environment.

  > **Caution:** Select this option *only* while performing the "Upgrade Agile Manager using a staging environment" on page 47 procedure.

After selecting **Create and upgrade staging**, do the following when prompted:

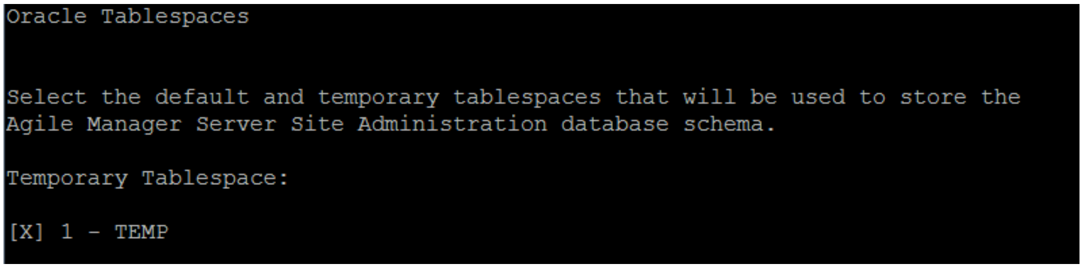
i. Enter or accept the provided values for the old system administration schema name and password.

ii. Enter a name for the new system administration schema.

In the rest of the configuration wizard, continue to use the existing data, except when defining the confidential data passphrase. Continue with "Enter a confidential data passphrase" on the next page and then "Review the settings" on page 37.

9. **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
```

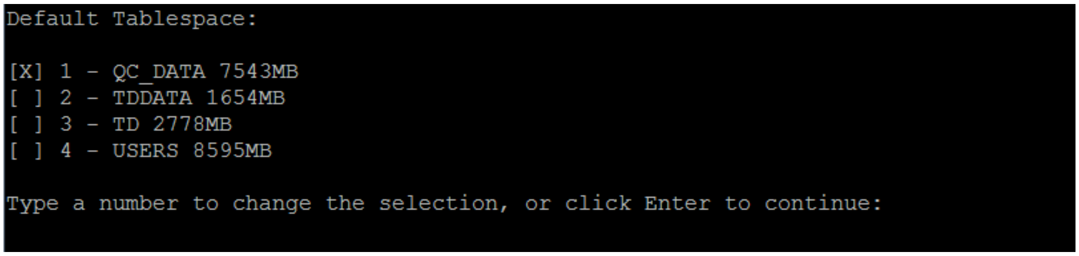
   Press **ENTER** to select the default **TEMP** directory.

10. **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 36.

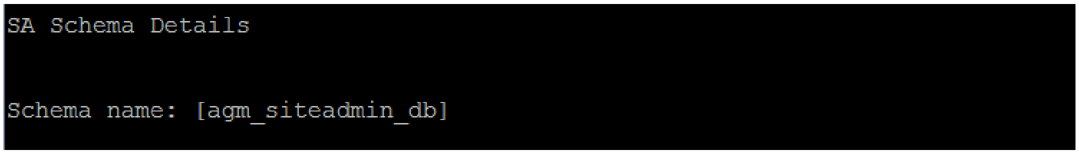
    The following screenshot is an example. Outputs will vary depending on your database structure.



```
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.

11. **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 production** above, the **New Schema Name** option appears. Type a name for the upgraded copy of the System Administration database schema.

   > **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.

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.

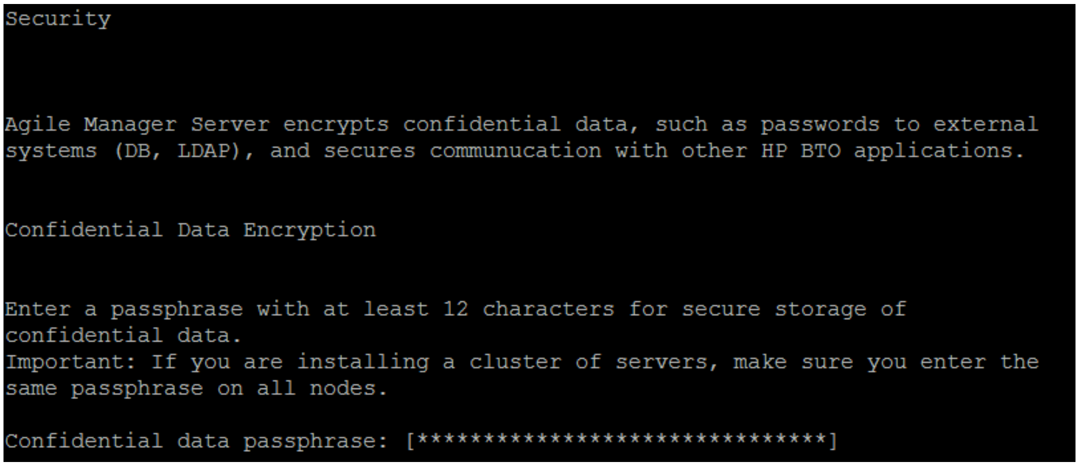
c. If you selected **Create a new schema** above, the licensing option appears.

   Agile Manager is installed with a trial **Instant On** license. Select whether you would like this license to support **concurrent** or **named** users.

   > **Note:** We recommend keeping the default concurrent licenses.

   For more details, see "Update user licenses" on page 89.

12. **Enter a confidential data passphrase**



```
Security


Agile Manager Server encrypts confidential data, such as passwords to external
systems (DB, LDAP), and secures communucation 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.

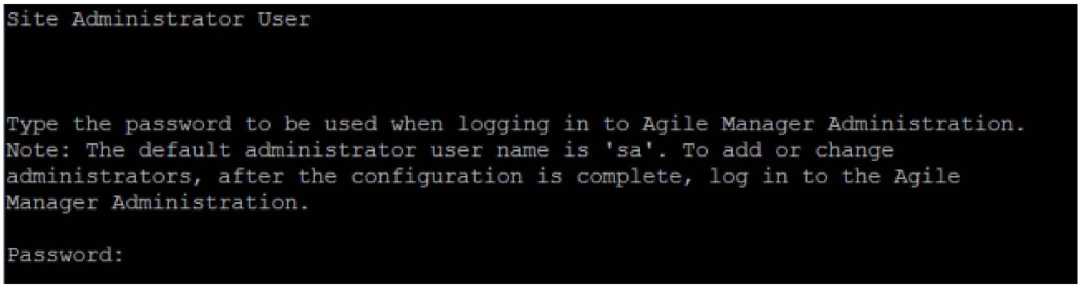
You can also select to use the default value of `Seashells Grow Like Misty Tunas`.

> **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.

13. **Enter system administrator login information**



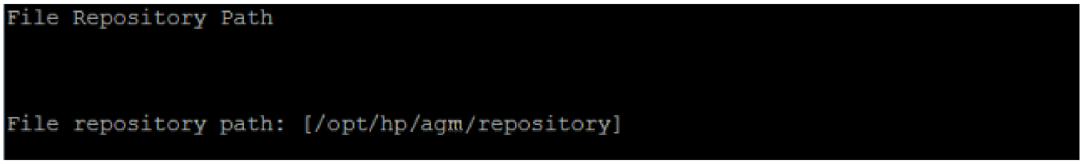
```
Site Administrator User


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.

