

HP Enterprise Maps

Software Version: 2.00
Windows and Linux Operating Systems

Administration Guide

Document Release Date: January 2015, Edition 2
Software Release Date: January 2015, Edition 2



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2014-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Intel® Xeon® and Intel® Core i7® are registered trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP and Windows 7® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of TheOpenGroup.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

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

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

Support

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

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>

About this PDF Version of Online Help

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

Contents

Chapter 1: Administration Overview	7
Security and Access Control	8
Chapter 2: Domain Management	10
Domains	11
How to Create and Delete Domains	14
How to Manage User Roles in Domains	14
How to Manage Default Access Rights	15
How to Export Domain Content	18
Chapter 3: User Management	19
How to Disable and Enable Users	19
How to Assign Users to Groups and Roles	20
How to Set Default Domains for Users	21
How to Set Default Domains for Groups	21
How to Set New Artifact Ownership	22
How to Import Users from LDAP	23
How to Synchronize Profiles with LDAP	24
Chapter 4: Group Management	25
How to Manage Group Membership	25
How to Assign Groups to Roles	26
How to Set Default Domains for Groups	26
How to Retire and Delete Groups	27
Chapter 5: Role Management	28
Roles	28
Roles in the User Interface	30
Roles in Lifecycle	30
Catalog User Role	32
Administrator Role	32
How to Manage Roles	33
How to Change the Sharing Principal	34
Create Role Page	34
Chapter 6: Lifecycle Process Management	35
How to Create Lifecycle Processes	35
How to Define Stages	36
How to Define Transitions	38
How to Define Tasks	40

How to Define Policies	40
How to Define Approvers	41
How to Define Automatic Actions	43
How to Define Permissions	44
How to Publish a Process	45
How to Export Lifecycle Processes	45
Lifecycle Best Practice	45
Application Lifecycle	47
Service Lifecycle	48
Service Implementation Lifecycle	48
Project Lifecycle	49
Process Lifecycle	49
Process Implementation Lifecycle	50
Chapter 7: Administration Task Management	51
How to Run Tasks	52
How to Schedule Tasks	53
How to Add Change Management Tasks	54
How to Add Custom Tasks	54
Chapter 8: Product Integration Management	55
Configure HP EM to access integration server via HTTPS	55
Chapter 9: Configuration Management	56
How to Manage Basic Configuration Options	57
Configure EM to access integration server via HTTPS	58
How to Manage the System Configuration	58
How to Manage System Settings	59
How to Export and Import System Settings	60
System Configuration Properties	61
How to Manage Artifact Form Validation	77
Chapter 10: Administration Utilities	81
HP EM Utilities	81
Export Tool	82
Import Tool	85
Rebrand Tool	88
Reset Tool	88
SDM to Database Mapping Tool	89
Setup Tool	90
Changing the License Key	90
Applying Extensions	91
Updating HP EM	91

Advanced Setup Tool Options	91
Setup Tool Command-Line Options	92
SSL Tool	92

Chapter 1: Administration Overview

Administration in HP Enterprise Maps can be broadly divided into the following areas:

- **Managing Content**

The most important content management concept in HP EM is the use of *Domains*. The administrator can create a domain structure that represents your organizational structure. Each domain represents a working area with users assigned to specific roles within each domain and the content of the domain managed to restrict its visibility and access rights. For more details, see ["Domains" on page 11](#).

The administrator is also responsible for the day-to-day maintenance of the data content in the Catalog and reports about its status. HP EM provides a set of administration tasks that the administrator can execute manually or schedule to run at set times or periodically to maintain and update this information. For details, see ["Administration Task Management" on page 51](#).

- **Managing Users**

The management of users is normally delegated to an external user store, such as LDAP, where the management of the people and groups who actually use HP EM should take place. HP EM represents users with *User* artifacts which the particular user or an administrator can manage. Users can create additional *Contact* artifacts to represent external contacts who do not use the product in order to associate them with particular artifacts in the Catalog. For details, see ["User Management" on page 19](#).

If necessary, the administrator can add and manage additional local groups to organize users into groups that are not represented by the external user store. For details, see ["Group Management" on page 25](#). HP recommends using roles instead of creating local groups.

An important concept in HP EM is the use of *Roles*. Roles are generic job descriptions that can apply to users and groups in specific domains. The use of roles enables the administrator to manage generic templates for lifecycle processes and security management in the top-level global domain which the resolve to specific users and groups within each working domain. Roles also control user access to functionality in the user interface. For more details, see ["Role Management" on page 28](#).

Administrators within each domain are responsible for assigning users to roles within their domain. For details, see ["Domains" on page 11](#).

- **Managing Security**

The administrator is responsible for managing and controlling user access to Catalog content. HP EM uses Access Control Lists (ACL) to restrict access based on users, groups, or roles. For details, see ["Security and Access Control" on the next page](#).

- **Managing Global Artifacts**

HP EM uses domains to divide content into working areas with users assigned to specific roles within the domain. Containing all the working domains is a top-level domain which contains global artifacts which apply across all domains. HP EM restricts access to these artifacts and their management to the top-level administrator. For details, see ["Lifecycle Process Management" on page 35](#).

- **Product Integration**

The user needs to import the certificate of the server, the data of which needs to be imported and integrated into HP EM. This import activity must be done via HTTPS. For details, see ["Product Integration Management" on page 55](#)

- **Configuration and System Management**

The administrator is responsible for the configuration of each deployment of HP EM.

The Administration tab provides access to certain aspects of the configuration which can be managed while HP EM is running. For details, see ["Configuration Management" on page 56](#).

- **Administration Utilities**

The administrator is responsible for the command-line tools located in the bin directory of the Installation folder. For details, see ["Administration Utilities" on page 81](#)

Security and Access Control

Most organizations restrict access to resources by user and group permissions. HP EM extends this type of security by enabling the use of domain and role-based access rights.

HP EM uses Access Control Lists (ACL) to define who can access particular resources and their permissions. Each ACL consists of a set of Access Control Elements (ACE) which define the following for a resource or collection of resources:

- **User Identification**

The user identification as a specified user, a group of users, or a role that resolves to users and groups in the domain that the artifact belongs to.

- **Granted Permission**

One of the following:

- **Read Permission**

Access to read the data and metadata of an artifact or resource, or a collection of artifacts.

- **Write Permission**

Access to modify the data and metadata of an artifact or resource, or to create new artifacts, resources, and sub-collections, and update the metadata of a collection of artifacts. Users assigned as the owner of an artifact and administrators always have write permission.

ACLs apply in the following use cases:

- **Artifact Creation Rights**

The administrator can define which roles can create artifact types within a domain. Within the domain, the users in the allowed roles can access the artifact creation pages for the specified artifact types. The default creation rights are cumulative, so default rights given in the top-level domain apply in all other domains, and rights given to a group or role also apply in addition to rights given to each user in the group or role. For details, see ["How to Manage Default Access Rights" on page 15](#).

- **Governed Artifact Access Rights**

The access rights for artifacts in governance are determined by the lifecycle process applicable to the artifact. The administrator can assign rights and permissions to particular roles for each stage of a lifecycle process. Within a domain, these roles resolve to the assigned users and groups who have the specified access to the artifact at that lifecycle stage. For details, see ["How to Define Permissions" on page 44](#).

- **Ungoverned Default Artifact Access Rights**

In the cases where artifacts are not governed, the administrator can define which roles can read or write particular artifact types within a domain. Within the domain, the users in the allowed roles can access the artifact edit pages for the specified artifact types. In addition, you can extend this default access control functionality using particular values of categorization properties. For example, this enables you to define different access rights for services categorized as application services and for services categorized as infrastructure services. The default access rights are cumulative, so default rights given in the top-level domain apply in all other domains, and rights given to a group also apply to all the users of the group. For details, see ["How to Manage Default Access Rights" on page 15](#).

Chapter 2: Domain Management

HP EM enables the administrator to create a domain structure that reflects the organization of your business. Each artifact in the Catalog belongs specifically to one domain and the administrator can assign users specific roles in specific domains. This enables you to compartmentalize your Catalog and restrict the access and visibility of data to only the users who need it. For more details about the concept of domains, see ["Domains" on the next page](#).

Access domain management from the Administration tab. In the Administration menu, click **Domains** to view the list of all domains. Click a domain name to view its details.

Responsibility for domain management is divided into the following parts:

- **Managing the Domain Structure**

Users with the Administrator role have responsibility for the overall domain structure. Only the Administrator can create and delete domains. For details, see ["How to Create and Delete Domains" on page 14](#).

- **Managing a Domain**

The Administrator can assign a separate administrator for specific domains. Users with the administrator role within a domain are responsible for the following:

- Editing the domain.
- Setting the default role for the domain. For details, see ["How to Manage User Roles in Domains" on page 14](#).
- Assigning users to roles in the domain. For details, see ["How to Manage User Roles in Domains" on page 14](#).
- Managing default permissions in the domain. For details, see ["How to Manage Default Access Rights" on page 15](#).

- **Setting Default Domains**

When users sign in they access their default domain. The administrator can set default domains for users and groups and individual users can set their own default domain. For details, see ["How to Set Default Domains for Users" on page 21](#) and .

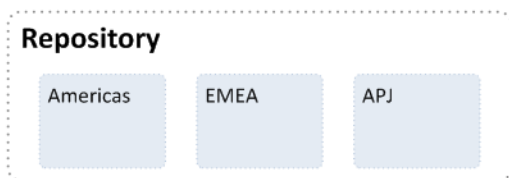
Note: By default, HP EM contains a default domain which users who are not assigned to a specific working domain sign-in to. To change which domain is the default, change the setting of the `platform.catalog.defaultUiAdapter.defaultDomain` property to the Domain ID of the required domain. For details, see ["How to Manage System Settings" on page 59](#). The administrator can also disable default domain sign-in to prevent users who are not assigned to

a specific working domain from signing-in. For details, see ["How to Disable and Enable Users" on page 19.](#)

Domains

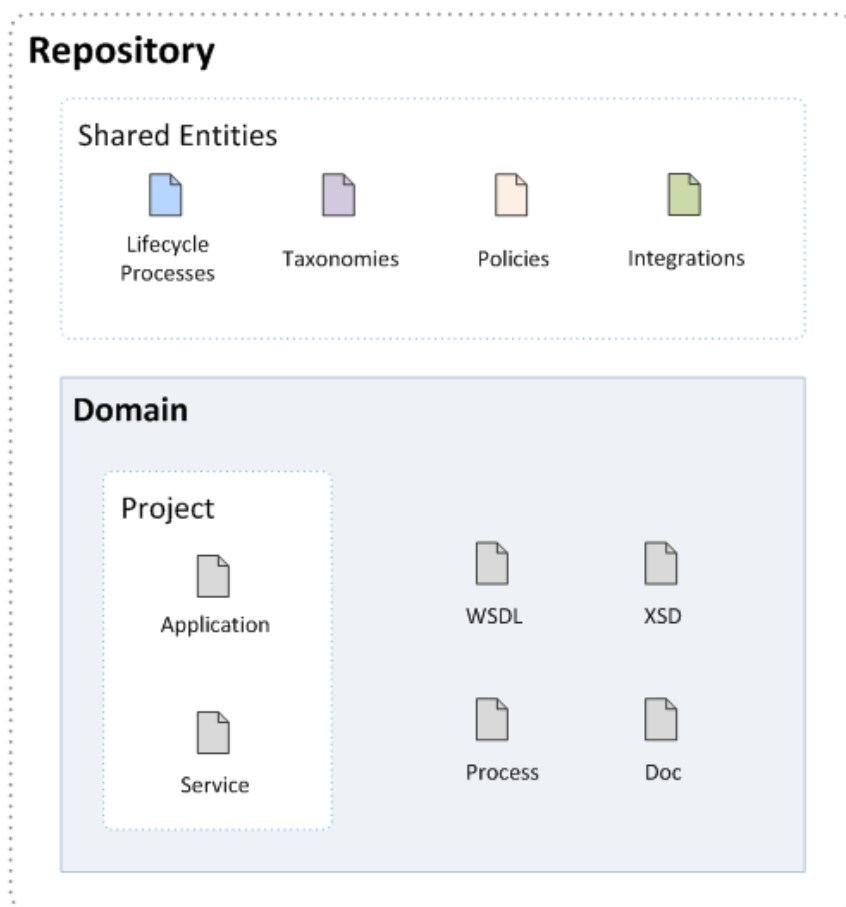
Domains provide a logical separation of data within the Catalog. Each domain can represent a discrete working area for an individual department or organizational unit. This separation allows users to focus on the data that is most relevant to them and enables data to be structured by working area.

In this release, HP EM provides support for a single layer of domains within a global top-level repository domain. For example, a domain structure representing organizational regions, Americas, EMEA, and APJ.



After installation, HP EM consists of the top-level repository domain and a default domain. The default domain represents a default working area for all users until the administrator creates additional working area domains and assigns users to them.

The top-level domain is a special domain containing system and global data, such as lifecycle processes, policies, and taxonomies, which apply across all domains, and each working domain contains the specific data relevant to users of that domain.



The exact separation of data between the top-level and working domains is as follows:

Top-Level Domain (Global Configuration)

- Lifecycle Processes
- Taxonomies
- Policies
- Roles Definition
- System settings (including SDM and UI customizations)

Working Domains

- Artifacts (for example, Services, Applications, WSDLs, and Documents) that belong to the domain
- User Role Assignments (for example, Joe is an architect in the EMEA domain)
- Default Settings (for example, a default server folder)
- BSM/UCMDB / SparX EA / PPM / RDBMS servers

Working domains inherit all settings applied in the top-level repository domain. For example, access rights, roles, and lifecycle processes set in the top-level domain apply in all domains.

This domain structure creates a logical separation, not only between departments or organizational units, but also between global functions and working area domain functions.

Users in HP EM perform specific functionality based on the roles assigned to them and the user interface restricts their access to functionality and artifacts based in these roles.

The user roles are split into the following user types:

- **Top-Level Repository Administrators**

Global administration with responsibility for the following functional areas:

- Domain Management for all domains. For details, see ["Domain Management" on page 10](#).
- Lifecycle process Administration. For details, see ["Lifecycle Process Management" on page 35](#).
- User and Group Management. For details, see ["User Management" on page 19](#) and ["Group Management" on page 25](#).
- Role Administration. For details, see ["Role Management" on page 28](#).
- Server Configuration Management. For details, see ["Configuration Management" on page 56](#).
- The Administrator can also access all the functionality of Domain Administrators.

