HP Agile Manager

Software Version: 2.0

Installation Guide

Document Release Date: April 2014

Software Release Date: April 2014

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

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

Contents

Welcome to Agile Manager

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 and managing your servers.

For details about how to use Agile Manager and the Agile Manager Administration site, 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 the Agile Manager system components in basic and clustered configurations.
- **"Linux prerequisites" on page 11.** Describes requirements for the Linux application servers and related procedures.
- **"Oracle prerequisites" on page 14.** Describes requirements for the Oracle database servers and related procedures.
- **"Pre-installation checklist" on page 20.** Lists the details you will need to supply during installation and should have available before you begin.
- **"Install a clustered system" on page 22.** Describes the high level steps required to install the system in a clustered configuration.
- **"Install Agile Manager" on page 23.** Describes how to install your Agile Manager system.
- **"Start/Stop the Agile Manager service" on page 32.** Describes how to start and stop the Agile Manager service.
- **"Log in to Agile Manager" on page 33.** 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 34.** Describes best practices and procedures for securing your Agile Manager system.
- **"Manage the application server" on page 49.** Describes optional procedures that are performed after installation to manage your Linux server.
- **"Uninstall Agile Manager" on page 51.** Describes how to uninstall Agile Manager.
- **"Troubleshooting" on page 52.** Describes the log files you should check if you encounter errors during your installation.

System architecture

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

Agile Manager components

The following table describes the Agile Manager system components.

Component	Description
Agile Manager client	Provides access to the Agile Manager application and Administration site via a web browser.
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: • **Site Administration schema.** Stores information related to the Agile Manager system, such as users and mail notification settings. • **Project schema.** Stores project information, such as backlog items. The schemas reside on an Oracle server. For details, see "Oracle prerequisites" on page 14.
Project repository	Stores project 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 that work in a clustered environment, it is advisable to install the repository on a dedicated machine.
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.

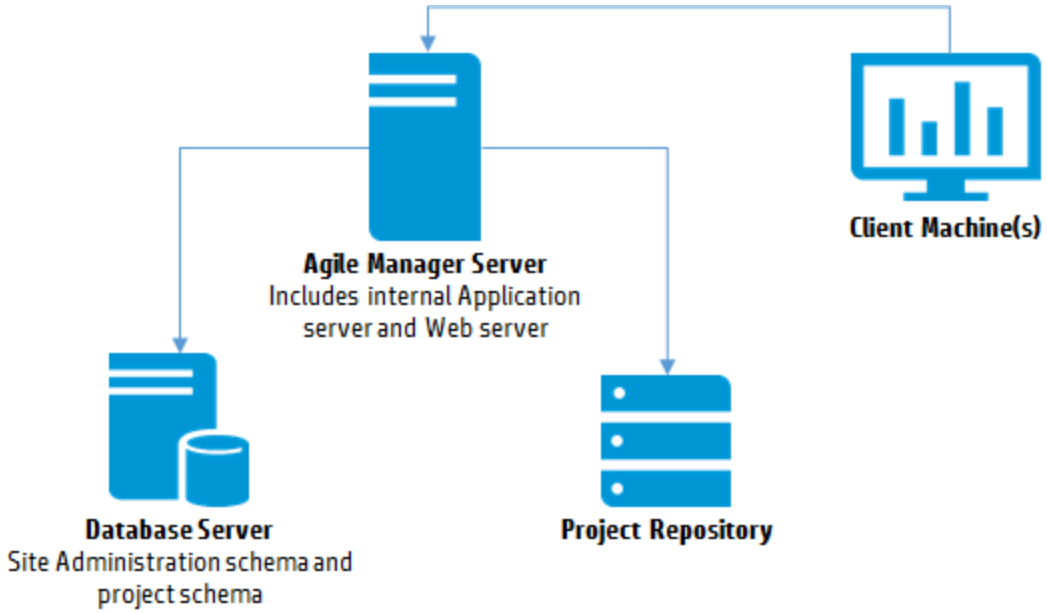
Component	Description
Tanuki wrapper	A Java service wrapper that allows Agile Manager to be installed and controlled like a native Windows Service. It also includes advanced fault detection software to monitor Agile Manager.

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 Jetty 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.