14. **Enter the file repository path**

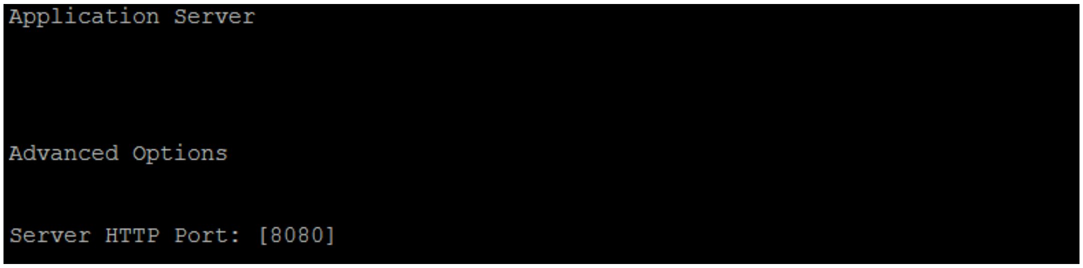


```
File Repository Path


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

Accept the default path or enter a new path.

> **Tip:** See "File repository" on page 27 for guidelines about defining this path.

15. **Verify that the application server port is free**

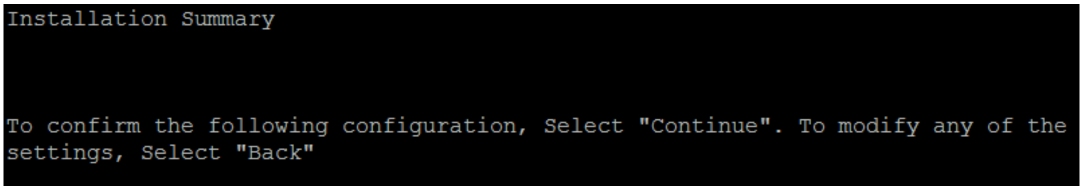


```
Application Server



Advanced Options


Server HTTP Port: [8080]
```

Accept the default (8080), or enter a new one.

> **Note:** If you modify this port number, note that Linux requires secure processes to use port numbers above 1024.
>
> Contact your system administrator to modify the process permissions and use lower ports.

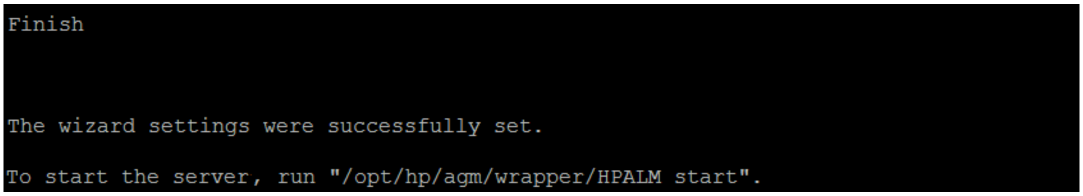
16. **Review the settings**



```
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.

17. **Complete the configuration**



```
Finish


The wizard settings were successfully set.

To start the server, run "/opt/hp/agm/wrapper/HPALM start".
```

Start the server as prompted. For more details, see "Start/Stop the Agile Manager service" on page 49.

> **Note:** The first time that the server is started, a new database schema is created for Agile Manager. This schema is named **t1_sa_main_db**.

18. When the service is up, continue by logging in to Agile Manager or the Agile Manager System Administration site. For details, see "Log in to Agile Manager" on page 50.

- For security best practices and procedures, see "Secure your system" on page 51.
- For other server and system management details, see "Manage the application server" on page 72 and "Agile Manager system administration" on page 78.

> **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 72.

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 17 and "Oracle prerequisites" on page 19.

1. **Create a shared network user**

   Create a network user, such as an NIS or LDAP user, that will be used as the owner of the a shared repository, accessible by all nodes, as well as to run the Agile Manager service.

   > **Note:** We recommend that this user be named **agml-user**. If you use a different name, be sure to perform "Modify the shared network user in Agile Manager system files (optional)" on the next page.

2. **Create and mount a shared file repository**

   Create a shared repository folder, and define its owner as the user you created in the previous step.

   For example, use the following command: `chown agml-user -R /opt/hp/agm/repository`

   - Mount this repository on each node. 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. We recommend using the following mount name on all nodes: **/opt/hp/agm/repository**

3. **Deploy the installation files on all nodes**

   For details, see "Deploy the installation files" on page 28.

4. **Modify the shared network user in Agile Manager system files** (optional)

   We recommend that the name of the shared network user be `agml-user`.

   To use a different name for this user, modify it in the system files **on all nodes** before configuring Agile Manager. For details, see "Change the name of the service user (optional)" on page 28.

5. **Configure Agile Manager on the first node**

   For details, see "Run the configuration wizard" on page 28. When defining the repository path, enter the shared folder you created earlier.

6. **Configure Agile Manager on all other nodes**

   a. Copy the **/opt/hp/agm/conf/qcConfigFile.properties** file from the first node to the same folder on all other nodes.

   b. On each of the other nodes, run the Agile Manager configuration wizard.

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

      - **Keep all current settings**
      - **Connect to an existing schema/second node**

      For details, see "Run the configuration wizard" on page 28 and "Connect to existing schema / second node" on page 32.

   c. Start Agile Manager after configuration is complete.

7. **Verify your installation**

   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 50.

8. **Configure an external URL for use in emails sent from Agile Manager**

   This step is relevant if you configure an email server for notification emails. For details, see "Configure an external URL for use in emails." on page 85.

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. Uninstall Agile Manager: `rpm -e Agile-Manager`

Caution: By default, the following files and directories are not deleted from your machine:

- the **conf**, **log**, **repository**, and **wrapper** directories
- the **webapps/qcbin/WEB-INF/siteadmin.xml** file

These files and directories are used during upgrades. Do not delete these files if you have subsequent upgrades planned.

Note: 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.

3. (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.

Upgrade a clustered system

This section describes how to upgrade Agile Manager in a clustered configuration. For details about upgrading a basic, standalone system, see "Upgrade a basic production system" on page 44.

If you would like to test the upgrades on a separate system before upgrading your production system, see "Upgrade Agile Manager using a staging environment" on page 47 instead.

This section includes the following:

1. "Prerequisites" on the next page
2. "Steps to perform on the first node only" on the next page
3. "Steps to perform on all nodes other than the first" on page 43

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.

Prerequisites

1. **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 13
   - "Linux prerequisites" on page 17
   - "Oracle prerequisites" on page 19

2. **Stop Agile Manager.**

   Stop the Agile Manager service on all nodes: `/opt/hp/agm/wrapper/HPALM stop`

   > **Note:** Customers upgrading from Agile Manager 2.20 installed on SUSE environments may see warnings about non-existent folders after starting or stopping the service. Such warnings can be ignored.

Steps to perform on the first node only

1. **Delete the agmuser user** (optional)

   If you previously created a simple user named **agmuser** to run Agile Manager with no special permissions, you can now delete this user. The current installation creates a user, named **agml-user**, which is used as the service user.

   To use a different name for this user, or to instruct Agile Manager to use an existing user, follow the relevant instructions during installation and configuration. For details, see "Change the name of the service user (optional)" on page 28.

2. **Create a shared network user for shared repository access**

   a. Create a network user, such as an NIS or LDAP user, that will be used as the owner of the shared repository, accessible by all nodes, as well as to run the Agile Manager service.

   > **Note:** We recommend that this user be named **agml-user**.
   >
   > To use a different name for this user, modify it during the installation and configuration procedure. For details, see "Modify the shared network user in Agile Manager system files (optional)" on page 43.

   a. Define this network user as the owner of the shared repository folder. For example: `chown -R agml-user /mnt/sharedfolder`

3. **Back up your data**

   - Back up your database schema and site repository before upgrading.

     > **Caution:** 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.

   - Back up the following system files by saving them outside of the **/opt/hp** directory:
     - `/opt/hp/agm/server/conf/jetty.xml`
     - `/opt/hp/agm/java/jre/lib/security/cacerts` (SSL/TLS configurations only)
   - If you have modified the **Max DB Connections** value from the default, record the current value. Upgrades restore the default value and any modifications will be lost.

     This value is defined in the Agile Manager System Administration site, on the **Servers** > **Application** tab. For details, see "Configure maximum database connections" on page 79.

4. **If you have SSL/TLS configured, locate and/or back up the server.keystore file**

   Open the `jetty.xml` file to determine where the `server.keystore` is saved.

   If this file is saved in the `/opt/hp/agm` directory, or any of its sub-directories, back up the file by saving it outside of the **/opt/hp** directory.