- **Domain Administrators**

Users assigned to the administrator role in a specific domain with responsibility for the following functional areas:

- Domain Management for all domains. For details, see ["Domain Management" on page 10](#).
- Management of administrative tasks within their domain. For details, see ["Administration Task Management" on page 51](#).

- **Domain Users**

Users assigned to a specific role within a domain with specific functionality associated with that role. The same user can access different domains in different roles.

This separation of functions and roles is described in more detail in ["Roles" on page 28](#).

Each artifact belongs to exactly one domain. This domain is set to the current domain when a user creates an artifact. Typically, the domain does not change during the artifact lifecycle, but if required it is possible to transfer single artifact or multiple artifacts from one domain to another one using the Change Domain operation.

By default, artifacts are only visible in the owning domain but they can be explicitly shared for all users across all domains using the Share operation. . Typically, this operation applies to artifacts entering

production and associated with a lifecycle process. For details, see ["How to Define Automatic Actions" on page 43](#).

How to Create and Delete Domains

The Administrator has responsibility for creating and deleting domains within the Catalog.

Access domain management functionality in the Administration tab. In the Administration menu, click **Domains** to open the Domains page. The Domains page provides Add and Delete Domain functionality for Administrators.

To Add Domains:

1. In the Domains page, click **Add Domain** to open the Create Domain page.
2. In the Create Domain page, set a name and description for the domain.
3. *Optional:* Set a Default Domain Location to be the default location for attached data content.
4. Click **Save** to create the new domain.

All working domains exist in a single layer as sub-domains of the top-level global domain. Administrators of the top-level domain have administrative rights in all domains and can assign users and groups to be administrators of specific domains.

To Delete Domains:

1. In the Domains page, select the domains to delete.
2. Click **Delete**, and confirm your choice to delete the selected domains.

Note: You cannot delete a domain if it contains any artifacts..

How to Manage User Roles in Domains

The administrator of a domain is responsible for assigning users to roles in the domain. For more details and domains and roles, see ["Domains" on page 11](#) and ["Roles" on page 28](#).

Managing roles in a domain consists of setting a default role and assigning users and groups to specific roles in the domain.

Note: If the administrator assigns a role to a user or a group in the top-level domain, the role assignment applies to all domains.

To Set a Default Role for a Domain:

1. In the Domain detail page select the Overview tab.
2. In the Default Role section, click **(Change)** to open the Choose Role dialog box.
3. Select the role from the list. Optionally, use the filter to find a particular role.
4. Click **Select** to set the selected role as the default role for the domain.

HP EM assigns the selected role to any user who signs into the domain who does not have a role assignment for the domain.

To Assign Users and Groups to Roles for a Domain:

1. In the Domain detail page select the Roles tab.
2. Select the role that you want to add users or groups to.
3. Click **Add Member** to open the Add Member dialog box.
4. Do one of the following:
 - Select the Users tab, and select the users to add. Optionally, use the filter to locate a particular user.
 - Select the Groups tab, and select the groups to add. Optionally, use the filter to locate a particular group.
5. Click **Select** to add the selected users and groups to the selected role in the domain.

To Assign Roles to Users and Groups for a Domain:

1. In the Domain detail page select the Members tab.
2. Click the Edit icon in the Roles column for the user or group you want to assign roles to. The Change Roles dialog box opens.
3. Select the roles that you want to add to the user or group. Optionally use the input dialog to search for a specific role.
4. Click **OK** to add the roles to user or group in the domain.

Once users or groups are assigned to roles within a domain, the administrator can extend their role memberships within specific domains. For details, see ["How to Assign Users to Groups and Roles" on page 20](#) and ["How to Assign Groups to Roles" on page 26](#).

How to Manage Default Access Rights

The administrator of a domain is responsible for defining who is able to create artifacts within the domain they manage. They can also define who has read and write access to artifact types. For more details about domains and security, see ["Domains" on page 11](#) and ["Security and Access Control" on page 8](#).

To access default access rights, in the Administration tab Administration menu, click **Domains** to open the Domains browse page. Select the domain that you administrate to open its details page and select the **Default Access Rights** tab.

The Default Access Rights tab displays the current Artifact Creation and Read / Write Access permissions for the domain.

Note: Domains inherit all default access rules from the top-level global domain and displays them as non-editable rules for the domain. Any permission rules set within the scope of the domain are additive to those global rules. The administrator of the top-level domain can edit these global rules from the detail page of the top-level domain.

To Manage Artifact Creation Rights:

1. In the Administration tab Administration menu, click **Domains** to open the Domains browse view.
2. Click the name of the domain you want to set creation rights for to open its details page.
3. Select the **Default Access Rights** tab to view the current permissions for the domain.
4. In the Artifact Creation table, do one of the following:
 - **To Add Artifact Creation Rules:**
 - i. Click **Add Rule** to open the Add Artifact Creation Rule page.
 - ii. Select the artifact type to add creation rights for from the **To Artifact Type** drop-down list.
 - iii. In the Granted To table, click **Add Member** to open the Add Member dialog box.
 - iv. Click **Browse Address Book** and select the roles to add creation rights for the selected artifact type. Optionally, use the dialog search input to find a particular role.
 - v. Click **Select** to add the selected roles to the Granted To table.
 - vi. Click **Save** to add the rule for the selected artifact type to the Artifact Creation table.
 - **To Edit Artifact Creation Rules:**
 - i. Click the **Edit** link for the rule to open the Edit Artifact Creation Rule page.
 - ii. Use the Granted To table to add and remove roles from the rule.
 - iii. Click **Save** to apply the changes to the rule to the Artifact Creation table.
 - **To Remove Artifact Creation Rules:**
 - Select the rules to remove, click **Remove Selected**, and confirm your decision.

To Manage Default Read / Write Access:

1. In the Administration tab Administration menu, click **Domains** to open the Domains browse view.
2. Click the name of the domain you want to set creation rights for to open its details page.
3. Select the **Default Access Rights** tab to view the current permissions for the domain.
4. In the Read / Write Access table, do one of the following:
 - **To Add Read / Write Access Rules:**
 - i. Click **Add Rule** to open the Add Read / Write Access Rule page.
 - ii. Select to add **Read** only or **Read / Write** access.
 - iii. Select the artifact type to add read / write access for from the **To Artifact Type** drop-down list.
 - iv. In the Granted To table, click **Add Member** to open the Add Member dialog box.
 - v. Select the roles, users, or groups to add read / write access for the selected artifact type. Optionally, use the dialog search input to find a particular role, user, or group.
 - vi. Click **Select** to add the selected roles, users, and groups to the Granted To table.
 - vii. *Optional:* Use the Condition table to add conditions to the access rule. These conditions enable you to further restrict access rights based on artifact type specific rules.
 - viii. Click **Save** to add the rule for the selected artifact type to the Read / Write Access table.
 - **To Edit Read / Write Access Rules:**
 - i. Click the **Edit** link for the rule you want to edit to open the Edit Read / Write Access Rule page.
 - ii. Select **Read** only or **Read / Write** access.
 - iii. Use the Granted To table to add and remove roles, users, and groups from the rule.
 - iv. *Optional:* Use the Condition table to edit conditions for the access rule. These conditions enable you to further restrict access rights based on artifact type specific rules.
 - v. Click **Save** to apply the changes to the rule to the Read / Write Access table.
 - **To Remove Read / Write Access Rules:**
 - Select the rules to remove, click **Remove Selected**, and confirm your decision.

Note: The default read and write permissions only apply to artifacts that are not governed by a lifecycle process or where the initial stage of the governing lifecycle process does not define access rights.

Caution: Do not remove write permission from the Contacts artifact type for the system#registered group. This permission is required for the registration of new users.

How to Export Domain Content

The administrator can export the content of an entire domain. Using this functionality for the top-level domain enables you to export the entire content of the Catalog.

Caution: The export / import functionality of the UI is not compatible with the command-line export / import tools available to the administrator. For more details about command-line export / import, see *HP Enterprise Maps Developer Guide - CSV Import and Export Tools*.

To Export Domains:

1. In the Domain Details page Overview tab, click the **Export** context action to open the Export dialog box.
2. *Optional:* Change the name of the archive.
3. *Optional:* Expand **Advanced Options**, and select from the following options:

Advanced Option	Description
Data	Select to export all artifacts that are assigned to the domain.
System Settings	Select which domain settings to export.

4. Click **Export** to create a ZIP archive containing the domain artifacts.

This process executes as a bulk operation. An information bar opens informing you that the operation is in progress with a progress bar with options to **Stop** the operation or to **Notify Me** when the operation is complete.



The operation executes asynchronously, so you can navigate and perform other tasks while the operation completes.

5. When the export archive is complete you are prompted for a download location. Alternatively, open the export report and click **Download Content** to save the archive.

The archive is available for import using the Import Repository Archive functionality.

Chapter 3: User Management

HP EM delegates user management to LDAP or an application server user store. Users are represented in HP EM by user artifacts for artifact ownership, notification, and contact purposes.

User artifacts represent users in the user store and contact artifacts represent external contacts. A contact does not have a corresponding LDAP or application user store account and cannot sign in.

When users first sign in, they are authenticated against the external user store and HP EM creates a user artifact based on their external account.

Note: HP EM also checks new users against existing contacts. If a matching contact artifact exists, the login name is attached and the contact becomes a user artifact.

Responsibility for user management is divided into the following parts:

- Each user can manage their own user artifact.
- Users with appropriate permissions can create new contacts in the Catalog tab.

Caution: Only create contacts for people who need to be represented in the Catalog but who do not need to use HP EM. Use LDAP or your application server user store to create users who use HP EM.

- The Administrator is responsible for the following aspects of user management:
 - ["How to Disable and Enable Users" below](#)
 - ["How to Assign Users to Groups and Roles" on the next page](#)
 - ["How to Set Default Domains for Users" on page 21](#)
 - ["How to Set New Artifact Ownership" on page 22](#)
 - ["How to Import Users from LDAP" on page 23](#)
 - ["How to Synchronize Profiles with LDAP" on page 24](#)

How to Disable and Enable Users

The administrator can block access to HP EM by disabling users.

To Disable Multiple Users:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Select the users to disable.
3. Click **Disable** and confirm your selection to block the selected users from accessing HP EM.

To Disable or Enable a Single User:

1. In the Administration tab Administration menu, click Users to open the Users browse page.
2. Click the name of the User you want to Disable or Enable to open their User details page.
3. In the User details page Overview tab, click the **Disable** or **Enable** context action.

How to Assign Users to Groups and Roles

The administrator can assign a user to be a member of multiple groups or roles within specific domains.

To Assign Users to Groups:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Click the name of the User to open its detail page.
3. Select the **Groups and Roles** tab to view the group details for the user.
4. In the Groups table, do one of the following:
 - **To remove the users from groups:**
 - i. Select the groups to remove the user from.
 - ii. Click Remove and confirm your decision.
 - **To add the users to groups:**
 - i. Click **Add to Group** to open the Add Groups to User dialog box.
 - ii. Select the groups to add the user to.
 - iii. Click **Select** to add the user to the selected groups.

The administrator can also manage the membership of groups from the group perspective. For details, see ["How to Manage Group Membership" on page 25](#).

To Assign Users to Roles:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Click the name of the User to open its detail page.
3. Select the **Groups and Roles** tab to view the role details for the user.

4. In the Roles by Domain section, click **Change** for the required domain to open the Change Role Membership dialog box.
5. Select the additional roles to assign to the user for the domain and click **Set** to apply the changes.

Note: This functionality is only available if the user is already assigned to roles in a domain and can only be used to extend the roles set there. For details, see ["How to Manage User Roles in Domains" on page 14.](#)

How to Set Default Domains for Users

The administrator can set the default domain that new users sign in to.

To Set the Default Domain for a Single User:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Click a user name to open their details page.
3. In the Overview tab Access Security section, click the Default Domain **Change** link to open the Set Default Domain dialog box.
4. Select a default domain and click **Select**.

When the user signs in for the first time they access the selected domain.

To Set the Default Domain for Multiple Users:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Expand Manage Members, and select **Set Default Domain** to open the Set Default Domain dialog box.
3. Select a domain from the list and click **Select** to set the domain as the default for new users.

When the selected users sign in for the first time they access the selected domain.

Default domains can also be set for groups and individual users can set their own default domain. For details, see ["How to Set Default Domains for Groups" on page 26](#)

How to Set Default Domains for Groups

The administrator can set the default domain that members of groups sign in to.

To Set the Default Domain for Groups:

1. In the Administration tab Administration menu, click **Groups** to open the Groups browse page.
2. Click the name of the group to open its details page.
3. Click **Set Default Domain** to open the Set Default Domain dialog box.
4. Select a domain from the list and click **Select** to set the domain as the default for the group.

When members of the selected group sign in they access the selected domain.

Default domains can also be set for users and individual users can set their own default domain.

How to Set New Artifact Ownership

By default, users who create artifacts become the *owner* of the artifact. The owner of an artifact has default read / write permission for the new artifact.

The administrator can configure new artifact ownership for users so that instead of the artifact ownership being assigned to the user, it is instead assigned to a specified role or group.

To Set New Artifact Ownership for a Single User:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Click a user name to open their details page.
3. In the Overview tab Access Security section, click the New Artifact Ownership **Change** link to open the Select New Artifacts Ownership dialog box.
4. Click **Change** to select a new owner.
5. Input a role or group search term or click **Browse Address Book** and select from the list of roles or groups.

Note: The users must be members of the selected group or assigned to the selected role in at least one domain.

6. Click **Select** to apply the new artifact ownership assignment to the selected users.

To Set New Artifact Ownership for Multiple Users:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Select the users to apply new artifact ownership assignment to.
3. Expand Manage Members, and select **Set New Artifacts Ownership** to open the Set New Artifacts Ownership dialog box.
4. Click **Change** to open the dialog box.

5. Input a role or group search term or click **Browse Address Book** and select from the list of roles or groups.

Note: The users must be members of the selected group or assigned to the selected role in at least one domain.

6. Click **Select** to apply the new artifact ownership assignment to the selected users.

When the selected users create artifacts, HP EM assigns ownership to the specified role or group.