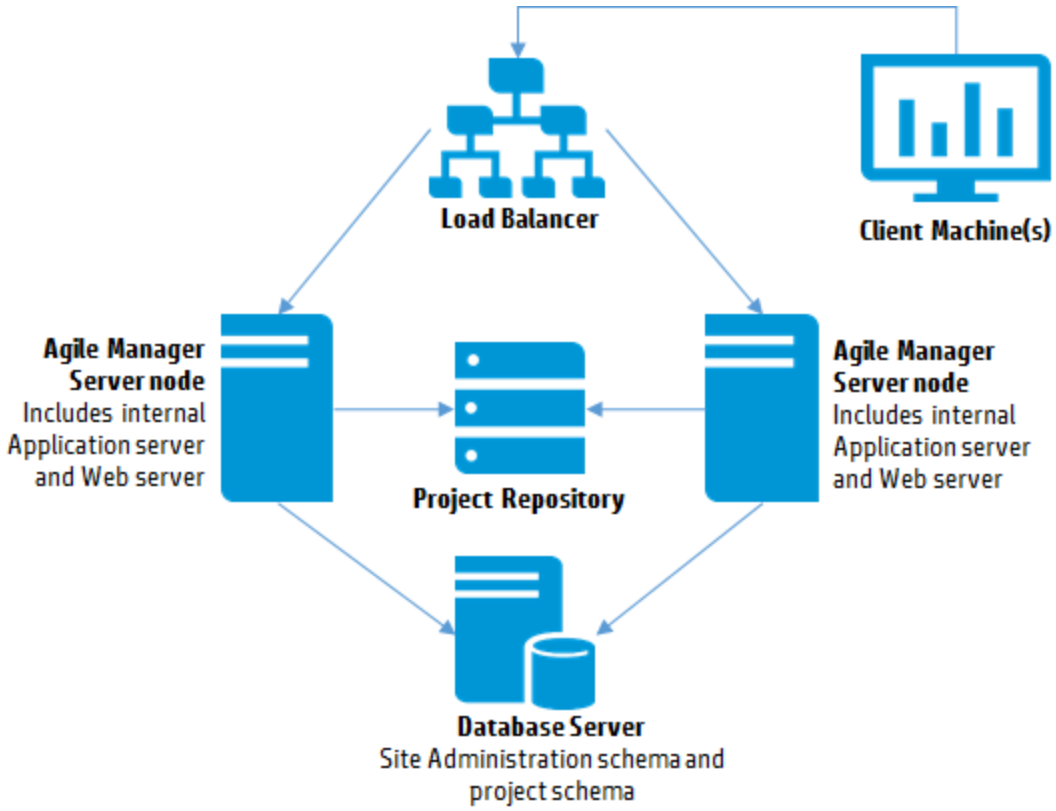
For more details, see "Agile Manager components" on the previous page and "Install Agile Manager" on page 23.

Clustered configuration example

Agile Manager supports clustering within the J2EE framework. 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.



For more details, see "Agile Manager components" on page 7 and "Install a clustered system" on page 22.

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.
Site administration database schema	All nodes must point to the Site administration database schema.

Cluster considerations	
Shared resources	All nodes must have access to: • All database servers • The Site Administration database schema • The project 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

Hardware Minimum Requirements	
CPU	Linux® Quad Core AMD64 processor or equivalent x86 compatible processor
Memory (RAM)	8 GB minimum
Free disk space	16 GB minimum
Application Server Requirements	
TCP Port	8080 must be free, or 8443 for secure connections
Supported Environments	
Operating system	Red Hat Enterprise Linux 6.2 or 6.3 (64 Bit) SUSE Linux Enterprise 11 Service Pack 3
Database	Oracle 11.2.0.3
Client Machines	
Supported browsers	Chrome 23 and above Firefox 16 and above Internet Explorer 9 and 10 **Note:** If you are using Internet Explorer 9, make sure that the Chrome Frame plug-in is disabled.
Screen resolution	1680x1050 (recommended) or 1024x768

Linux prerequisites

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

"Linux disk space requirements" below

"Linux server required permissions" below

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

See also:

- "System requirements" on the previous page
- "Oracle prerequisites" on page 14
- "Pre-installation checklist" on page 20

When you're ready to install, continue with "Install a clustered system" on page 22 or "Install Agile Manager" on page 23.

Linux disk space requirements

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

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

Verify disk space using the following command:

```
df -h
```

Linux server required permissions

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

Administrator user permissions

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

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

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

File directory permissions

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

If the file repository is located on a remote machine:

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

Install as a non-root user

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

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

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

1. Create a new user group: `groupadd agmadmins`
2. Create a new user: `useradd agmadmin`
3. Add the user to the group: `usermod -G agmadmins agmadmin`

   To verify, run: `id agmadmin`

4. If required, change the new user's password: `passwd agmadmin`
5. Grant the new user root user permissions. Add the following line to the **sudoers** file: `agmadmin ALL=(ALL) ALL`
6. Continue with "Install Agile Manager" on page 23, running the rpm file as the sudo user.

See also:

- "Install a clustered system" on page 22
- "Oracle prerequisites" on the next page
- "Pre-installation checklist" on page 20

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 17

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

See also:

- "System requirements" on page 10
- "Linux prerequisites" on page 11
- "Pre-installation checklist" on page 20

When you're ready to install, continue with "Install a clustered system" on page 22 or "Install Agile Manager" on page 23.