5. **Install the new version of Agile Manager**

   Copy the rpm and key 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 (for example, `cd /home`), and run one of the following:

As root user	`rpm --import keys/*.pub`
	`rpm –U AGM-ONPREM<version number>.rpm`

As sudo user	`sudo rpm --import keys/*.pub`
	`sudo rpm -U AGM-ONPREM<version number>.rpm`

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

6. **Restore backed up files**

   Restore the following files you backed up earlier:

   - `/opt/hp/agm/server/conf/jetty.xml`
   - `/opt/hp/agm/java/jre/lib/security/cacerts` (SSL/TLS configurations only)
   - `server.keystore` (if needed, for SSL/TLS configurations only)

> **Caution:** If you are upgrading from a version earlier than 2.40: If you changed the **wrapper.java.maxmemory** property in the **wrapper.conf** file in the previous release, manually migrate this change to the **/opt/hp/agm/conf/wrapper-install.conf** file.

7. **Modify the shared network user in Agile Manager system files** (optional)

   We recommend that the name of the shared network user be `agml-user`.

   To use a different name for this user, modify it in the system files **on all nodes** before configuring Agile Manager. For details, see "Change the name of the service user (optional)" on page 28.

8. **Run the configuration wizard and complete the configuration**

   For details, start with "Run the configuration wizard" on page 28.

   Use the same configuration details you used in the previous installation, except:

   In the **System Administration Database Schema** screen, select **Upgrade production**. For details, see "Upgrade production" on page 33.

> **Caution:** Do not select this option if you would like to test the upgrades on a separate system before upgrading your production system. To test the upgrades, start from "Upgrade Agile Manager using a staging environment" on page 47 instead.

> **Note:** Note the name of the new, upgraded schema. You will need this name when upgrading the other nodes.

Steps to perform on all nodes other than the first

1. If you have modified the **Max DB Connections** value from the default, record the current value. Upgrades restore the default value and any modifications will be lost.

   This value is defined for each server, in the Agile Manager System Administration site, on the **Servers** > **Application** tab. For details, see "Configure maximum database connections" on page 79.

2. **Install the new version of Agile Manager**

   Copy the rpm and key 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 (for example, `cd /home`), and run one of the following:

As root user	`rpm --import keys/*.pub`
	`rpm –U AGM-ONPREM<version number>.rpm`

As sudo user	`sudo rpm --import keys/*.pub`
	`sudo rpm -U AGM-ONPREM<version number>.rpm`

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

3. **Copy files from the first node to all other nodes**

   Copy the following files from the first node to the same location on all other nodes:

   - `/opt/hp/agm/server/conf/jetty.xml`
   - `/opt/hp/agm/java/jre/lib/security/cacerts` (SSL/TLS configurations only)
   - `server.keystore` (if needed, for SSL/TLS configurations only). Copy this file to the location defined in the `jetty.xml` file.
   - `/opt/hp/agm/conf/qcConfigFile.properties`
   - `/opt/hp/agm/conf/wrapper-install.conf`
   - `/opt/hp/agm/conf/wrapper-user.conf`

4. **Run the configuration wizard and complete the configuration**

   For details, start with "Run the configuration wizard" on page 28.

   Use the same configuration details you used in the previous installation, except:

   In the **System Administration Database Schema** screen, select **Connect to existing schema / second node**.

   For details, see "Connect to existing schema / second node" on page 32.

5. **Update your Max DB Connections value** (optional)

   If you had previously modified the **Max DB Connections** value, the default value is restored after the upgrade.

   Log in to the Agile Manager System Administration site and modify the value on the **Servers** > **Application** page, for each server in the cluster.

   For details, see "Configure maximum database connections" on page 79.

> **Note:** After the upgrade is complete, if you configure an email server for notifications emails, also configure an external URL for use in those emails.
>
> For details, see "Configure an external URL for use in emails." on page 85.

Upgrade a basic production system

This section describes how to upgrade Agile Manager in a basic, standalone configuration.

- For details about upgrading a clustered system, see "Upgrade a clustered system" on page 40.
- If you would like to first create and upgrade a blank system to use as a staging environment, see "Upgrade Agile Manager using a staging environment" on page 47.

> **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.

1. **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 13
   - "Linux prerequisites" on page 17
   - "Oracle prerequisites" on page 19

2. **Stop Agile Manager**

   Stop the Agile Manager service: `/opt/hp/agm/wrapper/HPALM stop`

   > **Note:** Customers upgrading from Agile Manager 2.20 installed on SUSE environments may see warnings about non-existent folders after starting or stopping the service. Such warnings can be ignored.

3. **Back up your data**

   - Back up your database schema and site repository before upgrading.

     > **Caution:** 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.

   - Back up the following system files:
     - `/opt/hp/agm/server/conf/jetty.xml`
     - `/opt/hp/agm/java/jre/lib/security/cacerts` (SSL/TLS configurations only)
   - If you have modified the **Max DB Connections** value from the default, record the current value. Upgrades restore the default value and any modifications will be lost.

     This value is defined in the Agile Manager System Administration site, on the **Servers** > **Application** tab. For details, see "Configure maximum database connections" on page 79.

4. **If you have SSL/TLS configured, locate and/or move the server.keystore file**

   Open the `jetty.xml` file to determine where the `server.keystore` is saved.

   If this file is saved in the `/opt/hp/agm` directory, or any of its sub-directories, back up the **server.keystore** file.

5. **Install the new version of Agile Manager**

Copy the rpm and key 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 (for example, `cd /home`), and run one of the following:

As root user	`rpm --import keys/*.pub`
	`rpm –U AGM-ONPREM<version number>.rpm`

As sudo user	`sudo rpm --import keys/*.pub`
	`sudo rpm -U AGM-ONPREM<version number>.rpm`

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

6. **Delete the agmuser user** (optional)

   If you previously created a simple user named **agmuser** to run Agile Manager with no special permissions, you can now delete this user. The current installation creates a user, named **agml-user**, which is used as the service user.

   To use a different name for this user, or to instruct Agile Manager to use an existing user, follow the relevant instructions during installation and configuration. For details, see "Change the name of the service user (optional)" on page 28.

7. **Restore backed up files**

   Restore the following files you backed up earlier:

   - `/opt/hp/agm/server/conf/jetty.xml`
   - `/opt/hp/agm/java/jre/lib/security/cacerts` (SSL/TLS configurations only)
   - `server.keystore` (if needed, for SSL/TLS configurations only)

   > **Caution:** If you are upgrading from a version earlier than 2.40: If you changed the **wrapper.java.maxmemory** property in the **wrapper.conf** file in the previous release, manually migrate this change to the **/opt/hp/agm/conf/wrapper-install.conf** file.

8. **Run the configuration wizard and complete the configuration**

   For details, start with "Run the configuration wizard" on page 28.

   When running the configuration wizard, use the same configuration details you used in the previous installation, with the following exceptions:

   - In the **System Administration Database Schema** screen, select **Upgrade production**. For more details, see "Upgrade production" on page 33.

     > **Caution:** Do not select this option if you would like to test the upgrades on a separate system before upgrading your production system. To test the upgrades, see "Upgrade Agile Manager using a staging environment" on the next page instead.

- If you previously modified the application port to a number lower than 1024, note that Linux requires secure processes to use port numbers above 1024.

  Modify this port number, or contact your system administrator to modify the process permissions and use lower ports. For details, see "Verify that the application server port is free" on page 37.

9. **Update your Max DB Connections value** (optional)

   If you had previously modified the **Max DB Connections** value, the default value is restored after the upgrade. Log in to the Agile Manager System Administration site and modify the value on the **Servers** > **Application** page.

   For details, see "Configure maximum database connections" on page 79.

Upgrade Agile Manager using a staging environment

When upgrading your Agile Manager system, you may want to first create a blank system with the new version to use as a staging environment.

To do this, you will need a separate application server. You may also choose to use a separate database server.