How to Import Users from LDAP

If HP EM is synchronized with an LDAP user store you can create user artifacts based on corresponding LDAP accounts.

To Import LDAP Accounts:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. Click **Import** to open the Select Import Users dialog box.
3. Do one of the following:
 - Use the Search input and click **Search** to populate the Users list with users in the LDAP user store matching the search term.

Tip: Select a user from the *as-you-type* drop-down to immediately create a matching user artifact.

- Click **Browse Address Book** to populate the Users list with all the users in the LDAP user store.
4. Select users from the Users or Groups list, and click **Select** to create matching user artifacts.

This process executes as a bulk operation. An information bar opens informing you that the operation is in progress with a progress bar with options to **Stop** the operation or to **Notify Me** when the operation is complete.



The operation executes asynchronously, so you can navigate and perform other tasks while the operation completes.

Note: Import uses the LDAP cache so changes in LDAP may not be immediately visible in HP

EM.

How to Synchronize Profiles with LDAP

If HP EM is synchronized with an LDAP user store you can update user artifacts with the latest versions of the corresponding LDAP accounts.

To Synchronize Profiles with LDAP Accounts:

1. In the Administration tab Administration menu, click **Users** to open the Users browse page.
2. In the Users browse page, select the users you want to synchronize.
3. Click **Synchronize** and confirm your decision.

This process executes as a bulk operation. An information bar opens informing you that the operation is in progress with a progress bar with options to **Stop** the operation or to **Notify Me** when the operation is complete.



The operation executes asynchronously, so you can navigate and perform other tasks while the operation completes.

Note: Synchronize uses the LDAP cache so changes in LDAP may not be immediately visible in HP EM.

Chapter 4: Group Management

In addition to any groups managed by the external user store, the administrator can manage local groups in HP EM.

Note: HP Software recommend using roles instead of local groups.

Access group management from the Administration tab. In the Administration menu, click **Groups** to view the list of all groups. Click a group name to view its details.

To Create Groups:

- In the Groups page, click **Create Group** to open the New Group page.
- Enter a name and description, and optionally add group members as described in ["How to Manage Group Membership" below](#).

The administrator is also responsible for the following aspects of group management:

- ["How to Manage Group Membership" below](#)
- ["How to Assign Groups to Roles" on the next page](#)
- ["How to Set Default Domains for Groups" on the next page](#)
- ["How to Retire and Delete Groups" on page 27](#)

How to Manage Group Membership

The administrator is responsible for managing the membership of local groups.

To Manage Group Membership:

1. In the Administration tab Administration menu, click **Groups** to open the Groups browse page.
2. Click the name of the group to open its details page.
3. Click **Edit** to open the Edit Group page.
4. In the Members table, do one of the following:
 - **To remove users from the group:**
 - i. Select the users to remove from the group.
 - ii. Click **Remove** and confirm your decision.

- **To add users to the group:**
 - i. Click **Add Member** to open the Add Users to Group dialog box.
 - ii. Select the users to add to the group.
 - iii. Click **Select** to add the selected users to the group.
- 5. Click **Save** to apply your group membership changes.

The administrator can also manage the membership of groups from the user perspective. For details, see ["How to Assign Users to Groups and Roles" on page 20](#).

How to Assign Groups to Roles

The administrator can assign a group to be a member roles within specific domains.

To Assign Groups to Roles:

1. In the Administration tab Administration menu, click **Groups** to open the Groups browse page.
2. Click the name of the Group to open its detail page.
3. In the Roles by Domain section, click **Change** for the required domain to open the Change Role Membership dialog box.
4. Select the additional roles to assign to the group for the domain and click **Set** to apply the changes.

Note: This functionality is only available if the group is already assigned to roles in a domain and can only be used to extend the roles set there. For details, see ["How to Manage User Roles in Domains" on page 14](#).

How to Set Default Domains for Groups

The administrator can set the default domain that members of groups sign in to.

To Set the Default Domain for Groups:

1. In the Administration tab Administration menu, click **Groups** to open the Groups browse page.
2. Click the name of the group to open its details page.
3. Click **Set Default Domain** to open the Set Default Domain dialog box.
4. Select a domain from the list and click **Select** to set the domain as the default for the group.

When members of the selected group sign in they access the selected domain.

Default domains can also be set for users and individual users can set their own default domain.

How to Retire and Delete Groups

The Administrator can retire and then delete internal groups.

Note: These processes do not retire or delete the users who are members of these groups.

To Retire Multiple Groups:

- In the Groups browse page, select the groups to retire, click **Retire** and confirm your decision.

To Retire a Single Group:

1. In the Group details page, click the **Retire Group** context action to open the Retire Group dialog box.
2. Click **(Change)** to select a new owner for any artifacts owned by members of the group.

To Delete Multiple Groups:

- In the Groups browse page, select the groups to delete, click **Delete** and confirm your decision.

To Delete a Single Group:

- In the Group details page, click the **Delete Group** context action.

Note: A group must be retired before you can delete it.

Chapter 5: Role Management

HP EM enables the administrator to assign users to specific roles related to their job functions. These roles restrict their access to artifacts, and limit their functionality only to that appropriate to their role. For more details about the concept of roles, see ["Roles" below](#).

Access role management from the Administration tab. In the Administration menu, click **Roles** to view the list of all roles. Click a role name to view its details.

Responsibility for role management is divided into the following parts:

- **Managing Roles**

Users with the Administrator role have responsibility for the roles available in HP EM. Only the Administrator of the top-level domain can create and delete roles. For details, see ["How to Manage Roles" on page 33](#).

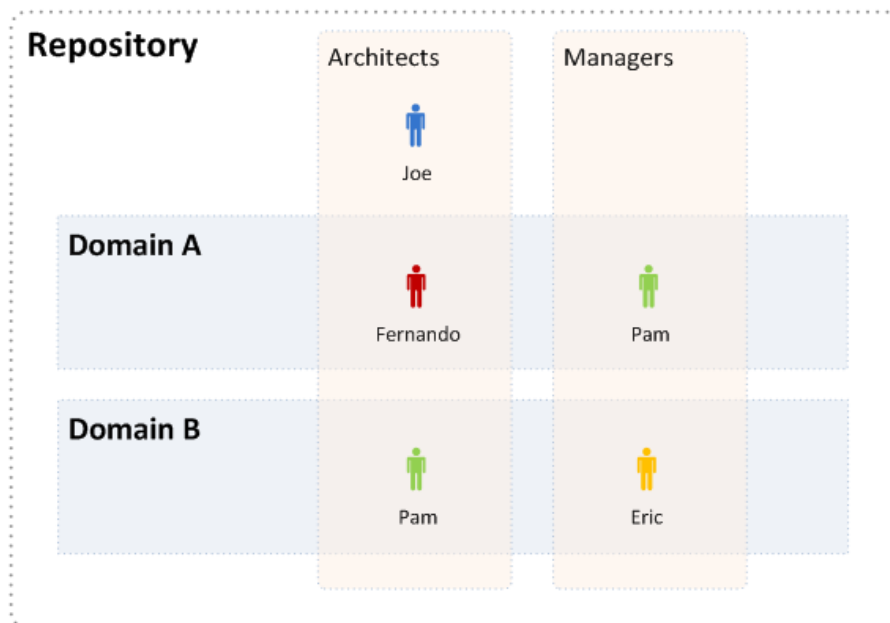
- **Assigning Users to Roles**

Users with the administrator role within a domain are responsible assigning users to specific roles within their domain and setting a default role for new users of the domain. For details, see ["How to Manage User Roles in Domains" on page 14](#).

Roles

HP EM offers functionality across the entire service development lifecycle. In most organizations, these functions are performed by many individuals and teams with specific permissions. HP EM uses *Roles* to enable you to define and assign these permissions, and use these assignments to focus each user or group on specific functionality and tasks and restrict their access to artifacts appropriate to their role.

The administrator defines roles in the top-level domain, but user assignment to roles can be global or to different roles in different domains. For example, in the following diagram, Joe is assigned a global architect role in the top-level repository domain, Fernando is assigned the architect role in Domain A, Pam is assigned the manager role in Domain A and the architect role in Domain B, and Eric is assigned to the manager role in Domain B.



These assignments mean that in Domain A, Joe and Fernando access functionality and artifacts relevant to the architect role, whereas Pam accesses functionality relevant to the manager role.

Pam has a different role in Domain B, so along with Joe, accesses architect functionality, whereas Eric accesses functionality relevant to the manager role.

To assign users or groups to roles, see ["How to Manage User Roles in Domains" on page 14](#). For more details about domains, see ["Domains" on page 11](#).

The following topics describe in more detail how HP EM uses roles:

- ["Roles in the User Interface" on the next page](#)

The UI uses roles to restrict the availability of functionality to users in appropriate roles.

- ["Roles in Lifecycle" on the next page](#)

You can create Lifecycle templates with specified tasks and actions assigned to specific roles.

- ["Catalog User Role" on page 32](#)

A role common to most users with access given to perform most tasks.

- ["Security and Access Control" on page 8](#)

HP EM restricts access to artifact types using ACLs which can use roles as well as users and groups.

The default roles and their assigned functionality is described in the following topic:

- ["Administrator Role" on page 32](#)

The administrator can extend the default roles by adding additional customized roles. For details, see ["How to Manage Roles" on page 33](#).

HP EM also includes a special role, Sharing Principal, specifically associated with sharing artifacts. By default, this role is associated with the `system#registered` group which represents all users who access HP EM. For more details, see ["How to Change the Sharing Principal" on page 34](#).

Roles in the User Interface

HP EM restricts access to UI functionality according to your role.

- **Catalog User**

The Catalog tab enables users in the Catalog User role to create, develop, and manage artifacts in architectures. For more details, see ["Catalog User Role" on page 32](#).

The Navigator tab provides a visual representation of the relationships between the artifacts. It provides various layouts and role-based filters to enable you to visualize the content of the repository from your point of view.

The Reports tab provides access to view and create reports on the Catalog content.

- **Administrator**

In addition to all the tabs and functionality accessible by users in the Catalog User role, administrators access an Administration tab to enable them to manage users, groups, roles, domains, and other system artifacts. For more details, see ["Administration Overview" on page 7](#).

Roles in Lifecycle

Lifecycle management makes use of roles to enable global lifecycle process management with role-based assignments in a lifecycle process template.

The administrator of the top-level domain manages lifecycle processes and uses roles to define the following:

- The user role responsible for approving particular lifecycle stages.
- The user roles with read-only, write access, and ownership permissions for artifacts at particular lifecycle stages.
- The user roles responsible for performing tasks associated with a lifecycle stage.
- The user roles that are automatically notified as a result of specific events within the lifecycle.

Within specific domains, these role assignments resolve to the users and groups assigned to the role in that domain. For example, consider the development stage of a lifecycle process for services.

The stage might consist of the following role assignments:

- A task to build and test the service assigned to the QA Engineer role.
- A stage approver in the Service Provider role.
- An automatic action to notify the users in the Operations Manager role when a service is approved at the development stage.

The screenshot displays the 'Application Component Lifecycle' configuration page. On the left, there is a navigation menu with 'Overview', 'Stages', and 'Permissions'. The main area shows a lifecycle flow diagram with stages: Candidate, Development, Production Shared, Deprecated Shared, and Retired. Below the diagram is a configuration panel with sections for Tasks, Policies, Approvers, and Automatic Actions. The 'Candidate' stage is highlighted with a green box, and the configuration panel below it is also highlighted with a green border.

In different domains, different users perform each of these roles. Within domains, HP EM replaces the roles in the template with the specific users and groups assigned to that role in that domain.

In the EMEA domain, this could result in the following specific assignments:

- A member of the EMEA QA Engineers group, assigned to the QA Engineer role, must complete the Build and Test task.
- An EMEA domain user, assigned to the Service Provider role, must approve the development stage for the service.
- When the service is approved, all users in the Operations Manager role in the EMEA domain are notified that the service is ready for deployment.

In the US domain these assignments are to different users and groups performing the same roles.

Catalog User Role

The Catalog User role is a common role for most users of Enterprise Maps. General users must be assigned to this role so that they can do most of the tasks including view, navigate and manage artifacts; view and print existing reports; and create new policy reports.

Users in the Catalog User role perform the following functions:

- Search and Discover artifacts. For details, see "Searching for Artifacts" in the *User Guide*.
- Collaborate with your colleagues, leave comments or rating on a particular artifact. For details, see "Collaboration Overview" in the *User Guide*.
- Author new Catalog content. For details, see "Creating Artifacts" and "Relationship Editor" in the *User Guide*.
- View and edit existing Catalog content. For details, see "Artifact View Page" in the *User Guide*.
- Visualize the Catalog content in Navigator graphical view.
- Synchronize Catalog content with integrated products. For details, see "Integrations" in the *User Guide*.
- Synchronize Catalog content with architecture tools. For details, see "Extension for Sparx Systems EA" in the *User Guide*.
- Participate in the lifecycle of Catalog content. For details, see "Lifecycle Overview" in the *User Guide*.
- View and print reports on Catalog content. For details, see "Reports" in the *User Guide*.

Administrator Role

HP EM provides an administrator role with responsibility for managing users, groups, roles, and system artifacts. The responsibilities of administrators vary according to the domain that they manage.

- **Top-Level Repository Administrators**

Global administration with responsibility for the following functional areas:

- Domain Management for all domains. For details, see ["Domain Management" on page 10](#).
- Lifecycle Process Administration. For details, see ["Lifecycle Process Management" on page 35](#).
- User and Group Management. For details, see ["User Management" on page 19](#) and ["Group Management" on page 25](#).
- Role Administration. For details, see ["Role Management" on page 28](#).

- Server Configuration Management. For details, see ["Configuration Management" on page 56](#).
- The Administrator can also access all the functionality of Domain Administrators.
- **Domain Administrators**

Users assigned to the administrator role in a specific domain with responsibility for the following functional areas:

 - Domain Management for their domain. For details, see ["Domain Management" on page 10](#).
 - Management of administrative tasks within their domain. For details, see ["Administration Task Management" on page 51](#).

How to Manage Roles

The Administrator has responsibility for managing roles in HP EM. For details about the concept of roles, see ["Roles" on page 28](#).

To view the list of roles in HP EM, in the Administration tab Administration menu, click **Roles** to open the Roles browse page.

The Roles browse page provides the following functionality:

- **Delete**

Select the roles to delete, and click **Delete**.