Database requirements

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

Database connection	• Connection to the database server • DNS resolution **Tip:** Test the DNS resolution by pinging the database server.
Charset	Database charset must be set to UFT-8.
Database column length semantics	Column length must be defined according to characters, and not according to bytes.
Tablespace name and size	• The tablespace names (default and temporary). • The minimum tablespace sizes for storing the Site Administration database schema. • That the tablespace is not locked.

Clustered configuration	To install Agile Manager on a second node in a clustered configuration: • 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 site 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 project user schema, copying data between projects, and checking that there is sufficient storage in a specific tablespace.

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

Run the following script on the Oracle database server, as the system database administrator, to grant the required database administrative user privileges.

For details, see "Database administrator 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 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;
```

Database administrator user privileges	
CREATE SESSION WITH ADMIN OPTION (1)	Required to connect to the database as the Agile Manager database administrative user.
CREATE USER	Required to create a new project user schema when creating a new Agile Manager project.
DROP USER	Required to remove a Site Administration database schema.
CREATE TABLE WITH ADMIN OPTION (1)	Required to grant this permission to a newly created Agile Manager project user schema.
CREATE VIEW WITH ADMIN OPTION (1)	Required to create views for an Agile Manager project.
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 SEQUENCE WITH ADMIN OPTION (1)	Required to create sequences for an Agile Manager project.
CREATE PROCEDURE WITH ADMIN OPTION (1)	Required to create stored packages for an Agile Manager project. Agile Manager uses packages to collect change history for specific tables.

Database administrator user privileges	
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.
SELECT ON DBA_FREE_SPACE (2)	Required to check free space on the database server prior to creating a new Site Administration database schema or a new project.
SELECT ON SYS.DBA_TABLESPACES (2)	Required to collect a list of tablespaces that exist on the database server prior to creating a new Site Administration database schema or a new project.
SELECT ON SYS.DBA_USERS (2)	Required to verify the existence of specific database project users. For example, you might want to verify the existence of an Oracle CTXSYS user before creating a new Agile Manager project.
SELECT ON SYS.DBA_REGISTRY (2)	Required to verify that the text search component is installed on the database server.
SELECT ON SYS.DBA_ROLES (2)	Required to verify that the text search role (CTXAPP) is installed on the database server.
SELECT ANY TABLE WITH ADMIN OPTION (1) **and** **INSERT ANY TABLE**	Required to enhance performance when restoring a project.

Note:

- (1) An Agile Manager database administrative 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 database administrative user. The recommended name for this role is **QC_SELECT_ON_SYS_OBJECTS**.

Enable Oracle RAC Support

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

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

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

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

To enable Oracle RAC support:

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

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

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

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

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.

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 10. More details and optional pre-installation procedures are described in "Linux prerequisites" on page 11 and "Oracle prerequisites" on page 14.

Pre-installation checklist	
Clusters	Cluster host names Required only if you are using a clustered configuration.
Encryption passphrase	Confidential data passphrase **Default.** `Seashells Grow Like Misty Tunas` In a cluster, you will use the same passphrase on all nodes. **Note:** Make a note of the passphrase you use for support calls.
Database server	**Database.** Host name, port, system identifier (SID), and administrator user name and password. The Oracle SID identifies the specific Oracle instance on the Oracle server host machine. **Tablespace.** Default tablespace selection.
Site Administration	**Site administration** Site administration password. The default password is empty. You can modify this password during installation. The default site administrator user name is **sa**. This cannot be changed. You can later define additional users as site administrators in the Agile Manager Administration site (**Users** > **User Management**). For details, see the *Agile Manager Help Center*. **Site administration database schema** Site administration database schema user name and password. The default Site Administration database schema name is **agm_siteadmin_db**, and the default password is **tdtdtd**. You can modify both of these defaults during installation.