1. Manually copy both the system administration schema and site schema to the staging database server.

   You can find the names of these schemas listed in the System Administration site, on the **Servers** > **Database** tab, under **General Information**. For details, see "Configure database settings" on page 82.

2. On the staging application server, deploy Agile Manager. For details, see "Deploy the installation files" on page 28.

3. The installation creates a user, named **agml-user** to run the Agile Manager service.

   To use a different name for this user, or to instruct Agile Manager to use an existing user, follow the relevant instructions during installation and configuration. For details, see "Change the name of the service user (optional)" on page 28.

4. Manually copy the repository to the staging application server.

   You can find the path to the repository listed in the System Administration site, on the **Servers** > **Database** tab, under **General Information**. For details, see "Configure database settings" on page 82.

   On the staging application server, verify that the **repositoryPath** property in the **/opt/hp/agm/conf/qcConfigFile.properties** file points to the correct location in the repository.

   If the **qcConfigFile.properties** file does not contain this property, add it manually, with the correct location.

5. On the staging application server, run the configuration wizard. For details, see "Run the configuration wizard" on page 28.

   While running the configuration wizard, keep the default values, except for the following:

Wizard screen	Enter.../Select...
Database Connection and **Database Administrator Login**	Provide details for the staging database server. These may or may not be the same as the original values. For details, see "Enter database parameters" on page 30 and "Enter database administrator login information" on page 32.
System Administration Database Schema	Select **Create and upgrade staging**. For details, see "Create and upgrade staging" on page 33.

6. Continue with the steps to complete the configuration wizard, and then start Agile Manager. For details, see "Start/Stop the Agile Manager service" on the next page.

   > **Note:** After this process, Agile Manager uses the default port number (8080). If necessary, "Change the application server port number" on page 73 before you start Agile Manager.

7. Access the System Administration site, and use the **Restore Site Schema** option to connect your staging environment to the site schema that you copied. For details, see "Restore a site schema" on page 83.

Deploy installation to an alternate location

Deploying installation files is the first step in installing or upgrading Agile Manager.

By default, installation files are deployed under **/opt/hp/agm**. This is the recommended location.

If you must deploy to a different location, use the `--prefix` option to specify this location.

For example:

```
rpm -i --prefix /opt/MyInstallPath Agile-Manager-ONPREM-<version number>.rpm
```

The installation files are deployed under an **agm** folder within the folder that you specify.

For more details, see "Deploy the installation files" on page 28.

> **Caution:** When upgrading Agile Manager, always upgrade to the same folder as the previous installation. For example: `rpm -U --prefix /opt/MyInstallPath Agile-Manager-ONPREM-<version number>.rpm`

Start/Stop the Agile Manager service

Action	Command (as root or sudo)
Start the service	As **root**. `/opt/hp/agm/wrapper/HPALM start` As **sudo**. `sudo /opt/hp/agm/wrapper/HPALM start`
Stop the service	As **root**. `/opt/hp/agm/wrapper/HPALM stop` As **sudo**. `sudo /opt/hp/agm/wrapper/HPALM stop`
Restart the service	As **root**. `/opt/hp/agm/wrapper/HPALM restart` As **sudo**. `sudo /opt/hp/agm/wrapper/HPALM restart`

For details about Agile Manager and sudo permissions, see "Linux prerequisites" on page 17.

Note:

- The first time that the server is started, a new database schema is created for Agile Manager. This schema is named **t1_sa_main_db**.
- Customers upgrading from Agile Manager 2.20 installed on SUSE environments may see warnings about non-existent folders after starting or stopping the service. Such warnings can be ignored.

Start the Agile Manager service after reboot

By default, Agile Manager starts when the system boots.

To remove this registration, run	As **root**. `/opt/hp/agm/wrapper/HPALM remove` As **sudo**. `sudo /opt/hp/agm/wrapper/HPALM remove`
To return this registration, run	As **root**. `/opt/hp/agm/wrapper/HPALM install` As **sudo**. `sudo /opt/hp/agm/wrapper/HPALM install`

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://<server>:<port>/agm/admin`

If you access Agile Manager via a reverse proxy, use the proxy address as the server address. For details, see "Integrate an Apache web server (example)" on page 69.

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 36).

To fully benefit from Agile Manager's rich feature set, access the *Help Center* (in the header, click ?) or join the discussion at Hewlett Packard Enterprise Software forums and blogs.

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`.
- If you are upgrading, and selected **Create and upgrade staging** in the configuration wizard, Agile Manager is not accessible. First, perform "Install Agile Manager" on page 27.

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.

We strongly recommend using the latest supported browser version to access Agile Manager. This will help you avoid known security flaws on outdated browser versions. For a list of supported browsers and browser versions, see the *Agile Manager User Guide*.

> **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 54
- "Secure system administration" on page 58
- "Secure user authorization" on page 60
- "Data encryption" on page 63
- "Integrate an Apache web server (example)" on page 69
- "Secure attachment files and downloads" on page 53
- "Secure the network and communication" on page 56
- "Secure user authentication" on page 59
- "Data integrity" on page 62
- "Data logging" on page 64

Additionally, you can configure SSL/TLS connections on the application, LDAP, and SMTP servers. Secure connections to the database server are not supported.

For details, see

- "Configure SSL/TLS on the application server" on page 65
- "Configure SSL/TLS on the LDAP server" on page 86
- "Configure SSL/TLS on the SMTP server (optional)." on page 84

By default, the database user installing Agile Manager must have sufficient privileges to perform certain administrative tasks in Oracle. For details, see "Grant administrative user privileges" on page 20. To install Agile Manager with lesser privileges, contact HP Customer Support.

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 is run using a non-root user, created by Agile Manager during installation. By default, this user is named **agml-user**, and has limited privileges for running the Agile Manager service only. You can modify the user name, and you can also instruct Agile Manager to use an existing user rather than creating a new one.

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/TLS	**Basic configuration.** Enable SSL/TLS on the Agile Manager Jetty and make it required. **Clustered configuration.** Require SSL/TLS for the Agile Manager virtual IP on the load balancer. For details, see: • "Configure SSL/TLS on the application server" on page 65 • "Configure SSL/TLS on the LDAP server" on page 86 • "Configure an email notification server" on page 84 **Note:** Secure connections to the database server are not supported.
Reverse proxy	Install a reverse proxy in front of the Agile Manager server, and then configure SSL/TLS on the reverse proxy server. For details, see "Reverse proxy architecture" on page 57 and "Integrate an Apache web server (example)" on page 69. For details about enabling SSL/TLS for all interactions with Apache, see http://httpd.apache.org/docs/current/ssl/ssl_howto.html. **Note:** When configuring a reverse proxy, also configure an external URL for use in emails sent from Agile Manager. For details, see "Configure an external URL for use in emails." on page 85.

Secure deployment methods	
Firewall	Use a firewall between the client and the other Agile Manager components. On the application server, block access to all incoming traffic except for the HTTP port (8080) or HTTPS port (8443) used by Agile Manager.

See also: "Secure the network and communication" on page 56

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, we recommend using SSL/TLS 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/TLS 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/TLS.
>
> Currently, a secure channel to the database server from Agile Manager is not supported.

Secure attachment files and downloads

This topic includes:

- "Secure attachment files" below
- "Secure downloads" on the next page

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)**
- **Maximum aggregated size for all attachments (MB)**
- **Blocked file extensions files types**

For details, see "Define attachment settings" on page 93.

> **Caution:**
>
> Attachment files can contain dangerous content, and must be downloaded and opened with caution.
>
> We strongly recommend implementing anti-virus protection for the file storage allocated for both the Agile Manager server and client machines

Secure downloads

NextGen Synchronizer's Integration Bridge supports synchronizing Agile Manager with ALM.

The first time you install the Integration Bridge, download it manually from Agile Manager. Subsequent upgrades take place automatically, downloading the bridge, verifying its authenticity, and upgrading the installation.

For more information, see the *Agile Manager Synchronization Guide*.