Note: You cannot delete the default roles.

- **Create Role**

Click **Create Role** to open the ["Create Role Page" on the next page](#).

After you create a role, it is available for user and group assignment, for use in lifecycle processes, and for default access rights.

Click a role name to open its details page, showing its properties and UI Access details.

Click **Edit** to change the details for a role. For system roles, you can only change the UI Access details. For details of the Edit Role page parameters, see ["Create Role Page" on the next page](#).

For details about using roles, see the following topics:

- ["How to Manage User Roles in Domains" on page 14](#)
- ["How to Create Lifecycle Processes" on page 35](#)
- ["How to Manage Default Access Rights" on page 15](#)

How to Change the Sharing Principal

The Sharing Principal is a special role associated with sharing artifacts to make them visible to more users. The default functionality is to use the `system#registered` group which represents all users who access HP EM.

To Change the Sharing Principal:

1. In the Administration tab Administration menu, select **Domains** to open the Domains page.
2. Select the Top-Level domain to open the Domains details page.
3. Select the Roles tab to view the roles and their membership for the domain.
4. Select the Sharing Principal role to view its membership.
5. Use **Remove Selected** and **Add Member** to edit the membership of the role.

The selected users and groups see any artifacts that are shared.

Create Role Page

The Create and Edit Role pages contain the following parameters:

Parameter	Definition
Name	Name of the Role.
Description	A description including rich text and HTML support. This description displays in the Artifact Details page Overview tab properties area. This description is limited by the display length available in the Overview tab. If you need a longer description or an artifact specification edit the Specification property.
Sub-Roles	Select from the set of existing roles to inherit their functionality and artifact access for the new role.
Additional UI Access	Select whether users in the new role can access additional specified tabs.
Allows Login	Allow users in the new role to access the UI.

Chapter 6: Lifecycle Process Management

Before a Lifecycle Process can be used, it must be first defined and published by a user with Administrator rights.

A Lifecycle Process can also be copied and modified so as to maintain certain values rather than having to be constructed from the beginning.

Lifecycle Processes are defined by clicking **Lifecycle Processes** under the Administration tab and either selecting an existing process for modification or clicking **Create** to build a new one.

In the Lifecycle Process Overview or Stages tab it is possible to edit, publish, clone, delete or export the current process by clicking on the appropriate action.

The following tasks may be required when defining a new, or editing an existing Lifecycle Process:

- ["How to Create Lifecycle Processes" below](#)
- ["How to Define Stages" on the next page](#)
- ["How to Define Transitions" on page 38](#)
- ["How to Define Tasks" on page 40](#)
- ["How to Define Policies" on page 40](#)
- ["How to Define Approvers" on page 41](#)
- ["How to Define Automatic Actions" on page 43](#)
- ["How to Define Permissions" on page 44](#)
- ["How to Publish a Process" on page 45](#)
- ["How to Export Lifecycle Processes" on page 45](#)

["Lifecycle Best Practice" on page 45](#) describes HP recommended principles for lifecycle governance and describes the default lifecycle processes included with HP EM.

See "Lifecycle Overview" in the *User Guide* for the user view of Lifecycle Processes.

How to Create Lifecycle Processes

The first step in artifact lifecycle management is the creation of a lifecycle process.

To create a new lifecycle process:

1. In the Administration menu, click **Lifecycle Processes** to open the Lifecycle Processes page, and then click **Create**.
2. In the upper section, enter a **Name** and **Description** for the lifecycle process.
3. Define the lifecycle stages for the lifecycle process as follows:
 - a. Select the Root Artifact Type from the drop down list.
 - b. Optionally select the Sub-Artifact Type(s) by selecting the check box of the required types
 - c. Traverse ArchiMate relationships: if unchecked, ArchiMate relationships are completely ignored on searching for sub-artifacts.
 - d. Traverse 'Composed of' only: if checked, when searching for sub-artifacts all ArchiMate relationships are ignored except 'Composed of'.
4. If the new process is to be automatically assigned to artifacts, click the check box and add categories for **Categorized as** and **Not Categorized as** to apply taxonomic association rules for the automatic assignment of the lifecycle process to artifacts based on their categorizations
 - **In Categories:** Artifacts must contain these categories to be automatically assigned to the lifecycle process.
 - **Not In Categories:** Artifacts must not contain these categories to be automatically assigned to the lifecycle process.
 - **In Domains:** Select which domains lifecycle process will be used in.

Note: In cases where two or more automatically assigned lifecycle processes apply for an artifact type, HP EM uses these association rules to assign the most appropriate lifecycle process.

5. Click **Save**.

The status of a newly created lifecycle process is set to **Draft** and the user is redirected to the Overview tab of the process page in which lifecycle stages can be defined.

How to Define Stages

Lifecycle stages represent important milestones in the lifecycle process. Lifecycle stages and their order are defined in the lifecycle process definition. New lifecycle processes have no stages assigned to them.

To define lifecycle stages:

1. In the Administration menu of the Administration interface, click **Lifecycle Processes** to open the Lifecycle Processes page, and then click the name of the required process.

The Lifecycle Processes page opens in the **Overview** tab.

- To set a initial stage definition for artifacts click **Add Stage**. The Add Initial Stage dialog opens

Screenshot: Add Stage Dialog

- Select Stage name from dropdown list or the user may enter a custom name.

Click the **Share Artifacts** radio button and select when the artifact will be shared if required (this can also be altered in the **Permissions** tab). The *After Approval* option is not available if the transition to the next stage is automatic.

Click **OK**

Additional stages can be added by clicking **Add Stage**, selecting a Stage name and a transition type.

Any process can be edited, cloned, exported, deprecated or deleted by clicking the appropriate button

It is also possible to add the same stage into a process multiple times. These are called referral stages and are visually different from regular stages. Attempting to edit a referral stage will automatically send the user back the properties of the initial version of that stage.

- Before publishing the process, go to the Stages tab and do the following:

Note: A valid stage definition must contain at least one of the following conditions.

- Set transitions
For details, see "[How to Define Transitions](#)" below
- Set voters for approval
For details, see "[How to Define Approvers](#)" on page 41.
- Define tasks to complete before stage approval.
For details, see "[How to Define Tasks](#)" on page 40
- Set policies to comply with before stage approval.
For details, see "[How to Define Policies](#)" on page 40
- Define automatic actions to execute when a lifecycle transition occurs.
For details, see "[How to Define Automatic Actions](#)" on page 43"
- Specify whether to automatically promote on stage approval
For details, see "[How to Define Permissions](#)" on page 44

Click **Save** to save the Stage Definition and return to the Lifecycle Process page.

All stage details are listed. You can edit or copy a stage definition using **Edit** or **Copy**. Stages can also be deleted by clicking the **Delete** link.

When process is complete, click **Publish** to make active.

Note: Stage layout cannot be changed once the process is published.

How to Define Transitions

When adding a stage a type of transition is required by HP EM and there are three options to choose from.

Screenshot: Transition Options

Add Stage [Close]

Name: [Dropdown]

Share Artifacts [Dropdown]

Transition from Candidate

Automatically, When Candidate is Approved

Manually, After Candidate is Approved

Manually, Anytime

[OK] [Cancel]

Automatically, When stage_name is Approved

- Stage will transition to the next stage as soon as approved by designated approvers.

Manually, After stage_name is Approved

- Stage will require approval from all designated approvers before it can be manually advanced to the next stage.

Manually, Anytime

- Stage does not require approval from all designated users before being manually advanced

Hovering over the stage or the transition between stages and clicking the pencil icon allows you to edit a transition.

Note: If a stage shares several common previous stages, the transitions types are presented together when editing the stage.

Caution: If a stage has several next stages, only one of the transitions may be automatic and the rest must be set as **Manually, Anytime**. In case of conflict the user will be notified about the automatic change.

How to Define Tasks

You can define a set of manual tasks to be performed as part of a lifecycle stage.

To add a task:

1. Click the **Stages** tab to enter the **Stage Definition** window and click on the stage that you would like to add a task to.
2. Click **Add Task** to open the Add Task dialog box.

Screenshot: Add Task Dialog

3. Enter a name and optional description for the task
4. A Task may be assigned to a Role, a User or a Group by clicking the **Select** next to **Assigned To:** label. Clicking the **Browse Addressbook** button will reveal lists of Roles, Users and Groups that can have assigned tasks.
5. A Task may be verified by policy by clicking the **Select** next to **Verified by Policy** label which will provide a list of existing policies that may be applied.

Note: Only one policy may be associated with a task at a time. Only policies not used within the same stage can be selected (either in tasks or policies).

6. Click **Ok**.

The new task is added to the Tasks field.

How to Define Policies

You can define a set of policies to validate artifact compliance as part of a lifecycle stage.

To add a policy:

1. Click **Stages** to open the **Stage Definition** window and click on the stage that requires a policy.
2. Click **Add Policy** to open the **Add Policy** dialog box.

Screenshot: Add Policy Dialog

	Name	Applicable To
<input type="radio"/>	☆ Administrator Should Not Be Artifact Owner	HP Enterprise Maps resource
<input type="radio"/>	☆ All Application Components Deprecated	HP Enterprise Maps resource
<input type="radio"/>	☆ All Application Components Developed	HP Enterprise Maps resource
<input type="radio"/>	☆ All Application Components in Production	HP Enterprise Maps resource
<input type="radio"/>	☆ All Application Components Retired	HP Enterprise Maps resource
<input type="radio"/>	☆ All Process Implementations Deprecated	HP Enterprise Maps resource
<input type="radio"/>	☆ All Process Implementations Retired	HP Enterprise Maps resource
<input type="radio"/>	☆ All Project Artifacts Developed	HP Enterprise Maps resource
<input type="radio"/>	☆ All Project Artifacts In Production	HP Enterprise Maps resource
<input type="radio"/>	☆ All Service Implementations Deprecated	HP Enterprise Maps resource

You may use either the search function or select a policy from the presented list using the radio button.

Note: Only policies not used within the same stage can be selected (either in tasks or policies).

3. Click **Select**.

The next window allows you to change your choice of policy, the artifact type it is applicable to and whether the policy is required to approve the stage.

4. Click **OK** to apply the policy.

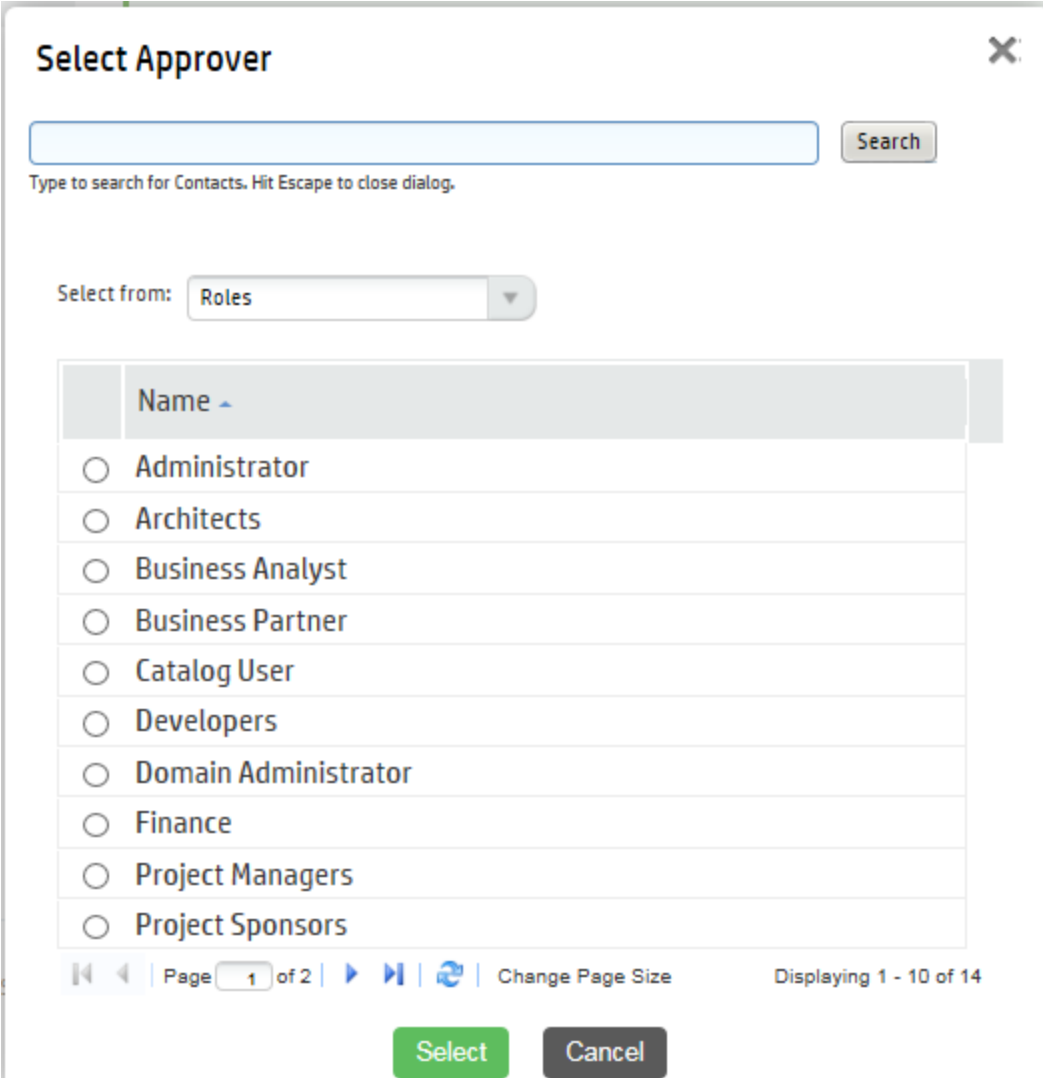
How to Define Approvers

For each lifecycle stage in a lifecycle process you can define a unique set of approvers. The approvers determine whether the artifacts governed by the process are complete for the current stage.

To define voters for approval:

- Click the **Stages** tab on the **Lifecycle Processes** page and then select the stage you require an approval.

Screenshot: Select Approver Dialog



Select Approver ✕

Type to search for Contacts. Hit Escape to close dialog.