Pre-installation checklist	
Project repository	Repository path • By default, the repository is configured in the deployment folder. It is recommended to modify this default to a different location. • The user who installs Agile Manager must be the owner of the repository folder.

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 11 and "Oracle prerequisites" on page 14.

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

   When defining the repository path, select the shared folder you created earlier.
4. After the wizard is complete, copy the **/opt/hp/agm/conf/qcConfigFile.properties** file from the server where you installed and configured Agile Manager to the same folder on all other nodes.
5. On each of the other nodes in the system, install Agile Manager. On each node, continue with the step entitled "Open the directory in which the Agile Manager files are deployed" on the next page.

   During installation, do not change any of the settings except for selecting the following options:
   - **Keep all current settings.** For details, see "Run the configuration wizard" on the next page
   - **Connect to an existing schema/second node.** For details, see "Select a database schema option" on page 25.
6. After completing the installation and configuration wizard on all nodes, access the Agile Manager Administration site. On the **Servers** > **Application** page, verify that all of your application servers are displayed correctly.

   For details, see "Log in to Agile Manager" on page 33.

Install Agile Manager

This section describes how to install and configure Agile Manager. For high level instructions for installing a clustered system, see "Install a clustered system" on the previous page. If you encounter problems during the installation process, see "Troubleshooting" on page 52 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 51.

1. **Mount the project repository (clusters only)**

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

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

2. **Deploy the installation files**

   Copy the rpm file provided in the installation package to the **tmp** folder, or any other accessible folder.

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

As root user	`rpm -i Agile-Manager<version number>.rpm`
As sudo user	`sudo rpm -i Agile-Manager<version number>.rpm`

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

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

   `Run cd /opt/hp/agm`

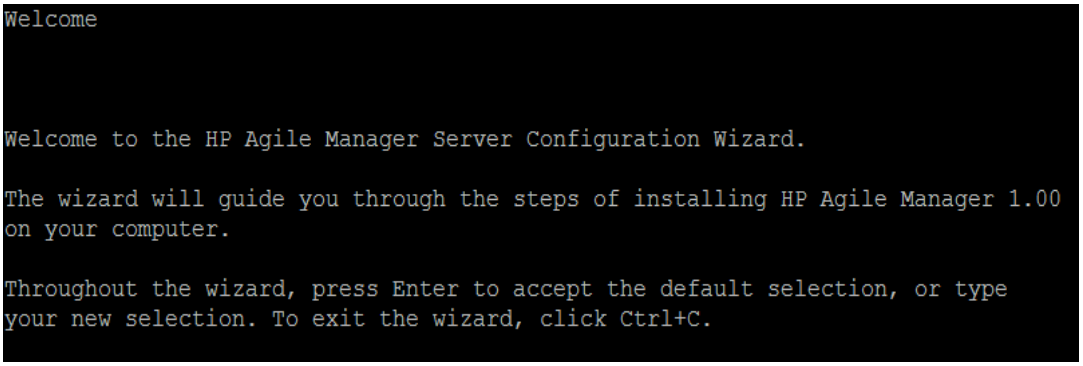
4. **Run the configuration wizard**

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

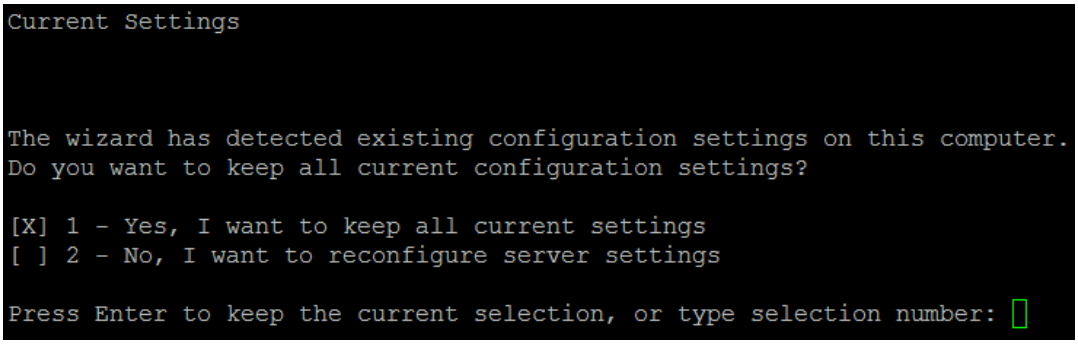
   Note: If you are installing Agile Manager on a secondary node of a cluster, some of the

steps that are needed only for the primary node are not displayed.

The Agile Manager configuration wizard opens.



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



Note: This step is displayed only if the **qcConfigFiles.properties** file exists.

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.

5. **Enter database parameters**

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

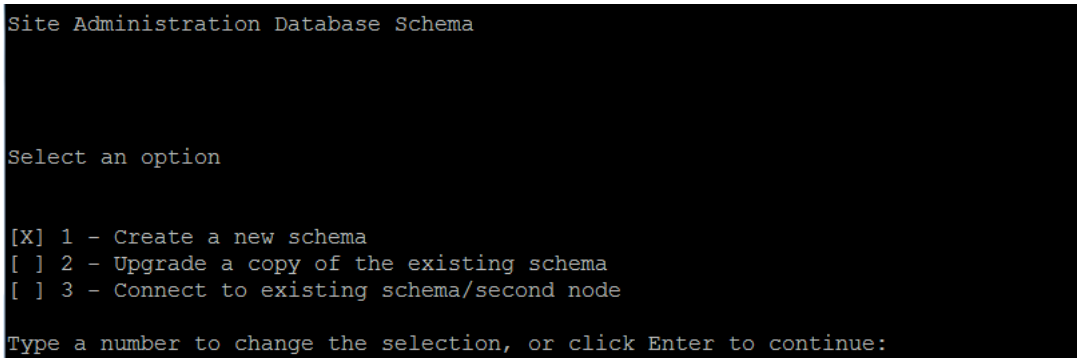
Parameter	Description
DB host name	The database server name.
DB port number	The database server port number. You can accept the default port number.
Oracle SID	The Oracle system identifier.

6. **Enter database administrator login information**

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.

7. **Select a database schema option**

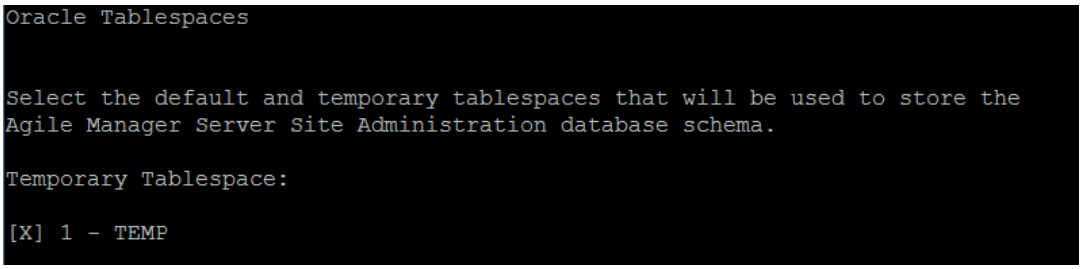


Select one of the following:

Option	Description
Create a new schema	Creates a new Site 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 Site Administration database schema. This option is relevant if: ▪ You are re-installing Agile Manager ▪ You are configuring a second node in a cluster configuration **Note:** If you are installing a clustered system, be sure to review the steps in "Install a clustered system" on page 22 and the considerations in "Clustered configuration example" on page 8.
Upgrade a copy of the existing schema	Creates a copy of the existing Site Administration database schema, and upgrades the copy. This option is relevant for upgrades only, and enables you to work with both versions of Agile Manager simultaneously. **Note:** Upgrade scenarios are not yet validated for Agile Manager.

8. **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.



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

9. **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 Site Administration database already exists, the new Site Administration database schema is created in the same tablespace as the existing schema. In such cases, ccontinue with "Enter site administrator login information" on page 29.

   ```
   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.