If your corporate rules prohibit automatic downloads, you can disable the automatic upgrades by setting the OPB_ENABLE_AUTO_UPGRADE system parameter to N. For details, see "Configure advanced parameters" on page 93.

In this case, whenever a new Agile Manager version includes an upgrade to the Integration Bridge, any existing synchronization bridges will stop running until they are manually upgraded.

Secure the application server

The Agile Manager installation process creates a local user, named **agml-user**, which has minimal privileges. This user is unable to log in to the server, and is used for security purposes only.

- The Agile Manager service runs using the **agml-user** user privileges.
- The **agml-user** is the owner of only a minimal set of directories, required for server operation. All other directories are owned by the **root** user.

Additional steps

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

- When configuring SSL/TLS 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 SSL/TLS on the application server" on page 65.
- 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.
- If you configure a mail server, Agile Manager sends emails to users that include links to Agile Manager. These emails might expose the actual machine names.

  Examples of such emails include when users send an entity to another user directly from within Agile Manager, or when new users receive a welcome email, inviting them to log in.

  To hide the actual machine names, add the **EXTERNAL_BASE_URL** advanced parameter on the **Advanced Parameters** page of the System Administration site. Define the value as the external URL you would like to appear in the emails.

  For example: `http://my-load-balancer-domain:8080/`

  > **Note:** Do not add `agm` to the end of the URL.

  For more details, see "Configure an email notification server" on page 84 and "Configure advanced parameters" on page 93.

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.

Question	Answer
Does Agile Manager ensure that configuration files are not stored in the same directory as user data?	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. Change the repository path on the **Servers** > **Database** page, and the log file path on the **Servers** > **Application** page. For details, see "Configure database settings" on page 82 and "Configure application server settings" on page 79.
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
- "Use SSL/TLS between system components" below
- "DMZ architecture using a firewall" on the next page
- "Reverse proxy architecture" on the next page
- "Benefits to using a reverse proxy:" on page 58
- "Secure communication channels" on page 58

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/TLS between system components

The SSL/TLS protocols secure 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 SSL/TLS on the application server" on page 65.

> **Note:** By default, the Agile Manager application server does not have SSL/TLS enabled. It is expected and recommended that the front-end server, either a load balancer or a reverse

> proxy, is configured to require SSL/TLS.

If the application server and the database server are not behind the same firewall, you can use SSL to secure the communication between the two:

On the database server (refer to Oracle documentation for details):

1. Configure your database to open a TCPS port.
2. Create server and client certificates.

On Agile Manager:

1. Copy the client certificate (also called Wallet) to a secure location on the Agile Manager computer.
2. During the Agile Manager installation, when you enter the database parameters, include the path to the client certificate and the certificate's password. For details, see "Enter database parameters" on page 30.

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 on the application server, 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 69.

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

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 **Configuration** > **Authentication** page in the Agile Manager Administration site. For details, see "Configure LDAP authentication" on page 86.
- **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/TLS.

  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 36), 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 **Configuration** > **Users** administration page. Use a strong password for the system administrator. For more details, see "Secure user authentication" below.

- Restrict site customization by modifying user permissions in the Agile Manager configuration area (**Site** > **Users**). For details, see the *Agile Manager Help Center*.
- To debug user actions, set the log level to **Debug**. Be sure to revert the log level back to the previous value when you are finished debugging. For details, see the Agile Manager Administration site (**Servers** > **Application**) and "Configure application server settings" on page 79.
- After updating your licenses, store the license file in a secure location to prevent unauthorized access. For more details, see "Update user licenses" on page 89.

For details see "Log in to Agile Manager" on page 50 and "Agile Manager system administration" on page 78.

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

For details see "Log in to Agile Manager" on page 50, "Configure user authentication" on page 86, 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.

Question	Answer
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 name	Description	Configure on..
System Administrator	Has read and write access to the Agile Manager On Premise System Administration site. No default privileges in the Agile Manager application.	The System Administration **Configuration** > **Users** page. For details, see "Define system administrators and reset user passwords" on page 91.
Site Administrator	Has read and write access to **Site** configuration pages and the **Workspace** > **Users** configuration page. Site administrators can restrict the workspaces that site users have access to.	The **Site** > **Users** configuration page.

Role name	Description	Configure on..
Workspace Administrator	Has read and write access to all application pages and functions, as well as the **Workspace** and **Integrations** configuration areas. Workspace administrators can restrict the applications that workspace users have access to.	The **Site** > **Users** or **Workspace** > **Users** configuration pages.
Team Member	Users can view only items associated with the applications to which they have access. Has read and write access to all application pages and functions for the applications to which they have access. The following exceptions apply: • **Workspace administrators** can set permissions to prevent team members from deleting items created by others. When the **Allow Team Members to delete backlog items created by others** option is cleared, team members can only delete themes, features, and backlog items that they author. By default, this option is selected, and team members can delete any items. Regardless of configuration, Team Members can modify tasks and acceptance tests, regardless of who the author is. • **Team members** have read-only access to the **Author** field. This field can be modified only by Workspace Administrators.	The **Site** > **Users** or **Workspace** > **Users** configuration pages.
	• **Team members** have view access only to public favorites on grid pages, to public Dashboard favorites, and to the public Dashboard gallery. Team members can no longer create, update, or delete these items. • **Team members** can also make only the following configuration changes: • Modify team work hours per day and working days in sprint for their team, from the bucket in the **Release Backlog** only. • Modify ALI configurations.	

Role name	Description	Configure on..
Viewer	Has read access only for all backlog items, grid pages, and the **Sprint Closure** page. Can also watch backlog items to receive notifications about status updates. Additionally: • Has read and write access to private favorites on grid pages. • Can create private buckets on the **Defect Management** page. • Has read access on the Dashboard, and read and write access for private Dashboard items and favorites.	The **Site** > **Users** or **Workspace** > **Users** configuration pages.
Integration Administrator	Has read and write access to the **Integrations** configuration area to configure NextGen Synchronizer.	The **Site** > **Users** or **Workspace** > **Users** configuration pages.
Integration Bridge	Manages communication between Agile Manager and the Integration Bridge. **Note:** • For security purposes, this user should have no other roles. • This role is supported for backward compatibility only. It is used for existing Integration Bridges that still connect to Agile Manager using Agile Manager user credentials.	The **Site** > **Users** configuration page.

For details about defining site and workspace users and ALI, see 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 82.
- 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/TLS on the Agile Manager and LDAP servers to ensure secure account password transmission. For details, see "Uninstall Agile Manager" on page 39 and "Configure LDAP authentication" on page 86.
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.
What base product and service authentication methods are provided?	Agile Manager can be configured to support the following authentication methods: • Username/password • LDAP authentication For details, see "Secure user authentication" on page 59.
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 27.

Data logging

Agile Manager provides the following types of logs:

"Application logs" on the next page

"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.

For details, see "Configure application server settings" on page 79.

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 SSL/TLS on the application server

The following procedure describes how to configure a Secure Socket Layer (SSL) or Transport Layer Security (TLS) connection to Agile Manager, on the Agile Manager application server.

> **See also:** "Configure SSL/TLS on the LDAP server" on page 86 and "Configure an email notification server" on page 84.

Caution: This procedure must be performed only after installing Agile Manager. For details, see "Install Agile Manager" on page 27.

1. Log in to the server machine as the same user who installed Agile Manager (either **root** or the **agmadmin** sudo user).
2. 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.

   Copy the certificate to the **/opt/hp/agm/server/conf/** folder and rename to **server.keystore**.

   Alternatively, *for non-production purposes only*, you can create this certificate by yourself as follows:

   Run the following commands one by one (where **<server>** is the fully qualified name of the Agile Manager application server).