Select from:

Name ▾
<input type="radio"/> Administrator
<input type="radio"/> Architects
<input type="radio"/> Business Analyst
<input type="radio"/> Business Partner
<input type="radio"/> Catalog User
<input type="radio"/> Developers
<input type="radio"/> Domain Administrator
<input type="radio"/> Finance
<input type="radio"/> Project Managers
<input type="radio"/> Project Sponsors

Page 1 of 2 | | Displaying 1 - 10 of 14

- To add an individual, group or role of voter(s):
 - a. Click the **Browse Addressbook** button.
 - b. Principals can be found in the lists or can be found by entering a name in the **Search** field and clicking **Search** to show matching search results.
 - c. Click the radio button next to the Role/User/Group required and click **Select** to add selection as an approver.
 - d. If the selected approver is not an individual, but a role or group, select the number of votes required by that role or group.
 - e. The Passive Approval option can now be selected with a specified number of days before

automatic approval.

- f. Click **OK** to add the Approver
- To remove voters, click on the **Delete** button next to their name.
 - To edit the Passive Approval option, click the **Edit** button next to the name of the approver.

Note: Approvers can also be viewed, edited or added under the **Permissions** tab.

How to Define Automatic Actions

To define automatic actions, click on the **Add Automatic Actions** link at the bottom of the stage details window on the stages tab.

Dependent on the artifact type, the following actions may be available:

- **Execute Script** - Invoke a custom javascript code previously defined using administration, customization, and manage scripts. In the Advanced tab, you can define a javascript fragment, which is executed prior to running the referenced script artifact.
- **Parent Request Approval** - Create approval request for parent artifact. Parent Artifact Type and Parent Stage must be selected in the pop-up dialog. Click **OK** to add automatic action. The approval on parent's artifact will be requested automatically.
- **Remove Comments** - Once artifact goes into production, all comments will be removed.
- **Notify** - HP EM Enables you to send e-mail notifications to artifact stakeholders. You can send set up automatic notifications to be sent as a result of lifecycle changes. Notifications require a subject, and may include Lifecycle Status and an attached text.

The possible recipients of the notification are described in the following table:

Notification Recipients

Recipient	Description
Owner	The user, group, or role that owns the artifact. "How to Edit Artifact ownership" in the UG.
Maintainers	Users, groups, and roles groups with write permission for the artifact. For details, see "How to Edit Access Rights in the UG.
Contacts	Users and organizational units associated with the artifact by the contact relationship or listed in the artifact stakeholder property. For details, see "How to Manage Contacts" in the UG. The Contacts recipient group can be refined into selectable contact roles.

Notification Recipients, continued

Recipient	Description
Other Recipients	Click Add Other Recipients and use the user, group, and role search feature to add any other required recipients.
Previous Stakeholders	Expand Show Advanced Options and select Include Recipients from Previous Versions to notify stakeholders from previous versions of the artifact about changes to a newer version. The stakeholders notified by this option match those for the current artifact version. For example, if Consumers is selected, then the consumers of previous versions are notified.

Automatic actions can be deleted by clicking the **Delete** icon and the Notifications and Parent Request Approval actions can be edited by clicking the **Edit** icon.

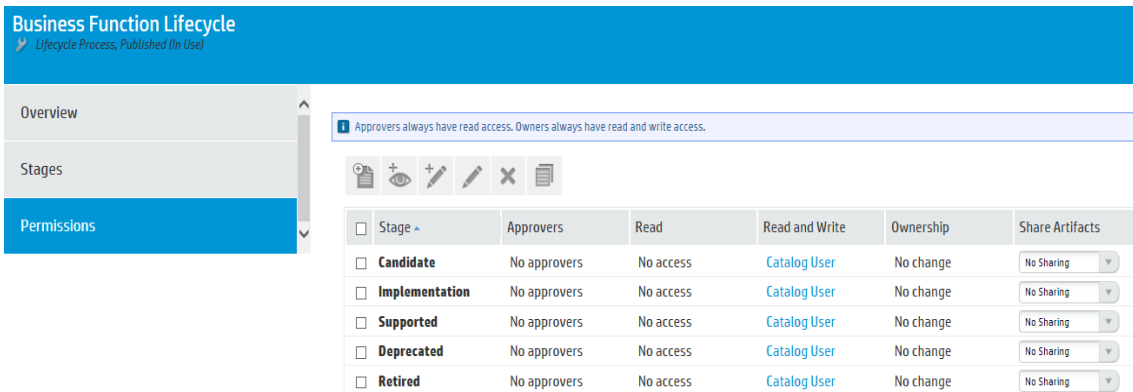
How to Define Permissions

For each lifecycle stage in a lifecycle process you can define a set of permissions. These permissions determine which Role, Group or User has ownership, access rights, approver status and whether artifacts are shared or not.

Note: Permission settings are not carried forward to the next stage.

To set permissions for a stage, select the **Permissions** tab in the **Lifecycle Process** window.

Screenshot: Permissions Matrix



Click the select box for any stage that requires a change in **Permissions** setting.

Add Approver

- Click **Add Approver** to open the Add Approver dialog box

Approvers can be assigned from either the Roles, Users or Groups lists

- Click **Select**

The Approver can be given passive approval with a set date if required

- Click **OK**

Read or Write Access can be assigned to individual Users, Roles or Groups by clicking on the Add Read Access or Add Write Access buttons or the corresponding value in the permissions matrix.

- The owner of the Stage can be assigned by clicking the **Set Owner** button or the **Ownership** value in the matrix.
- Artifacts can be shared by selecting a value from the **Share Artifacts** drop-down list.
- Permissions for a stage can be removed by clicking the **Clear** button
- Defined Stage Permissions can be copied to another stage by clicking the **Copy** button and selecting which stages and/or roles require the copies values.

How to Publish a Process

After creating a lifecycle process, the next step is to make it available for the governance of artifacts.

To publish a lifecycle process:

- From the Lifecycle Processes page, select the processes to be published by clicking on the check box next to the process name and click **Publish**.
- Processes can also be published from the Overview or Stages tab of a selected process.
- Processes can be deprecated by clicking the **Deprecate** button in either the processes page or the Overview or Stages tab of a selected process.

This lifecycle process is now available to be used in the governance of root and sub-artifacts.

How to Export Lifecycle Processes

Any Lifecycle Process can be exported from either the Overview or Stages tab.

1. Click **Export** from the right menu.
2. Provide a name for the exported file and click **Export** in the dialog window.
3. Either open or provide a location for the exported file.

Lifecycle Best Practice

The following list enumerates the lifecycle basic best practice:

- Govern all artifacts.

HP recommends governing artifacts whenever possible. We are aware that in some situations (such as for system artifacts) there may be additional overhead, but the benefits gained are worth it. For example, versioning works properly only for governed artifacts.

- Assign lifecycle processes automatically.

HP recommends marking lifecycle processes as automatically assignable. In our opinion, common users should not select a lifecycle process for their artifact(s). Instead, the Administrator should create an appropriate lifecycle process that is assigned to the artifact automatically after artifact creation.

Action Set Lifecycle Process / Stage provides users with the possibility to set any process to the artifact. Administrators can even set a specific stage and mark it as approved. This action is intended mainly for administrators who import data to the repository. If the data is suitable, Administrators can use this action to set for example, Production stage.

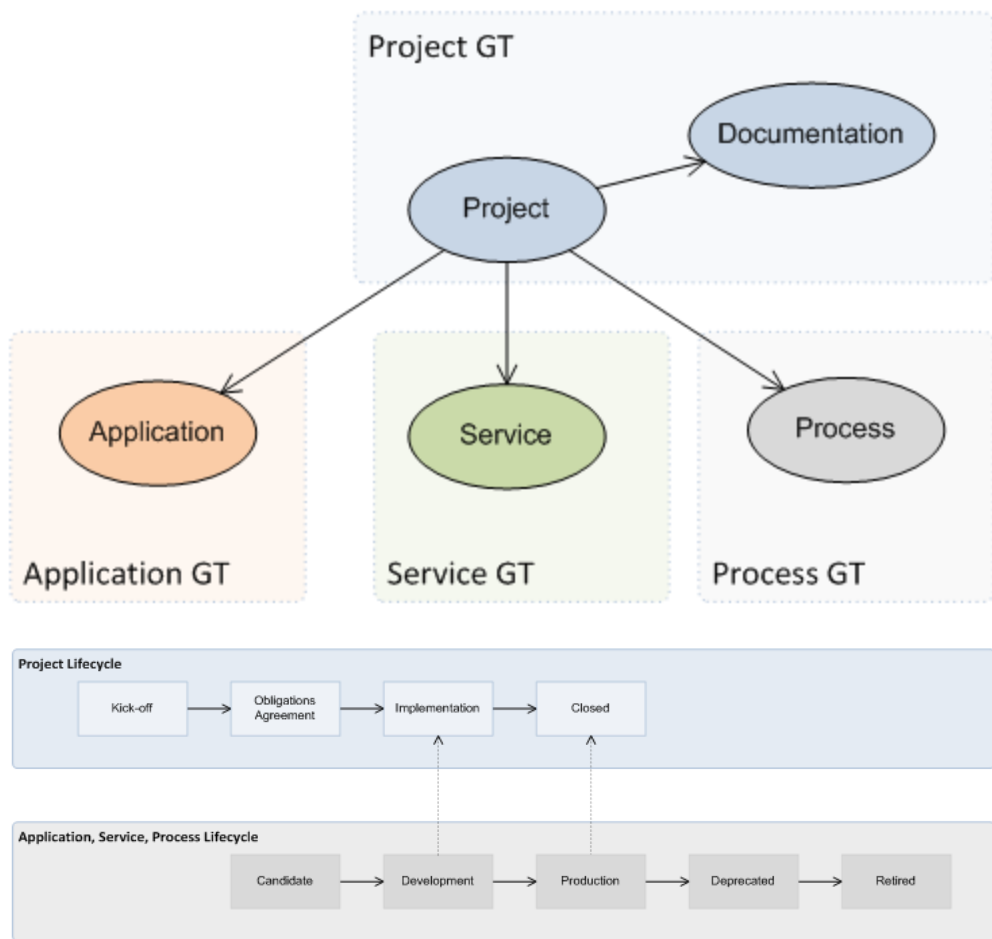
- Separate lifecycle processes.

HP recommends separating lifecycle processes and defining different lifecycle process for different artifact types. These processes can be connected together via policies but it is crucial to not govern all artifacts in one process.

As an example, you can review the default lifecycle processes include in this topic. There is a special lifecycle process for Project artifacts containing only Project artifacts and their documents. And similarly there are separated lifecycle processes for Applications, Services, and Processes.

As mentioned, processes are separated but they can be tied together. For example it is possible to define the following rules.

- A Project can be approved at the Implementation stage only if all project artifacts (Applications, Services or Processes) are approved at the Development stage. Similarly, a Project can be approved at the Closed stage only if all underlying artifacts (such as applications, services and processes) are approved at the Production stage.

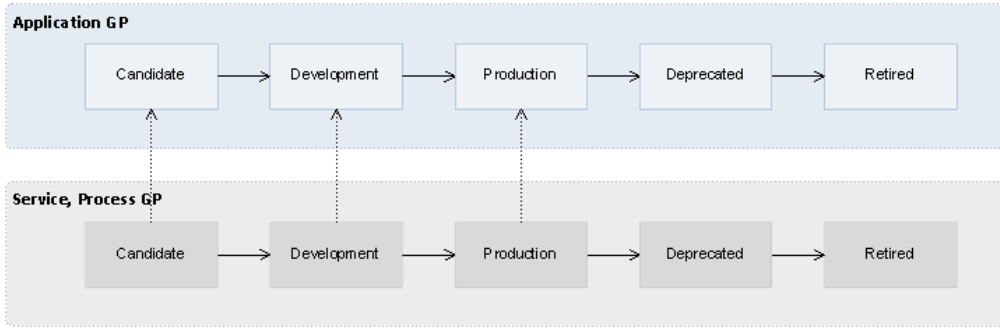


Application Lifecycle

Applications represent business functionality in the real world. Applications can consist of multiple components (services and business processes) but these do not form part of the application lifecycle tree.

Application Lifecycle Tree:

- Application
 - Documentation
 - SLO



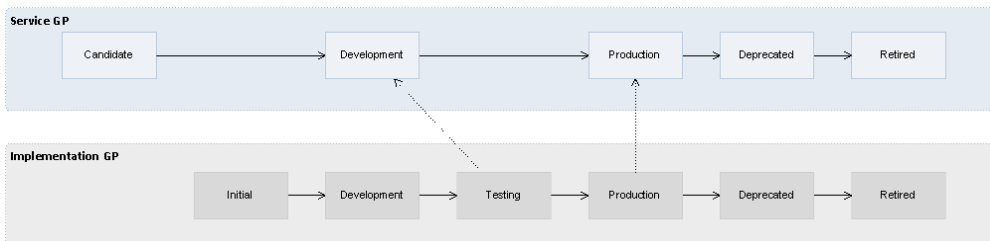
The Application Lifecycle Process depends on the lifecycle processes of its component artifacts. For example, the Production stage of an application cannot be approved until all its component artifacts are approved in the Production stage.

Service Lifecycle

Services represent business functionality (or concepts) in the real world. Services consist of sub-services and implementations but these do not form part of the lifecycle tree.

Service Lifecycle Tree:

- Service
 - Documentation
 - SLO



The Service Lifecycle Process depends on the lifecycle processes of its constituent artifacts. For example, the Development stage of a service cannot be approved until all its sub-services are approved in the Development stage and at least one of its implementations is approved in the Testing stage.

Service Implementation Lifecycle

In the real world an implementation represents a specific service version being implemented, in the repository it represents a package with the service executables which can be later deployed to multiple environments.