10. **Enter site administration database schema details**

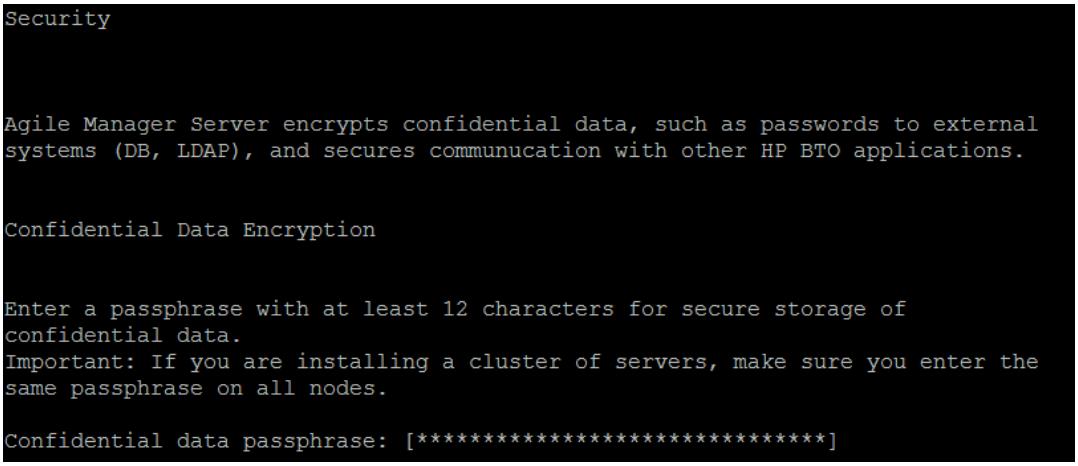
    ```
    SA Schema Details


    Schema name: [agm_siteadmin_db]
    ```

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

    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.

11. **Enter a 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.

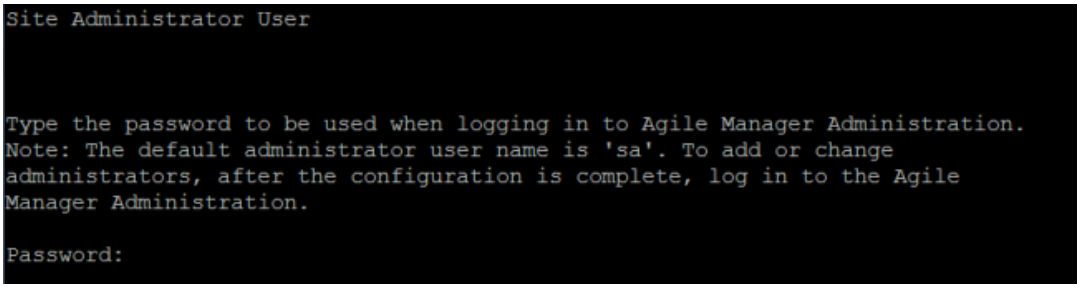
You can also select to use the default value of `Seashells Grow Like Misty Tunas`.