   ```
   cd ~

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

   export KSDEFAULTS="-storepass changeit"

   export KEYINFO="-keyalg RSA"

   /opt/hp/agm/java/jre/bin/keytool -genkey -alias tomcat -dname $SERVER_DN
   $KSDEFAULTS -keystore server.keystore $KEYINFO -keypass changeit

   cp ~/server.keystore /opt/hp/agm/conf/server.keystore

   /opt/hp/agm/java/jre/bin/keytool -export -alias tomcat -file temp_
   server.cer $KSDEFAULTS -keystore server.keystore

   /opt/hp/agm/java/jre/bin/keytool -import -keystore
   /opt/hp/agm/java/jre/lib/security/cacerts $KSDEFAULTS -alias tomcat -file
   temp_server.cer
   ```

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 open the **jetty.xml** file.

   Under the **Configure** element, add the section below.

   Note: As a best practice, we recommend including the bold lines in the section below. This restricts the use of certain cryptographic algorithms and protocols in Agile Manager, and ensures that only the most secure protocols and ciphers are used.

   Before you do this, download Java Cryptography Extension (JCE) Unlimited Strength policy files to get full strength ciphers like AES-256. Download the files from

> **http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html**.
>
> Unzip and copy the two JAR files to this location: **<Agile Manager installation folder>/java/jre/lib/security**

```
<New id="sslContextFactory"
class="org.eclipse.jetty.http.ssl.SslContextFactory">
    <Set name="ExcludeProtocols">
        <Array type="java.lang.String">
              <Item>SSLv3</Item>
        </Array>
    </Set>
</New>


<Call name="addConnector">
 <Arg>
    <New class="org.eclipse.jetty.server.ssl.SslSocketConnector">
       <Arg><Ref id="sslContextFactory" /></Arg>
       <Set name="host"><Property name="jetty.host" /></Set>
       <Set name="Port">8443</Set>
       <Set name="maxIdleTime">30000</Set>
       <Set name="keystore">/opt/hp/agm/conf/server.keystore</Set>
       <Set name="password">changeit</Set>
       <Set name="keyPassword">changeit</Set>
       <Set
name="truststore">/opt/hp/agm/java/jre/lib/security/cacerts</Set>
       <Set name="trustPassword">changeit</Set>
       <Set name="IncludeCipherSuites">
            <Array type="java.lang.String">
                  <Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
                  <Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
                  <Item>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</Item>
                  <Item>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</Item>
            </Array>
       </Set>
    </New>
 </Arg>
</Call>
```

5. In the added section, do the following:

   - If you want to change the port number, replace **8443** with the new port number.
   - If you have changed the default keystore password (recommended), replace **changeit** with the new password.

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

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

   > For example, if you run the following command:
   >
   > ```
   > /opt/hp/agm/java/jre/bin/java -cp
   > ".:/opt/hp/agm/server/lib/*:/opt/hp/agm/server/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.

7. After ensuring that the SSL/TLS 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.

8. Save the **jetty.xml** file.
9. Restart the Agile Manager service: `/opt/hp/agm/wrapper/HPALM restart`
10. 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	`https://<server>:<port>/agm/login`
Agile Manager Administration site	`http://<server>:<port>/agm/admin`

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 57.

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. We recommend using 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

LoadModule rewrite_module modules/mod_rewrite.so
```

> **Note:** Make sure that all of the above modules exist in your Apache installation.

5. Add the following section to the end of the file (see note below).

```
# 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 /qcbin http://<server>:<port>/qcbin