Service Lifecycle Tree:

- Implementation
 - Operation
 - Endpoint
 - Interface (WSDL)
 - Schema (XSD)
 - Documentation
 - SLO

Each implementation represents one service and the Service Lifecycle Process depends on the Implementation Lifecycle Process. For details, see ["Service Lifecycle" on the previous page](#)

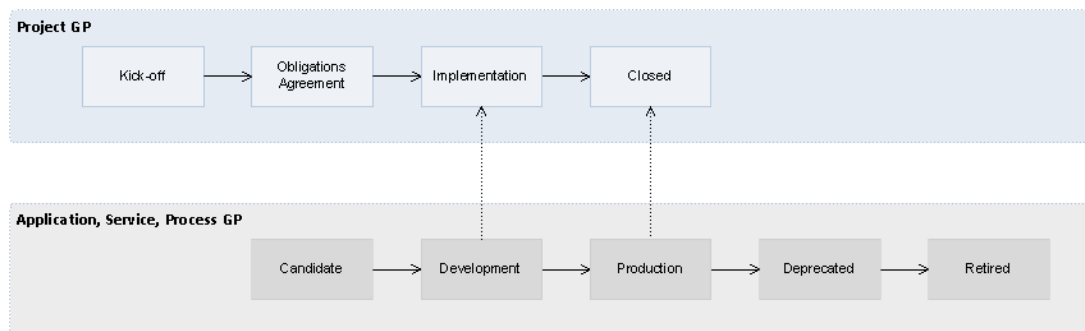
Project Lifecycle

Projects represent any progressive activity (such as service development). Projects can be composed of services, applications, business processes, and other artifacts. In this release, the goal of a project is to successfully deploy its constituent artifacts to a production environment.

Project Lifecycle Tree:

- Project
 - Documentation

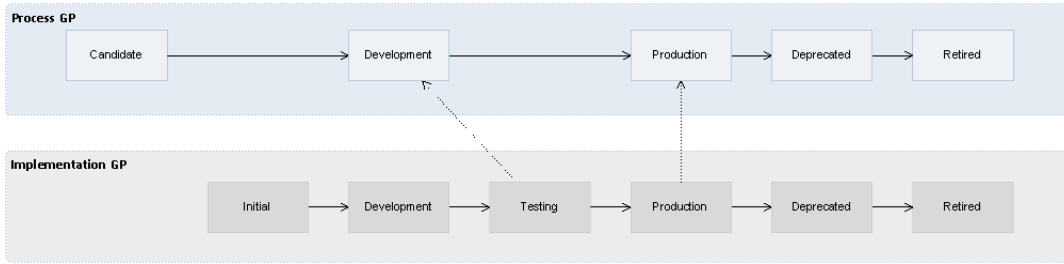
Promotion is automatic after the approval of each stage as per the following image:



The Project Lifecycle Process depends on the lifecycle processes of its constituent artifacts (applications, services, and business processes). For example, the Closed stage of a project cannot be approved until all its constituent artifacts are approved in the Production stage.

Process Lifecycle

The Process lifecycle is similar to the Service Lifecycle. Some of the tasks and policies vary, but the stages and dependency on the process implementation lifecycle is the same as that between a service and its implementation.



Process Implementation Lifecycle

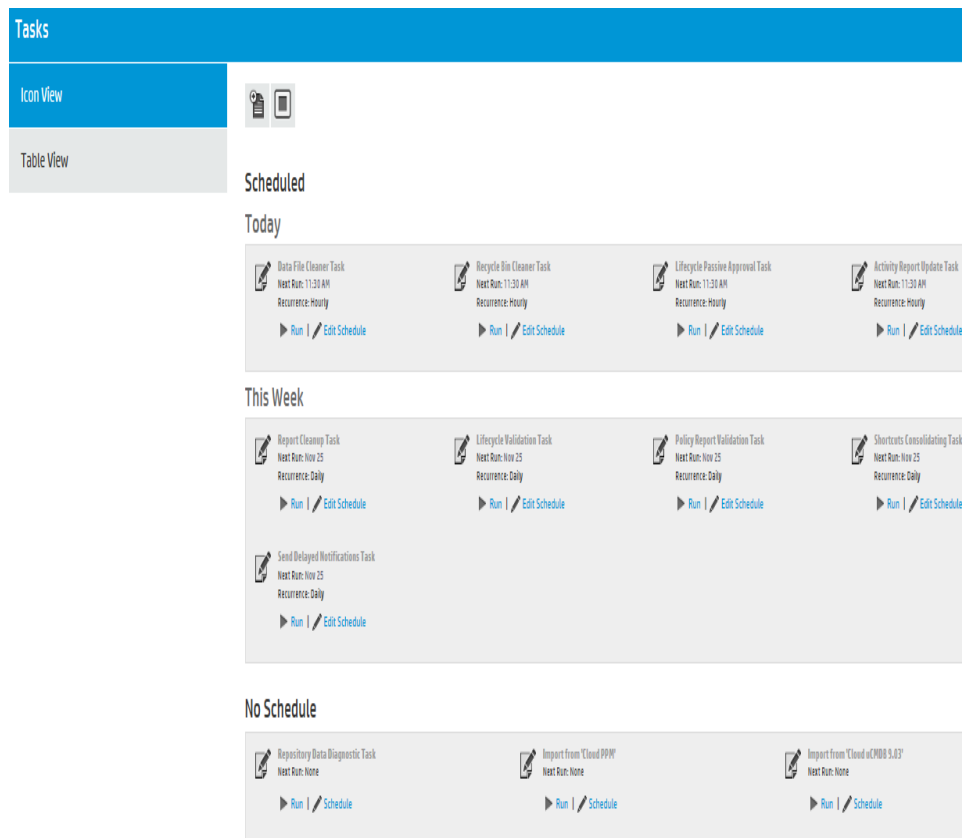
The lifecycle process for business process implementations is similar to that for service implementations. Some tasks and policies vary, but the stages and relationships to the process lifecycle are the same.

Chapter 7: Administration Task Management

HP EM includes a number of default administration tasks to help administrators to manage their deployment and the data it contains. In addition, the administrator can configure additional tasks to perform change management or custom tasks included in an extension.

Access Task Management from the Administration tab. In the Administration menu, click **Tasks** to open the Tasks page.

Screenshot: Tasks Page



The initial view of the Administrator Task page provides a simplified grid interface for dealing with the administration of Daily, Weekly, and unscheduled tasks. Any running tasks will also be visible with a options to either stop them independently or to stop all running tasks.

HP EM provides the following default administration tasks:

- **Activity Report Update**

Updates the artifact activity data used to generate the Activity Report shown in the Reports tab Home page.

- **Lifecycle Passive Approval**

Approves Lifecycle stages that have been set to automatic approval after a set number of days.

- **Lifecycle Validation**

Performs a validation of all artifacts in governance against the policies that apply to their current lifecycle stage.

- **Policy Report Validation**

Performs an update of any policy reports.

- **Recycle Bin Cleaner**

Permanently removes deleted artifacts from the recycle bin as the defined schedule.

- **Report Cleanup**

Removes old reports and events based on their age against properties set in the Configuration page Report Cleanup tab. For details, see "[Configuration Management](#)" on page 56.

- **Data File Cleaner**

Removes deleted artifacts in recycle bin based on their age against property `platform.recycleBin.timeout` set in the Configuration page System Properties tab. For details, see "[System Configuration Properties](#)" on page 61.

- **Shortcuts Consolidating**

Consolidates all shortcut instances available in the server.

- **Send Delayed Notifications**

Sends all expired delayed notifications.

The administrator can execute tasks immediately or schedule them to run on a periodic basis. For details, see "[How to Run Tasks](#)" below and "[How to Schedule Tasks](#)" on the next page.

In addition to the default tasks, the administrator can add change management tasks and custom tasks. For details, see "[How to Add Change Management Tasks](#)" on page 54 and "[How to Add Custom Tasks](#)" on page 54.

How to Run Tasks

You may want to immediately execute a task. If you have sufficient permissions, there is a **Run** option in the initial Tasks overview as well as in the detail view of the task.

To Manually Execute Tasks:

- Click **Run** in either the Task overview or in the Task detail page.

How to Schedule Tasks

HP EM enables you to execute tasks on a timed or periodic basis.

Caution: HP EM converts and stores any input time to GMT. If you import scheduled tasks from a data image, review the scheduling to ensure that the tasks execute at the local time that you require.

To Schedule Tasks:

1. Do the following:
 - In the task window or detail view of the task click **Edit Schedule** to open the Edit Schedule dialog.

Screenshot: Edit Schedule Dialog

- Select a start date and start time for the task
- Set the frequency that the task will run
- Either set the task to run Indefinitely, set a finish date and time or enter a value representing the number of times the task should run
- Advanced Options allow you to select whether the schedule should be followed during downtime or to wait until HP EM start running.
- Click **OK** to set the schedule for the task

How to Add Change Management Tasks

Sync Tasks enable the administrator to synchronize artifacts in the repository with those imported from an external source

To Create Sync Tasks:

1. Click **Add Data Synchronization Task** to open the dialog.
2. Add a name and optional description for the task.
3. Artifacts can be selected through using either standard search methods or they can be selected from a filtered list.

Click **Save** .

4. Clicking **Edit Schedule** will allow you to set a schedule for the running of the new task or the task can be run immediately by clicking **Run**.
5. The task may be edited by clicking on **Edit**.

How to Add Custom Tasks

If HP EM includes an extension which contains custom task implementations, you can add and schedule them in the Tasks page.

To Create Custom Tasks:

1. Click **Add Javascript Task** to open the dialog.
2. Select a Task Implementation and add a name for the task.

Task parameters and variables are defined according to how the task component was composed.

3. Click **Save** .
4. Clicking **Edit Schedule** will allow you to set a schedule for the running of the new task or the task can be run immediately by clicking **Run**.
5. The task may be edited by clicking on **Edit**.

Chapter 8: Product Integration Management

To enable product integration in Enterprise Maps, the administrator must create server artifacts representing the integrated servers and perform some configuration tasks.

Access server management from the Administration tab Administration menu. Click Configuration to open the Integration tab in the current domain.

Note: There can only be one instance of BSM / UCMDB and they are associated with the top-level domain, regardless of the domain you are using when you create the server.

Configure HP EM to access integration server via HTTPS

In order for the HP EM server to connect with the integration server (BSM/UCMDB, PPM, etc.) via HTTPS protocol, you need to import the certificate of that server into HP EM truststore.

To import the certificate of integration server into HP EM:

1. Access the integration server URL (HTTPS protocol) via web browser. The web browser asks for import of the server certificate.
2. Export the certificate from the web browser (for example: export the certificate into bsm.cert).
3. Run the following command:

```
keytool -import -alias myBSMServer -file bsm.cert -keystore EM_  
HOME/conf/client.truststore
```

4. Restart EM server.
5. Login to EM as administrator and create an integration server using HTTPS protocol.

Chapter 9: Configuration Management

HP EM provides a customizable configuration that enables the administrator to control nearly every aspect of the behavior of HP EM.

The Administrator can modify most parts of the configuration of HP EM from the Administration tab.

In the Administration menu, select **Configuration** > **Setting** to open the Configuration page.

The Configuration page is split into the following tabs:

- **Basic Settings**

Settings that affect the operation of HP EM repository. For more details, see ["How to Manage Basic Configuration Options" on the next page](#).

- **System Properties**

The detail level settings of the configuration. The administrator can use this tab to modify individual settings at a global, or domain level. This tab also enables the export and import of the configuration as a whole. For details, see ["How to Manage System Settings" on page 59](#).

- **License**

A summary page detailing the terms of the current license with an option to enter a new license key and manage licensed users. For more details, see "License Management" in the *Installation and Deployment Guide*.

- **Self-Test**

Details the status of HP EM with an option to disable self-test. For more details, see ["Configure EM to access integration server via HTTPS" on page 58](#).

- **Report Cleanup**

Set the maximum age of reports and events to be retained when the Report Cleaner Task executes. You can set a different age by report and event type. You can also use the following system properties to filter the processing of the Report Cleaner Task:

- `platform.reportCleanerDao.batchNum` - Sets the number of reports to be cleaned in a database transaction. The default value is 20.
- `platform.reportCleanerDao.interval` - Sets the interval (in millisecond) that the Report Cleaner Task will sleep after a database transaction is committed. The default value is 10000.

Manage the execution and scheduling of the Report Cleaner Task using the Tasks page. For details, see ["Administration Task Management" on page 51](#).

How to Manage Basic Configuration Options

HP EM enables the administrator to control some basic aspects of the configuration from the Administration tab.

To Configure Basic Settings:

1. In the Administration menu, select **Configuration > Setting** to open the Configuration page in the Basic Settings tab.
2. In the Basic Settings tab, set any of the following options:

■ Full Text Search

Select this option to enable full text search in the HP EM UI.

Note: Full-text search must also be enabled on the database as described in the following sections of the *Installation and Deployment Guide* under *Deploying HP EM*:

- Enable Full-Text Search in MSSQL
- Enable Full-Text Search in Oracle

By default, HP EM appends a % to search terms. To disable this functionality after installation, set the configuration property `shared.db.fulltextsearch.appendpercentage` to `FALSE`. For details, see ["How to Manage System Settings" on page 59](#).

■ Create Empty Data Artifacts

Data artifacts are normally associated with data content, such as a WSDL or document, uploaded from an external source.

By default, HP EM does not offer the option to directly create new data artifacts (for example, documentation or WSDLs) and only creates artifacts of these types when data content is uploaded. For example, a documentation artifact can only be created by uploading a document.

Set the **Create Empty Data Artifacts** option if you want to enable the creation of new data artifacts without requiring the upload of associated data content.

■ SSL Customization

Select the authentication method to apply to SSL certificates.

Certificate Trust and Customization Categories

Certificate Trust	Customization
Java/JSSE default key/trust stores...	default

Certificate Trust and Customization Categories, continued

Certificate Trust	Customization
Server certificates are always trusted...	skipped
Database key/trust stores...	database
Composition of database and default...	composite

3. Click **Save** to make your changes or **Reset to Defaults** to restore these settings to their defaults.

Configure EM to access integration server via HTTPS

In order for the HP EM server to connect with the integration server (BSM/UCMDB, PPM, etc.) via HTTPS protocol, you will need to import the certificate of that server into HP EM truststore.

To import the certificate of integration server into HP EM:

1. Access the URL (HTTPS protocol) of integration server via web browser. The web browser will ask you to import that server certificate.
2. Export the certificate from the web browser (for example, export the certificate into bsm.cert).
3. Run the following command:

```
keytool -import -alias myBSMServer -file bsm.cert -keystore EM_
HOME/conf/client.truststore
```

4. Restart EM server.
5. Login to EM as administrator and create an integration server using HTTPS protocol.

How to Manage the System Configuration

HP EM stores system settings in a configuration file in the installation folder. The Administrator can view and edit these settings directly in the Administration tab.

In the Administration menu, click **Configuration > Setting** to open the Configuration page, and select the **System Properties** tab to view the current system configuration.