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.
Installing on a cluster	If you are installing Agile Manager on a cluster, you must use the same passphrase for all nodes.

12. **Enter site administrator login information**



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.

13. **Enter the file repository path**

Accept the default path or enter a new path.

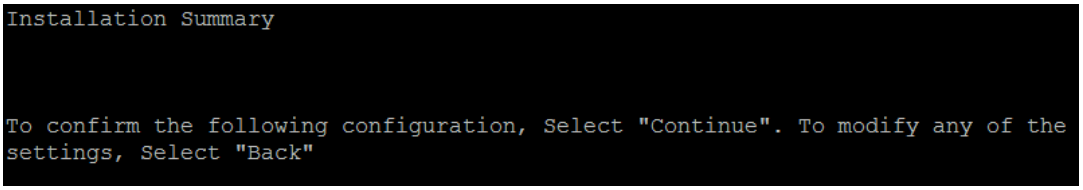
> **Tip:** See "Project repository" on page 21 for guidelines about defining this path.

14. **Verify that the application server port 8080 is free**

> **Note:** You can change the default port after configuration is complete. For details, see

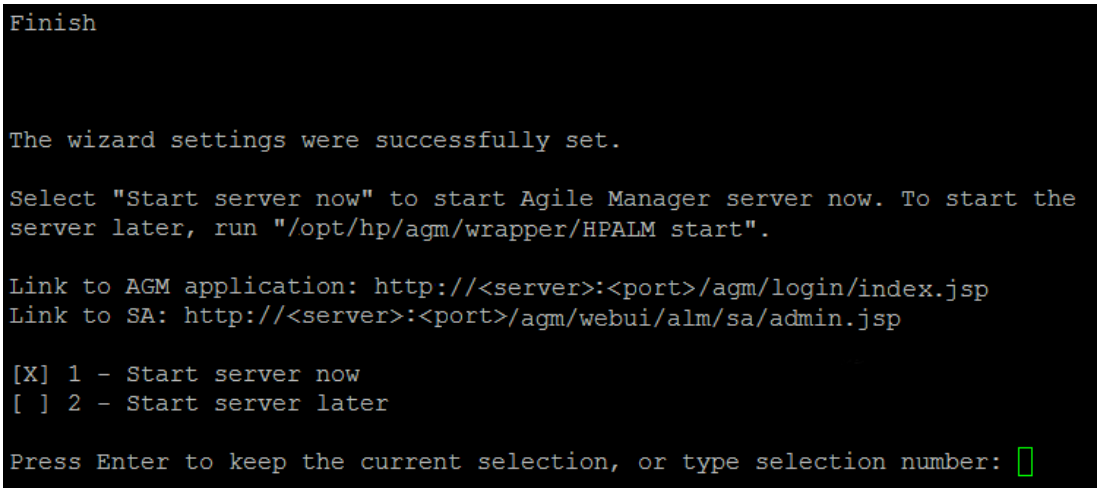
"Changing the application server port number" on page 49.

15. **Review the settings**



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

16. **Complete the configuration**



Select whether you want to start the Agile Manager service now or later. If you select to start the service later, see "Start/Stop the Agile Manager service" on page 32 for details.

When the service is up, continue with "Log in to Agile Manager" on page 33. For security best practices and procedures, see "Secure your system" on page 34. For other server and site management details, see "Manage the application server" on page 49 and the *Agile Manager Help Center*.

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. To change the

application server port number, see "Changing the application server port number" on page 49.

Start/Stop the Agile Manager service

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

Start the Agile Manager service after reboot

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

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

Run Agile Manager as a simple user

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

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

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

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

Log in to Agile Manager

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

Agile Manager	`http://<server>:<port>/agm/login/index.jsp`
Agile Manager Administration site	`http://<server>:<port>/agm/webui/alm/sa/admin.jsp`

The default user installed with Agile Manager is the **sa** user. You defined the **sa** user password during installation (see "Enter site administrator login information" on page 29).

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

Note: The *Agile Manager Help Center* is installed together with Agile Manager. You can access it outside of Agile Manager in the following path: `http://<server>:<port>/agm/agmdocs/Default.htm`.