ProxyPassReverse /qcbin http://<server>:<port>/qcbin

ProxyPass /agm http://<server>:<port>/agm

ProxyPassReverse /agm http://<server>:<port>/agm

# Rewrite rule trailing slash must be used in the VirtualHost

# sectionLoadModule rewrite_module modules/mod_rewrite.so
```

```
RewriteEngine On
```

> **Note:**
>
> - Replace **<server>** with the fully qualified host name of the Agile Manager application server.
> - Modify the port number and protocol as needed.

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 50, using the apache port in the URL.

> **Note:** If you configure an email server for notifications emails, also configure an external URL for use in those emails.
>
> For details, see "Configure an external URL for use in emails." on page 85.

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.

- "Password modifications" below
- "Change the heap memory size" below
- "Change the application server port number" on the next page
- "Application server management tools" on page 75

> **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 83.

Password modifications

Passwords used to connect to various system components will change over time. Use the following procedures to modify those password definitions in your Agile Manager system:

- "Change the database system password" on the next page
- "Change the system schema password" on page 74
- "Change the site schema password" on page 83

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 **/opt/hp/agm/conf/wrapper-install.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.

> **Note:** If you modify this port number, note that Linux requires secure processes to use port numbers above 1024. Contact your system administrator to modify the process permissions and use lower ports.

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 database system password

Change the database system password routinely to maintain system security. When you do, modify the password defined in Agile Manager as well.

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 27.

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

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

3. Start Agile Manager. For details, see "Start/Stop the Agile Manager service" on page 49.
4. When the service is up, continue with "Log in to Agile Manager" on page 50.

Change the system schema password

Change the password used to access the system schema routinely to maintain system security. When you do, modify the password defined in Agile Manager as well.

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 27.

   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. Start Agile Manager. For details, see "Start/Stop the Agile Manager service" on page 49.
4. When the service is up, continue with "Log in to Agile Manager" on page 50.

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://docs.oracle.com/javase/8/docs/technotes/guides/management/jconsole.html To connect to jconsole using a remote process, use the following URL syntax: `service:jmx:rmi://<server>:29601/jndi/rmi://<server>:9999/server` If you do not want to expose this console, you must close the relevant ports (**29601** and **9999**) on your server.
jstack	http://download.oracle.com/javase/1.5.0/docs/tooldocs/share/jstack.html
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

Troubleshooting

If you encounter problems installing or upgrading 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 page 39.

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. For details, see "Change the application server port number" on page 73.

Error: Couldn't flush system prefs

If you upgraded from Agile Manager 2.10 to Agile Manager 2.50, the **wrapper.log** contains errors that read: `Couldn't flush system prefs`.

Fix:

1. Back up the **/opt/hp/agm/wrapper/wrapper.conf** file.
2. In the same folder, rename the **wrapper.conf.rpmnew** file to **wrapper.conf**.
3. Run the configuration wizard again. This time, in the **System Administration Database Schema** screen in the configuration wizard, select **Connect to existing schema / second node**.

   For details, see "Install Agile Manager" on page 27 and "Connect to existing schema / second node" on page 32.

> **Note:** If you previously changed the **wrapper.java.maxmemory** property in the **wrapper.conf** file, manually migrate this change to the **/opt/hp/agm/conf/wrapper-install.conf** file.

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 50.

The Administration Home page provides a checklist of configurations you must perform before setting up your Agile Manager site.

✓	Green check marks indicate that the configuration step is complete.
✎	Blue edit icons indicate that configuration information is required.

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.

About this PDF Version of Online Help

This section of the 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.

What do you want to do?

Configure application server settings

Tab: Servers > Application

This page displays data for the application server selected on the left. If you have a clustered configuration with multiple application servers, select a server to configure and view data relevant to that server.

For more details about clustered configurations, see "Clustered configuration example" on page 11.

Configure maximum database connections

Modify the **Max DB Connections** value to set the maximum number of simultaneous connections to the database from the selected application server.

The default value is **100**.

> **Note:**
>
> - You must restart the server after modifying this value for any change to take effect.
> - This value is set back to the default after upgrading. If you modify this value and then upgrade, modify the value again after the upgrade is complete.

Balance synchronization load

If you are using NextGen Synchronizer on a clustered system, you can prevent the automatic synchronization from causing extra load on your main Agile Manager server.

Divide the server load by designating nodes for Agile Manager user activity that will not handle synchronization processes. Data from all nodes is still synchronized.

Do the following:

1. On a node that should be used only for Agile Manager user activity:

   On the Servers > Application tab, select **Disable NextGen Synchronizer processes**.

   > **Note:** You must restart the server after modifying this setting for the change to take effect.

2. In the **Configuration > Advanced Parameters** tab:

   a. Add a system parameter named OPB_AGM_SERVER_URL.

   b. Set the parameter's value to the URL used to access the node(s) that will be running synchronization processes. This might be the URL of the Agile Manager node or the URL of a load balancer.

      Use this format: `http(s)://<server hostname or IP address>:<port>/agm`

   This ensures that when the Integration Bridge is downloaded, it is set up by default to access the Agile Manager node(s) that handle synchronization.

   > **Tip:** A **server-connection.conf** file is downloaded with the Integration Bridge. This file contains the URL and site ID that the bridge will use to access Agile Manager.

3. Any Integration Bridges previously downloaded from the node on which you now disabled NextGen Synchronizer processes need to be modified.

   The Integration Bridge is set up by default to access the node from which is was downloaded. To make sure that it communicates with a node that will be running synchronization processes, do the following:

   a. Navigate to the **<HP Integration Bridge installation folder>\product\conf** folder (on Linux, reverse the slashes).

   b. Open the **server-connection.conf** file for editing.

   c. In the **agm.base.url** property, replace the hostname/IP address with the hostname/IP address of the relevant Agile Manager node or the load balancer.

   d. Restart the bridge.

Application log files

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.
PublicApiAudit.logger.txt	Records public API REST calls, including the user name of the user who made the call. Stored in the **/opt/hp/agm/log/qc** directory.
PublicApi.logger.txt	Records events that occur during a specific public API session. Stored in the **/opt/hp/agm/log/qc** directory.

Default values

By default:

- 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.

See the table below for additional details about specific parameter default values.

Configure log settings

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

> **Note:** The application log server name is listed at the top of the page. If you are working in a clustered environment, select a server name from the list on the left.

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

Configure the following log values:

Parameter	Description
Log level	Defined in the first line of the file. **Default.** WARN **Note:** If you change the log level to **Debug**, make sure to change it back when you are finished debugging.
FileAppender	Defines the appender added to each file name when the log file reaches the maximum configured size. **Default.** `RollingFileAppender` (standard log4j value)

Parameter	Description
FileAppender.File	Defines the location and name of the log file. **Default.** `${log.folder}qc/agm.logger.txt`
FileAppender. MaxFileSize	Defines the maximum size of the log file. **Default.** `10000 KB`
FileAppender. MaxBackupIndex	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
FileAppender.layout	Defines the log files layout and organization. **Default.** `PatternLayout` (standard log4j value)
FileAppender.layout. ConversionPattern	Defines the data displayed in the log files. **Default.** Standard log4j values, as well as the following custom attributes: • `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

Database server details are configured during Agile Manager installation and configuration, and most of the data on this page is read-only. For details about database configuration, see "Enter database parameters" on page 30.

If your site is undergoing maintenance, such as a site upgrade, view details about the maintenance in the **Maintenance Status** field, in the **Site Status** area. This field appears only during maintenance.

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

The Administration site enables you to do the following:

- "Activate your site" below
- "Change the site schema password" below
- "Restore a site schema" below

Activate your site

Your site is deactivated during maintenance procedures, such while you're editing configured passwords, or upgrading your site.

When the maintenance is complete, under **Site Status**, click **Activate** to reactivate your site.

Change the site schema password

If you update the password used to access your site schema , you will also need to edit the password configured in Agile Manager accordingly.

In the **Database User Credentials** area, click **Edit Password**. Enter the new password, and then enter it again to confirm.

> **Note:**
>
> - Clicking **Edit Password** deactivates your site, even if you do not finish changing your password. Click **Activate** to reactivate your site.
> - This is different than updating your system schema password. For details, see "Change the system schema password" on page 74.

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 (as listed under **General Information** on the **Servers** > **Database** page).

Caution:

- You can access only a single site from Agile Manager at a time. This means that after restoring a site schema, all the data currently displayed in Agile Manager will be inaccessible. Instead, you will be able to access the data from the restored schema only.
- To restore a site, you must use a schema hosted on the same database server, with identical credentials to the ones defined in the current version.
- If you are working with a completely new system administration schema, and restore an existing site schema, data residing in the administration schema will be unavailable after the upgrade. This includes user passwords for users authenticated by Agile Manager, as well as user avatar photos.
  - User login for users authenticated LDAP will not be affected at all.
  - Users authenticated directly by Agile Manager will be able to log in with no password at all.
  - All users will have to reset their avatar photos.

  For more details, see "Upgrade a basic production system" on page 44.

At the top of the page, click **Restore Site Schema**, and enter the site schema and repository information for the site you want to restore.

Configure an email notification server

Tab: Servers > Mail

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

1. From the **Mail server** drop-down, select **SMTP Server**.
2. Define the server name and server port number.
3. If your mail server requires SMTP authentication, select **Enable connection to an SMTP server that requires authentication**, and enter the authentication details.

   Note: You must configure your authentication details if you are planning on configuring SSL/TLS on the SMTP server.

4. Configure SSL/TLS on the SMTP server (optional).

To connect to a secured SMTP mail server, do the following:

a. Select **Enable SSL support**.

b. Pre-configure a certificate trust store on the Agile Manager application server.

   In most cases, the default trust store is used. The default trust store is **/opt/hp/agm/java/jre/lib/security/cacerts**, and the default password is **changeit**.

   To establish trust to the SMTP server certificate, import it into the Java trust store using the keytool utility. The keytool utility is located in the **/opt/hp/agm/java/jre/bin** directory.

   For example