The Configuration page System Settings tab provides functionality described in the following topics:

- ["How to Manage System Settings" on the next page](#)
- ["How to Export and Import System Settings" on page 60](#)
- ["System Configuration Properties" on page 61](#) provides a reference to configuration properties available in the System Settings tab.

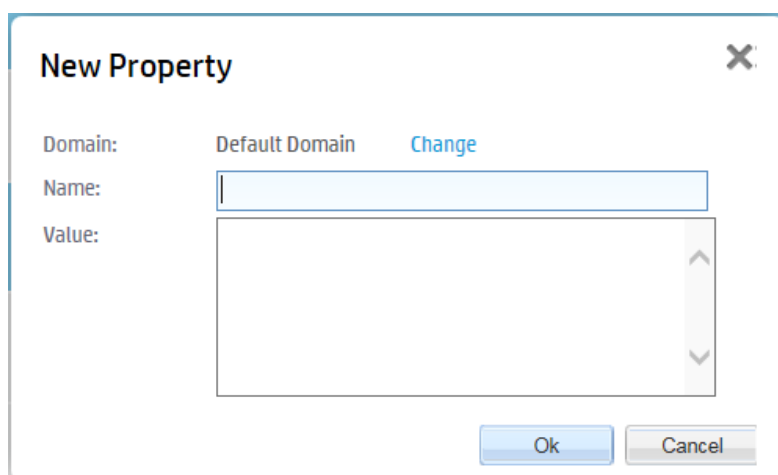
How to Manage System Settings

In the Configuration page System Settings tab, the administrator can add, edit, and remove system properties.

System properties can apply globally, or within a specific domain. If a domain setting exists, it takes precedence over a global setting.

To Add System Properties:

1. In the Configuration page System Settings tab, click **New Property** to open the New Property dialog box.
2. *Optional:* Click **Change** to alter the domain that the setting applies to.



The screenshot shows a dialog box titled "New Property" with a close button (X) in the top right corner. On the left side, there are three labels: "Domain:", "Name:", and "Value:". The "Domain:" label is followed by a dropdown menu currently showing "Default Domain" and a blue "Change" link. The "Name:" label is followed by a single-line text input field. The "Value:" label is followed by a multi-line text area with a vertical scrollbar on the right side. At the bottom of the dialog, there are two buttons: "Ok" and "Cancel".

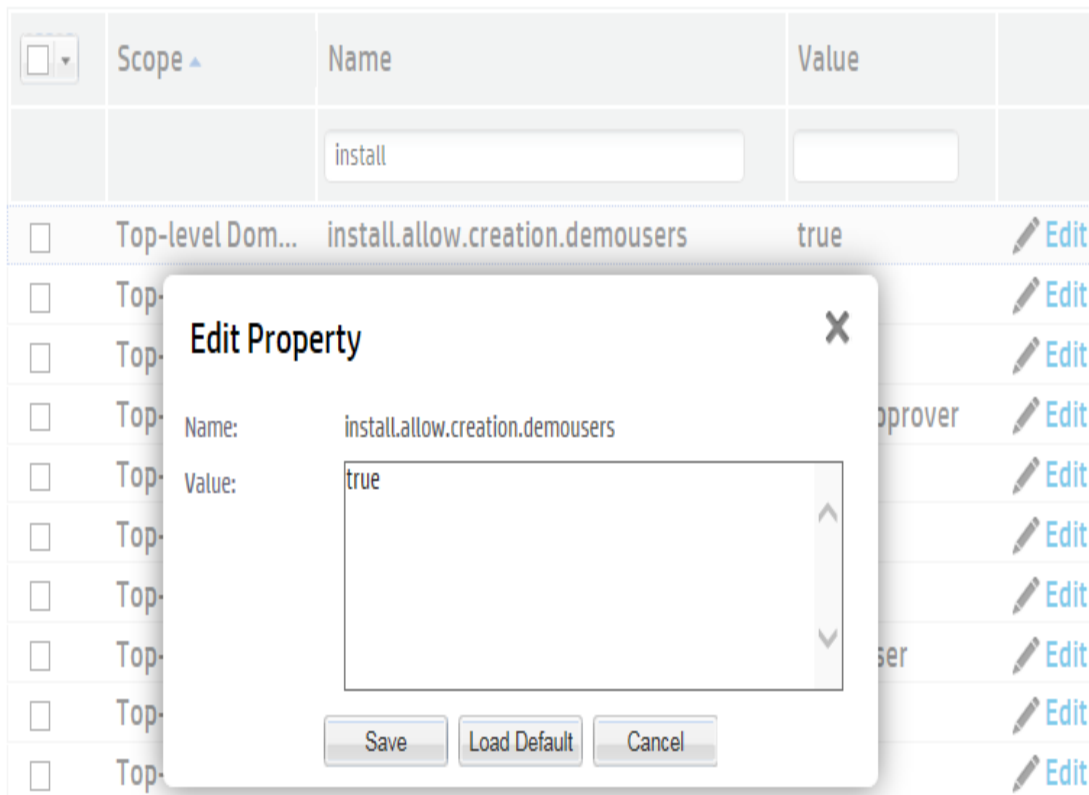
3. Set a name and value for the property, and click **OK** to add the property to the system settings for the selected domain.

To Add System Properties from a File:

1. In the System Settings tab, click **Add File Property** to open the Add File Property dialog box.
2. *Optional:* Click **Change** to alter the domain that the setting applies to.
3. Set a name for the property, browse for the file on your local filesystem, and click **OK** to add the property to the system settings for the selected domain.

To Edit System Settings:

1. In the System Settings tab, use the Name filter to locate the setting you want to edit.
2. Click **Edit** for the setting to open the Edit Property dialog box.



3. Do one of the following:

- Input a new value and click **Save** to set a new value.
- Click **Load Default Value** to reset the value to its default installation value.

To Delete System Settings:

1. In the System Settings tab, select the properties you want to delete.
2. Click **Remove** and confirm your decision.

How to Export and Import System Settings

The administrator can export system settings to a ZIP file to preserve a particular configuration. Import enables a stored configuration to overwrite the current settings.

To Export System Settings:

1. In the Configuration page System Settings tab, select the properties to export, click **Export**, and confirm your decision.
2. Click **Save** and select a file location for the ZIP file.

To Import System Settings:

1. In the System Settings tab, click **Import** to open the Import dialog box.
2. Input or Browse for the file, and click **OK**.

System Configuration Properties

This reference topic divides the configuration properties by module and specified their type into the following scenarios:

- **SC-I:** Runtime configurable properties that apply immediately.
- **SC-II:** Runtime configurable properties with additional steps required. After the change, the administrator should make some additional changes outside the application, for example, change the application server configuration.
- **SC-III:** Runtime configurable properties which require a restart of the application server.
- **SC-IV:** These properties can only be changed using the Setup Tool.

Usage Statistics

Property Name	Description	Value Type	Default	Scenario
platform.usage.stats.excluded.artifact.types	List of artifact types which are excluded from Activity Report (usage stats) computation.	Comma-separated list of artifact types.	<i>reportArtifact,taskArtifact</i>	SC-I

Security

Property Name	Description	Value Type	Default	Scenario
shared.siteminder.enabled	Turns on Siteminder (HTTP Header) authentication.	Boolean value	<i>false</i>	SC-IV
shared.siteminder.useCookie	Sets whether use cookie to pass the login name.	Boolean value	<i>false</i>	SC-I
shared.siteminder.useHeader	Sets whether use HTTP Header to pass the login name.	Boolean value	<i>true</i>	SC-I
shared.siteminder.loginNameField	Sets name of login name header/cookie.	Text value	<i>sm-userdn</i>	SC-I

Security, continued

Property Name	Description	Value Type	Default	Scenario
shared.siteminder.importGroups	Sets whether import also groups to security context.	Boolean value	<i>false.</i>	SC-I
shared.siteminder.groupsHeaderName	Name of groups header or cookies used in case useCookies equal to true.	Text value	<i>sm-role</i>	SC-I
shared.siteminder.groupsHeaderDelimiter	Delimiter for found groups.	Text value	^	SC-I
shared.siteminder.requireAuthentication	Require authentication by siteminder, it fails when no user is received from siteminder.	Boolean value	<i>false.</i>	SC-I
shared.dql.security.allowNoAcl	Determines whether ACL settings are used for DQL queries.	TRUE or FALSE	FALSE	SC-III
shared.dql.security.allowNative	Determines whether NATIVE clauses are allowed in DQL queries.	TRUE or FALSE	FALSE	SC-III

Versioning

Property Name	Description	Value Type	Default	Scenario
platform.versioning.schema.initial	Initial schema version.	Text value	<i>1.0</i>	SC-I

HTTP Client

Property Name	Description	Value Type	Default	Scenario
shared.http.connections.per.host	Max count of connections per host.	Integer value.	<i>30</i>	SC-I

HTTP Client, continued

Property Name	Description	Value Type	Default	Scenario
shared.http.total.connections	Max count of available connections by HTTPClient.	Integer value.	100	SC-I
shared.http.user.agent.identification	Identification of user agent header. Sets user agent header field for all calls which do not specify another one.	Text value.	HTTPClient/?.?	SC-I
shared.http.client.proxy.enabled	Sets whether proxy is enabled.	Boolean value.	false.	SC-I
shared.http.client.proxy.nonproxyhosts	Sets all non proxy hosts.	Text value.	Not used. (localhost,127.0.0.1)	SC-I
shared.http.client.proxy.host	Proxy host.	Text value.	Not used. (proxyhost)	SC-I
shared.http.client.proxy.port	Proxy port.	Text value.	8080 - Not used.	SC-I
shared.http.client.proxy.user	If is proxy secured, user name of proxy user.	Text value.	Not used.	SC-I
shared.http.client.proxy.password	If is proxy secured, password of proxy user.	Text value.	Not used.	SC-I

Publishing

Property Name	Description	Value Type	Default	Scenario
platform.publishing.limit.concurrent.uploads.user	Maximum count of concurrent uploads by a single user.	Integer value.	3	SC-I
platform.publishing.limit.concurrent.uploads.total	Maximum count of concurrent uploads by all users.	Integer value.	6	SC-I
platform.publishing.limit.max.archive.files	Maximum number of files in an archive file for publishing.	Integer value.	10000	SC-I
platform.publishing.limit.max.archive.bytes	Maximum size of an archive file for publishing.	Integer value.	10000000	SC-I
platform.publishing.memory.limit.single	Max possible amount memory used by single consumer.	Integer value.	65536	SC-I
platform.publishing.memory.limit.all	Max possible amount of usable memory.	Integer value.	2097152	SC-I

Publishing, continued

Property Name	Description	Value Type	Default	Scenario
shared.http.urlbase	URL base of repository.	URL.	Inserted in installation process.	SC-IV
platform.publishing.duplicates.limit	Max count of duplicities returned by duplicate finder in publisher.	Integer value.	5	SC-I
platform.publishing.http.connection.manager.timeout	HTTP connection manager timeout.	Integer value.	3000	SC-I
platform.publishing.http.socket.timeout	Socket timeout.	Integer value.	3000	SC-I
shared.http.urlbase	Unsecured URL base of repository.	URL.	Inserted in installation process.	SC-IV
shared.https.urlbase	Secured (SSL) URL base of repository.	URL.	Inserted in installation process.	SC-IV

Publishing, continued

Property Name	Description	Value Type	Default	Scenario
platform.publishing.ui.zipArchiveExtensions	A list of archive types that HP EM extracts during publishing.	Comma-separated list of archive extension types that must conform to the ZIP format.	<i>zip,jar,ear,war,bpr</i>	SC-I
platform.publishing.ui.enforcedCollections	By default, if publishing fails for a data resource, HP EM publishes it as documentation. Use this property to prevent this default functionality for specified artifact types.	List of collections to enforce during publishing.	<i>documentation</i>	SC-I

Publishing, continued

Property Name	Description	Value Type	Default	Scenario
platform.ui.upload.allowed.extensions.enable	Set whether to enable upload prevention for malicious files.	Boolean value	False	SC-I
platform.ui.upload.allowed.extensions	List of extensions allowed for upload.	Comma-separated list of allowed extensions	txt,html,htm,xml,csv,doc,docx,odt,ppt,pps,pptx,odp,xslx,xsl,ods,odg,odf,odb,pdf,svg,jpg,jpeg,png,gif,ico,xslt,dtd,xsd,wSDL,xpdl,bpel,composite,sca,zip,jar,rar,tar,gzip,gz.	SC-I
platform.publishing.limit.max.file.bytes	Maximum size of a file for import (such as wdsi, docx, xslx.) Limit to 2000000 bytes.	Integer value.	2000000 bytes	SC-I
platform.publishing.limit.max.archive.bytes	Maximum size of an archive file for publishing. Limit to 10000000 bytes.	Integer value.	10000000 bytes	SC-I

WSDL Publishing

Property Name	Description	Value Type	Default	Scenario
platform.publishing.ui.defaultDecomposition	Default decomposition setting on Upload Data Content. 0 - None (Only WSDL), 1 - Implementations (WSDL and related, SOAP S.+Enpoint+Opreations), 2 - As 1 + Business S.	Integer value.	2	SC-I
platform.publishing.ui.defaultServiceType	Means default service type. One of [businessService, applicationService, infrastructureService]	One of service type.	<i>businessService</i>	SC-I

Contract Management

Property Name	Description	Value Type	Default	Scenario
platform.cm.consumers	Artifact types defined as contract consumers.	Comma-separated list of artifact localnames.	See "Default Provider / Consumer Artifact Types" in the <i>User Guide</i>	SC-I
platform.cm.providers	Artifact types defined as contract providers.	Comma-separated list of artifact localnames.	See "Default Provider / Consumer Artifact Types" in the <i>User Guide</i>	SC-I
platform.cm.consumers.of.provider	Artifact types defined as contract consumers for the specified provider artifact type.	Comma-separated list of artifact localnames.	None	SC-I
platform.cm.providers.of.consumer	Artifact types defined as contract providers for the specified consumer artifact type.	Comma-separated list of artifact localnames.	None	SC-I

Lifecycle

Property Name	Description	Value Type	Default	Scenario
platform.lifecycle.notify.approvers	Sets whether the approvers are automatically notified by e-mail containing approval request.	Boolean value.	<i>true</i>	SC-I
platform.lifecycle.notify	Turns off lifecycle notifications when set to false.	Boolean value.	<i>true</i>	SC-I