Secure your system

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

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

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

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

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

This chapter includes:

Secure deployment

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

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

Secure deployment methods	
SSL	**Basic configuration.** Enable SSL on the Agile Manager Jetty and make it required. **Clustered configuration.** Require SSL for the Agile Manager virtual IP on the load balancer. For details, see "Configure SSL authentication" on page 44.
Reverse proxy	Install a reverse proxy in front of the Agile Manager server, and then configure SSL on the reverse proxy server. For details, see "Reverse proxy architecture" on page 38 and "Integrate an Apache web server (example)" on page 46. For details about enabling SSL for all interactions with Apache, see http://httpd.apache.org/docs/current/ssl/ssl_howto.html.
Firewall	Use a firewall between the client and the other Agile Manager components. 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 37

Common considerations and best practices

- Thoroughly review the trust boundaries between application, exchange, database, and LDAP servers to minimize the number of hops between the components. Additionally, it is recommended to use SSL to secure access to servers located across such boundaries.
- When there is a firewall between any Agile Manager deployment components, ensure the proper configuration according to the vendor recommendation.
- Run periodic trusted root Certificate Authority certificate updates on your clients and servers to ensure that the publisher certificates used in digital code signing are trusted.

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

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

Secure attachment files

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

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

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

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

Secure the application server

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

- Always use the minimal possible permissions when installing and running Agile Manager. For example, install Agile Manager using sudo permissions, and run Agile Manager as a simple user with no special permissions. For details, see "Install as a non-root user" on page 12 and "Run Agile Manager as a simple user" on page 32.
- When configuring SSL on the Agile Manager application server, keep your keystore in a private directory with restricted access. Although the Java keystore is password protected, it is vulnerable as long as the password was not changed from its default value of **changeit**. For details, see "Configure SSL authentication" on page 44.
- Always obfuscate passwords entered into the **jetty.xml** file. For details, see http://www.eclipse.org/jetty/documentation/current/configuring-security-secure-passwords.html.
- Always modify the default passwords when prompted, such as the default **sa** user password, or the confidential data passphrase.

Application server security FAQs

Question	Answer
Are application resources protected with permission sets that allow only an application administrator to modify application resource configuration files?	Yes. Only the user with permission to access specific directories on the Agile Manager application server machine can modify Agile Manager configuration files.

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 the *Agile Manager Help Center*.
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

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

Use SSL between system components

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

For details, see "Configure SSL authentication" on page 44.

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

DMZ architecture using a firewall

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

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

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

Reverse proxy architecture

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

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

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

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

For example of how to configure a reverse proxy, see "Integrate an Apache web server (example)" on page 46.

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.
- 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 **Users** > **Settings** page in the Agile Manager Administration site.

  For details, see Enable LDAP over SSL topic in the *Agile Manager Help Center*.
- **Application server / Mail server.** Specify a secure port when defining the mail server.
- **Reverse proxy or load balancer / Application server.** Configure the Agile Manager application server with SSL.

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

Secure site administration

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

- Secure the Administration site by changing the site administrator password during the initial setup (see "Enter site administrator login information" on page 29), or later in the Agile Manager Administration site. Use the Administration site to designate other site administrators.

  To manage site administrators and passwords, see the **Users** > **User Management** administration page. Use a strong password for the site administrator.
- Restrict project customization by modifying user permissions in the Agile Manager configuration area (**Project** > **Project Users**).
- To debug user actions, set the log level to **Debug** in the Agile Manager Administration Site (**Servers** > **Application**). Be sure to revert the log level back to the previous value when you are finished debugging.

For details see "Log in to Agile Manager" on page 33 and the *Agile Manager Help Center*.

Secure user authentication

Agile Manager supports the following authentication methods:

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

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

For details see "Log in to Agile Manager" on page 33 and the *Agile Manager Help Center*.

Secure authentication FAQs

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

Secure user authorization

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

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

Users can have any of the following roles:

Role	Description	Location defined
Site administrator	Authorized to access the Agile Manager Administration site and modify site administration values.	Agile Manager Administration site (**Users** > **User Management**)
Project administrator	Has full permission in the Agile Manager application and configuration areas. Project administrators can restrict the applications that team members have access to	Agile Manager configuration area (**Project** > **Project Users**)
Team member	Has full permissions in the application area and read-only access to the configuration area. Users can view only items associated with the applications to which they have access.	Agile Manager configuration area (**Project** > **Project Users**)

For details, 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 project upgrade.

  You can restore your project to a specific backup file using the Agile Manager Administration site (**Servers** > **Database Server**). For details, see the *Agile Manager Help Center*.

- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.

- Data backup consumes a lot of resources. It is strongly recommended to avoid running backups during peak demand times.

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

Data encryption

Agile Manager supports the following types of encryption:

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

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

  Agile Manager uses the following security configuration:

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

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

- **Password encryption.** User passwords are never stored.Only the hash versions of passwords are stored.

- **Transparent Data Encryption (TDE).** Agile Manager is certified to work with TDE for Oracle databases.