```
 keytool -import -alias <your SMTP CA> -trustcacerts -file <SMTP CA
cert> -keystore /opt/hp/agm/java/jre/lib/security/cacerts
```

c. If there are any intermediate Certificate Authorities, import their certificates as well.

> **Note:** Using an encrypted connection on the SMTP server may cause your SMTP port to change. Verify the port, and change it if necessary.

5. Save your changes. At the top of the page, click **Save**.
6. If you are using an encrypted connection, restart Agile Manager after importing the certificate. For details, see the "Start/Stop the Agile Manager service" on page 49.
7. Test your settings. At the top of the page, click **Test Send Mail**.

   Enter the email address you want to send the test mail to, and click **Test**.
8. Configure an external URL for use in emails.

   If you configure a mail server, Agile Manager sends emails to users that include links to Agile Manager. These emails might expose the actual machine names.

   Examples of such emails include when users send an entity to another user directly from within Agile Manager, or when new users receive a welcome email, inviting them to log in.

   To hide the actual machine names, add the **EXTERNAL_BASE_URL** advanced parameter on the **Advanced Parameters** page of the System Administration site. Define the value as the external URL you would like to appear in the emails.

   For example: `http://my-load-balancer-domain:8080/`

   > **Note:** Do not add `agm` to the end of the URL.

   For more details, see "Configure advanced parameters" on page 93.

See also:

- "Configure SSL/TLS on the application server" on page 65
- "Configure SSL/TLS on the LDAP server" on the next page

Configure user authentication

Tab: Configuration > Authentication

Agile Manager supports the following types of authentication:

Type	Description
Agile Manager authentication	By default, users are added to and authenticated directly by Agile Manager. Select **Agile Manager**, and continue directly to the Agile Manager configuration area (**Site** > **Users**) to add individual users. This page is visible to Agile Manager Site Administrators only. For more details, see the *Agile Manager Help Center*.
LDAP authentication	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. For details, see "Configure LDAP authentication" below.

Configure LDAP authentication

> **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.

Configure SSL/TLS on the LDAP server

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

LDAP server configuration	Pre-configure the following on the LDAP server: • Enable SSL/TLS. • Define a secure port. Agile Manager uses port 636 by default. • Install a server certificate. Additionally, obtain a root certificate (and any intermediate) from the certificate authority (CA) that issued the LDAP certificate.

Agile Manager server configuration	Pre-configure a certificate trust store on the Agile Manager application server. In most cases, the default trust store is used. The default trust store is **/opt/hp/agm/java/jre/lib/security/cacerts**, and the default password is **changeit**. To establish trust to LDAP server certificate, import it into the java trust store using the keytool utility. The keytool utility is located in the **/opt/hp/agm/java/jre/bin** directory. **For example:** `keytool -import -alias <your LDAP CA> -trustcacerts -file <LDAP CA cert> -keystore /opt/hp/agm/java/jre/lib/security/cacerts` If there are any intermediate Certificate Authorities, import their certificates as well.

> **Note:** You must restart Agile Manager after adding a certificate, and prior to connecting to an LDAP server over SSL/TLS. For details, see the "Start/Stop the Agile Manager service" on page 49.

See also:

- "Configure SSL/TLS on the application server" on page 65
- "Configure SSL/TLS on the SMTP server (optional)." on page 84

To configure LDAP authentication:

1. Select **LDAP**, and configure Agile Manager to connect to your LDAP system using the fields below in the following areas.

   Hover over tooltips ⓘ if you need additional clarifications about a specific field.

LDAP Settings	Description
Authentication Settings	General authentication data, including the LDAP server URL, and the directory authentication type. When setting the **Directory Provider URL** field for SSL/TLS, use on of the following syntaxes: • `ldaps://<server name>:<port>` • `ldap://<server name>:<port>`, if the LDAP server is not configured to use SSL/TLS Click **Test connection** to test the connection with the LDAP server.
Base Settings	Details about the directory node from which users are retrieved, which users are retrieved, and how many at a time. 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.
Field Mappings and Search Types	Map LDAP fields to Agile Manager fields and define the LDAP searches supported. If your organization prefers to use login identifications other than the email address, enter the relevant LDAP field in the **Alternative Login ID** field. For details about defining searches, see "Configure searches for LDAP users" below.

2. To verify both authentication and base settings, click **Test LDAP Settings** ⚙ at the top of the page.
3. After the LDAP settings are defined, continue to the Agile Manager configuration area to import users (**Site** > **Users**). This page is visible to Agile Manager Site Administrators only.

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

Configure searches for LDAP users

Under **Field Mappings and Search Types**, select the type of search you want to enable for each field. Select one of the following:

Option	Description
Contains	Returns results where the search string does not match the results exactly. For example, if you select **Contains** for a full name field, a search for **John** will return users that include John Doe, Johnny Smith, and John Carter. It will not return users named Jon.
Equals	Requires search strings to match the results exactly. For example, if you select **Equals** for a full name field, the search string will have to include the user's full name, such as **John Doe**. A simple search for John will not return results for John Doe.
None	All searches ignore this field. For example, if you select **None** for a phone number field, administrators will not be able to search for users by their phone numbers.

Update user licenses

Tab: Configuration > Licenses

Agile Manager is installed with a default Instant On 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.

When you have your **.dat** file ready, do the following:

1. At the top of the page, 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.

Juggling users and licenses

Adding or importing more users than your licenses support will cause those users to be added as **Inactive**. Juggle user licenses by activating or deactivating users in the Agile Manager configuration area (**Site** > **Users**). This page is visible to Agile Manager Site Administrators only.

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

License installations in clustered configurations

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.

Concurrent licensing

Concurrent licenses apply to a pool of users who are logged in simultaneously.

Upon initial installation, administrators can select to install concurrent Instant On licenses, or named Instant On licenses, which apply only to specifically named users.

If you are planning on using concurrent licenses, we recommend selecting Instant On concurrent licenses to start.

- You can purchase Named or Concurrent licenses, but you cannot use both types of license on the same system. After you install purchased licenses of one type on your system, you cannot install the other type of license.
- Instant On and Evaluation named licenses can be overridden by purchased concurrent licenses, and vice versa.

For more details, see "License types" below.

License expiration

If a limited time license expires, all users who are active on that license are deactivated (for details, see "License types" below). Purchase additional licenses to continue working with Agile Manager.

If System Administrators are among the users who will be deactivated, Agile Manager first verifies whether there is another currently valid license installed. If there is, these System Administrators are moved to that other license, and can continue working with Agile Manager.

System Administrators have access to the Agile Manager On Premise System Administration site. For more details, see "System Administrators" on the next page.

License types

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

Type	Description
Evaluation	License that supports a specific number of users, for a limited period of time, for evaluation purposes. Used to replace the default **Instant On** license, in case you need more time to evaluate Agile Manager.
Perpetual	Purchased license that supports a specific number of users for an indefinite period of time. Purchase additional licenses to add more users.
Term	Purchased license that supports a specific number of users, for a limited period of time. After this time period is complete, additional licenses must be purchased for the supported users to continue using Agile Manager, or to add additional users.

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.

> **Note:** You must add or import users in the Agile Manager configuration area (**Site** > **Users**), and only then define users as System Administrators. This page is visible to Agile Manager Site Administrators only.
>
> For more details, see the *Agile Manager Help Center*.

- To define a user as a System Administrators, select the user row and click **Set as System Administrator**.
- To remove the System Administrators 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 authenticated directly by Agile Manager (and not via an LDAP system).

1. In the grid, select the user, and click **Reset User Password**.
2. Enter the new password and confirm it.

Configure general system settings

Tab: Configuration > General

Define security settings

Under **Security**, define the following:

- **inactivity session timeout.** The number of minutes after which an inactive user is logged out of Agile Manager.

  > **Note:** There can be a extra delay of up to 15 minutes until a user is logged out.

  Changes to this setting take effect only after users log out and log in again.

- **Allow 'sa' user to log in with AGM credentials.** 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, but 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 "System Administrators" on the previous page.
  >
  >   **Site Administrators** are configured in the Agile Manager configuration area (**Site** > **Users**). For details, see the *Agile Manager Help Center*.

Define attachment settings

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

- Maximum file size for each file uploaded
- Maximum aggregated size for all attachments in the site
- Blocked file extension types

Define settings for custom fields

Administrators can create custom fields for the following entity types: *Themes*, *Features*, *User Stories*, *Defects*, or *Backlog Items* (which apply to both user stories and defects)

Define limits for:

- The maximum number of custom fields allowed in your site *per entity type*.

  By default: 12

  Maximum: 40

  > **Note:**
  >
  > - Site administrators can divide this quota between site and workspace fields. For details, see Maximum number of custom fields in the *Agile Manager User Guide*.
  > - The total number of custom fields defined for themes, features, and user stories together cannot exceed 40.
  >   Therefore, if you increase the maximum number of custom fields to 14 or higher, you will not be able to reach this maximum in all three entity types.

- The maximum number of values allowed per list field.

  Default: 20

  Maximum: 100

Define report settings

Define when Agile Manager aggregates daily data for Dashboard graphs over time.

> **Note:** You must restart the server after modifying this value for any change to take effect.

Configure advanced parameters

Tab: Configuration > Advanced Parameters

Advanced parameters are system parameters that change the default behavior of your system.

Usually, you define system parameters only when it is suggested by HP customer support.

- Click + **Add Parameter**. Enter the parameter's name and value, as well as an optional description.

> **Note:** Spaces, and the following special character are not supported in parameter names:
>
> **[\ !@ # $ % ^ & *( ) = + | < , > / ? { [}`~"";:]**

- Sort parameters by column, or filter parameters by any matching text in the parameter's name, value, or description.

System parameters you can define on your own

- **PRODUCT_GROUP_FUSE.** The number of workspaces that can be defined on your site. (Default=100, we recommend that you not set this higher than 400)
- **OPB_AGM_SERVER_URL.** The URL for an Integration Bridge to use when accessing Agile Manager. For details, see "Configure application server settings" on page 79.
- **OPB_ENABLE_AUTO_UPGRADE**. Specifies whether the Integration Bridge can be automatically upgraded.

  By default, the Integration Bridge is automatically upgraded. To disable the upgrades, set this parameter to N. For more details, see "Secure attachment files and downloads" on page 53.

Send Us Feedback

Let us know how we can improve your experience with the Installation and Administration Guide.

Send your email to: docteam@hpe.com

Java™
COMPATIBLE