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

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

Encryption FAQs

Question	Answer
Does Agile Manager transmit account passwords in an approved encrypted format?	It is strongly recommended to enable SSL on the Agile Manager and LDAP servers to ensure secure account password transmission. For details, see "Uninstall Agile Manager" on page 51 and **Enable LDAP over SSL** in the *Agile Manager Help Center*.
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 39.
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 23.

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.

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

Recommendations:

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

Log levels and log rotations are set using the Agile Manager Administration site (**Servers** > **Application**). For details, see the *Agile Manager Help Center*.

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 authentication

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

Caution: This procedure must be performed only after installing Agile Manager. For details, see "Install Agile Manager" on page 23.

1. Obtain the server certificate issued to the name of this server in java keystore format. It must contain a private key and the certificate authority that issued it.
2. Verify that all users have logged out of Agile Manager, and stop the Agile Manager service:
   `/opt/hp/agm/wrapper/HPALM stop`
3. Navigate to the **/opt/hp/agm/server/conf/** directory and make a backup of the **jetty.xml** file:

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

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

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

5. In the added section, do the following:
   - Replace the **/home/admin/Downloads** path with the location of your keystore file.
   - If you want to change the port number, replace **8443** with the new port number.
   - If you have changed the default keystore password, replace **changeit** with the new password.
6. (Optional) To encrypt the password, perform the following steps:
   a. Run: `./java -cp ".:/opt/hp/agm/lib/*:/opt/hp/agm/lib/ext/" org.eclipse.jetty.http.security.Password <password>`

      For example, if you run the following command:

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

      The output will appear as follows:

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

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

   For example:

   ```
   <!--
   <Call name="addConnector">
   <Arg>
   <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
   <Set name="host"><Property name="jetty.host" /></Set>
   <Set name="port"><Property name="jetty.port" default="8080"/></Set>
   ```

```
<Set name="maxIdleTime">300000</Set>
<Set name="Acceptors">2</Set>
<Set name="statsOn">false</Set>
<Set name="confidentialPort">8443</Set>
<Set name="lowResourcesConnections">20000</Set>
<Set name="lowResourcesMaxIdleTime">5000</Set>
</New>
</Arg>
</Call>
-->
```

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

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 using the following URLs:

Agile Manager	`https://<server>:<port>/agm/login/index.jsp`
Agile Manager Administration site	`https://<server>:<port>/agm/webui/alm/sa/admin.jsp`

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 38.

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

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

1. Verify that the Apache Web server is stopped.
2. Navigate to the **<Apache Home directory>\conf** directory.

3. Open the **httpd.conf** file.
4. Uncomment or add the following load module commands:

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

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

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

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

```
# Turn off support for true Proxy behavior as we are acting as     a reve
rse 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 direc
tive can be

# used to send requests received on a particular URL to a Jetty instance.

ProxyPreserveHost off

ProxyPass /qcbin http://localhost:8080/qcbin

ProxyPassReverse /qcbin http://localhost:8080/qcbin

ProxyPass /agm http://localhost:8080/agm

ProxyPassReverse /agm http://localhost:8080/agm


# Rewrite rule trailing slash must be used in the VirtualHost sectionLoad
Module rewrite_module modules/mod_rewrite.so

RewriteEngine On

# Add trailing slash if was not present in the original request

#RewriteRule ^/qcbin$ /qcbin/ [R]
```

6. Save the changes to the file.
7. Restart the Apache Web server. Connect to Agile Manager using the following URLs (the port number in this syntax is optional):

Agile Manager	`https://<server>:[<apache port>]/agm/login/index.jsp`
Agile Manager Administration site	`https://<server>:[<apache port>]/agm/webui/alm/sa/admin.jsp`

Manage the application server

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

"Change the heap memory size" below

"Changing the application server port number" below

"Application server management tools" on the next page

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 Project** option in the Agile Manager Administration site (**Servers** > **Database**). For details, see the *Agile Manager Help Center*.

Change the heap memory size

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

Note:

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

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

Changing the application server port number

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

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

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

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

Application server management tools

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

Tool	Address
jconsole	http://java.sun.com/developer/technicalArticles/J2SE/jconsole.html **Note:** 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

Uninstall Agile Manager

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

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

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

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

4. (Optional) To remove all traces of Agile Manager from the machine, delete all remaining files in the installation directory as well as the deployment path.

   - Removing the **conf** directory will require you to manually add values the next time you run the configuration wizard.
   - Removing the **repository** directory also removes all project repositories. The database is still retained unless it is specifically deleted.

Troubleshooting

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

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

If an error message displays during the installation indicating that 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.

For details, see "Uninstall Agile Manager" on the previous page.

We appreciate your feedback!

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

Feedback on Installation Guide (Agile Manager 2.0)

Just add your feedback to the email and click send.

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