Artifact Icons

Property Name	Description	Value Type	Default	Scenario
platform.integration.discovery.bac.mappingConfiguration9	Maps artifacts between Enterprise Maps and HP Business Service Management 9.x.	XML file which contains mapping from Enterprise Maps artifacts to BSM entities.	XML file mapping from Enterprise Maps artifacts (SOAP Service, Business Service, Organization Unit) to BSM entities (webservice, business_service, organization).	SC-III
shared.ui.artifact-icons.	Prefix of artifact icons configuration.	Prefix of artifact icons configuration.	Without default value.	SC-I

User Management

Property Name	Description	Value Type	Default	Scenario
---------------	-------------	------------	---------	----------

User Management, continued

shared.um.scenarios.type	Type of scenario for communication with LDAP server.	One of single.ldap.[single or multiple].searchbase, , multiple.ldap.[single or multiple].searchbase values.	<i>single.ldap.single.searchbase</i>	SC-I
shared.um.account.caseInsensitiveLoginName	Sets whether login may be name case insensitive.	Boolean value	<i>true</i>	SC-I
shared.um.account.backend.type	Type of group backend.	Text value. One of [ldap, database, external]	Inserted in installation process.	SC-IV
shared.um.account.backend.className	Group backend class name.	Text representation of whole class name.	Inserted in installation process.	SC-IV
shared.um.account.backend.enablemoreBackends	By group backend allows more backends.	Boolean value.	<i>true</i>	SC-IV
shared.um.group.backend.type	Type of account backend.	Text value. One of [ldap, database, external]	Inserted in installation process.	SC-IV
shared.um.group.backend.className	Account backend class name.	Text representation of whole class name.	Inserted in installation process.	SC-IV
shared.um.group.backend.enableMoreBackends	By account backend allows more backends.	Boolean value.	<i>true</i>	SC-IV

User Management, continued

shared.um.account.domain.enabled.name	Name of enabled domain.	Text representation name of enabled domain.	Not set.	SC-I
shared.um.account.domain.enabled.dn	Distinguished Name of enabled domain.	Text representation DN of enabled domain.	Not set.	SC-I
shared.um.account.domain.disabled.name	Name of disabled domain.	Text representation name of disabled domain.	Not set.	SC-I
shared.um.account.domain.disabled.dn	Distinguished Name of disabled domain.	Text representation DN of disabled domain.	Not set.	SC-I
shared.um.group.ldapName	LDAP property name for group name.	Text value.	Inserted in installation process. (<i>cn</i>)	SC-II
shared.um.group.ldapOwner	LDAP property name for group owner.	Text value.	Inserted in installation process. (<i>owner</i>)	SC-II
shared.um.group.ldapMember	LDAP property name for group member.	Text value.	Inserted in installation process. (<i>uniqueMember</i>)	SC-II
shared.um.group.ldapDescription	LDAP property name for group description.	Text value.	Inserted in installation process. (<i>description</i>)	SC-II
shared.um.account.ldapLoginName	LDAP property name for login name.	Text value.	Inserted in installation process. (<i>uid</i>)	SC-II

User Management, continued

shared.um.account.ldapFullName	LDAP property name for full name.	Text value.	Inserted in installation process. (<i>cn</i>)	SC-II
shared.um.account.ldapEmail	LDAP property name for email.	Text value.	Inserted in installation process. (<i>mail</i>)	SC-II
shared.um.account.ldapDescription	LDAP property name for account description.	Text value.	Inserted in installation process. (<i>description</i>)	SC-II
shared.um.account.ldapLanguageCode	LDAP property name for language code.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapBusinessName	LDAP property name for business name.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapPhone	LDAP property name for phone.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapAlternatePhone	LDAP property name for alternate phone.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapAddress	LDAP property name for address.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapCity	LDAP property name for city.	Text value.	Inserted in installation process.	SC-II

User Management, continued

shared.um.account.ldapCountry	LDAP property name for country.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapBlocked	LDAP property name for index of blocking.	Text value.	Inserted in installation process.	SC-II
shared.um.account.ldapZip	LDAP property name for zip code.	Text value.	Inserted in installation process.	SC-II
shared.um.uddi.ldap.searchfilter.group	LDAP search filter for group.	Text value.	Inserted in installation process. (<i>objectClass=groupofuniqueNames</i>)	SC-IV
shared.um.uddi.ldap.searchbase.group	LDAP search base for group.	Text value.	Inserted in installation process. (<i>ou=groups,ou=big,dc=example,dc=com</i>)	SC-IV
shared.um.uddi.ldap.searchscope.group	These property sets search scope for users and group entries within an LDAP : 0 = object scope (useless in this case), 1 = one level (flat) scope, 2 = subtree scope.	Integer value.	Inserted in installation process. (2)	SC-IV
shared.um.uddi.ldap.searchMaxResults.group	LDAP search max results for user.	Integer value.	Inserted in installation process. (10000)	SC-IV

User Management, continued

shared.um.uddi.ldap.searchfilter.user	LDAP search filter for user.	Text value.	Inserted in installation process. (<i>objectClass=person</i>)	SC-IV
shared.um.uddi.ldap.searchbase.user	LDAP search base for user.	Text value.	Inserted in installation process. (<i>ou=people,ou=big,dc=example,dc=com</i>)	SC-IV
shared.um.uddi.ldap.searchscope.user	These property sets search scope for users and group entries within an LDAP : 0 = object scope (useless in this case), 1 = one level (flat) scope, 2 = subtree scope.	Integer value.	Inserted in installation process. (2)	SC-IV
shared.um.uddi.ldap.searchMaxResults.user	LDAP search max results for user.	Integer value.	Inserted in installation process. (10000)	SC-IV
shared.um.uddi.ldap.allowBlankPassword	LDAP sign for allowing blank password.	Boolean value.	Inserted in installation process. (<i>false</i>)	SC-IV
shared.um.java.naming.provider.url	LDAP url.	URL.	Inserted in installation process. (<i>ldap://ldap.example.com:389</i>)	SC-IV
shared.um.java.naming.factory.initial	LDAP factory.	Full LDAP factory class name.	Inserted in installation process. (<i>com.sun.jndi.ldap.LdapCtxFactory</i>)	SC-IV

User Management, continued

shared.um.java.naming.security.principal	LDAP principal.	Text value.	Inserted in installation process.	SC-IV
shared.um.java.naming.security.credentials	LDAP credentials.	Text value.	Inserted in installation process.	SC-IV
shared.um.java.naming.security.authentication	LDAP authentication type. [none, simple, sasl_mech] where sasl_mech is a space-separated list of SASL mechanism names.	Text value.	Inserted in installation process.	SC-IV
shared.um.ldap.connect.timeout	Timeout for connection to LDAP.	Integer value.	0	SC-I
shared.um.ldap.connect.pool	Enabling connection pooling.	Boolean value.	false	SC-I
shared.um.ldap.connect.pool.authentication	Connection pooling authentication value.	Text value.	Not used.	SC-I
shared.um.ldap.connect.pool.debug	Connection pooling debug switch.	Boolean value.	Not used. (false)	SC-I
shared.um.ldap.connect.pool.initsize	Connection pooling initial size.	Integer value.	Not used. (1)	SC-I
shared.um.ldap.connect.pool.maxsize	Connection pooling max size.	Integer value.	Not used. (no max size)	SC-I

User Management, continued

shared.um.ldap.connection.protocol	Connection pooling protocol.	Text value.	Not used. (<i>plain</i>)	SC-I
shared.um.ldap.connection.timeout	Connection pooling connection timeout.	Integer value.	Not used. (<i>no timeout</i>)	SC-I

Uncategorized

Property Name	Description	Value Type	Default	Scenario
shared.smtp.host	SMTP host name.	Text representation of host name.	<i>localhost</i>	SC-II, SC-III
platform.smtp.host	SMTP host name.	Text representation of host name.	<i>localhost</i>	SC-II, SC-III
shared.smtp.port	SMTP port.	Integer value.	25	SC-II, SC-III
platform.smtp.port	SMTP port.	Integer value.	25	SC-II, SC-III
shared.smtp.auth	SMTP authentication switch.	Boolean value.	<i>false</i>	SC-II, SC-III
platform.smtp.auth	SMTP authentication switch.	Boolean value.	<i>false</i>	SC-II, SC-III
shared.smtp.auth.username	SMTP user name name.	Text value.	Not used.	SC-II, SC-III
platform.smtp.auth.user	SMTP user name name.	Text value.	Not used.	SC-II, SC-III
shared.smtp.auth.password	SMTP user password.	Text value.	Not used.	SC-II, SC-III
platform.smtp.auth.password	SMTP user password.	Text value.	Not used.	SC-II, SC-III
shared.http.urlbase	HTTP URL base.	URL.	Inserted in installation process.	SC-IV

Uncategorized, continued

shared.http.port	HTTP port.	Integer value.	Inserted in installation process. (8080)	SC-IV
shared.https.urlbase	HTTPS URL base.	URL.	Inserted in installation process.	SC-IV
shared.https.port	HTTPS port.	Integer value.	Inserted in installation process. (8443)	SC-IV
shared.https.use	Switch for use HTTPS.	Boolean value.	<i>false</i>	SC-IV
platform.webui.max.branch.count	Maximum number of concurrent windows.	Integer value.	4	SC-III
platform.webui.max.branch.depth	Page browsing history limit.	Integer value.	10 (effectively 5 pages)	SC-III
shared.db.fulltextsearch.appendpercentage	Determines whether a % is appended to search terms	TRUE or FALSE	TRUE	SC-III
platform.webui.max.upload.size	Determines maximum size of a repository archive file for import.	Unlimited.	-1	SC-I

How to Manage Artifact Form Validation

The Administrator can assign policies to validate artifacts when a user creates or edits them. For example, to ensure that keywords are set when a user creates a service.

To Assign Artifact Validation Policies:

1. In the Administration tab Administration menu, click **Governance > Data Integrity Constraints** to open the Artifact Validation page.

2. Select the artifact type that you want to validate for creation and edit. The Validated By table refreshes to show the policies used to validate the selected artifact type.

Artifact Type

- Agreement (3) ▾
- Application Collaboration
- Application Component
- Application Component Financial Profile
- Application Function
- Application Interaction
- Application Interface
- Application Layer
- Application Service
- Artifact
- Assessment
- Batch/File processing
- Binary Document
- BPPEL Process
- Business Actor (3)

▲ Previous
Next ▼

Validated by

✕
📄

<input type="checkbox"/>	Name ▲	Description
<input type="checkbox"/>	Administrator Should Not Be Artifact Owner	
<input type="checkbox"/>	All Application Components Developed	All application's components (services) are approved in Development stage.
<input type="checkbox"/>	All Application Components Deprecated	All application's components (services) are approved in Deprecated stage

3. Do one of the following:

- **To Add Policies:**

- i. Click **Add technical policy** to open the Add Policy dialog.
- ii. Use the search criteria to locate the technical policies you want to use.
- iii. Select the policies to use and click **Select** to add the policies to the Validate By table.

Add Policy



Enter text to search ...

<input type="checkbox"/>	Name ▲	Applicable To
<input type="checkbox"/>	☆ Administrator Should Not Be Artifact Owner	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Application Components Deprecated	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Application Components Developed	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Application Components Retired	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Application Components in Production	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Process Implementations Deprecated	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Process Implementations Retired	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Project Artifacts Developed	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Project Artifacts In Production	HP Enterprise Maps resource
<input type="checkbox"/>	☆ All Service Implementations Deprecated	HP Enterprise Maps resource

Page 1 of 4 | Show descriptions | Change Page Size

Displaying 1 - 10 of 37

■ **To Remove Policies:**

- i. Select the policies to remove.
- ii. Click **Remove all selected policies** and confirm your decision to remove the selected policies from the Validated By table.

Validated by

✕ +

<input type="checkbox"/>		Description
<input checked="" type="checkbox"/>	Administrator Should Not Be Artifact Owner	
<input type="checkbox"/>	All Application Components Developed	All application's components (services)
<input type="checkbox"/>	All Application Components Deprecated	All application's components (services)

You can extend form validation to also validate data attachments to artifacts. Set property `platform.autovalidation.validateData` to true. For details, see ["How to Manage System Settings" on page 59](#).

Chapter 10: Administration Utilities

HP EM administration utilities consist of command-line tools located in the `bin` directory of the installation folder.

The utilities are summarized in ["HP EM Utilities" below](#).

This chapter describes the following utilities:

- ["Export Tool" on the next page](#)
- ["Import Tool" on page 85](#)
- ["Rebrand Tool" on page 88](#)
- ["Reset Tool" on page 88](#)
- ["SDM to Database Mapping Tool" on page 89](#)
- ["Setup Tool" on page 90](#)
- ["SSL Tool" on page 92](#)

Note: If passwords are encrypted, set the option `--passphrase passphrase` on the command-line when you launch any tool that requires authentication.

HP EM Utilities

The HP EM utilities are located in `EM_HOME/bin`. These are either batch BAT files or shell SH scripts, depending on the server operating system.

Note: If a utility is not in `EM_HOME/bin`, a relative path is shown for the command in table ["Admin Utilities" below](#).

Admin Utilities

Command	Description
<code>env</code>	A script used by other HP EM tools to set system variables. Do not execute this script directly.
<code>env-jboss</code>	Called by <code>serverstart</code> to set system variables for the application server. Do not execute this script directly.
<code>export</code>	Creates a data image for specified components of HP EM. For details, see "Export Tool" on the next page .

Command	Description
import	Imports a data image for specified components of HP EM. For details, see "Import Tool" on page 85 .
rebrand	Re-brand or co-brand HP EM with your company specific logos and names. For details, see "Rebrand Tool" on page 88 .
reset	Resets the data for specified components of HP EM. For details, see "Reset Tool" on page 88 .
../lib/sdm/bin/sdm2dbmap	Creates a report of the relationship between the SDM structure and the database tables. For details, see "SDM to Database Mapping Tool" on page 89 .
serverstart	Calls env-jboss to set critical system variables for JBoss, and then starts the platform application server. For other application servers, use the server start functionality in the application server.
serverstop	Stops the platform application server for JBoss. For other application servers, use the server stop functionality in the application server.
setup	Starts the Setup Tool to reconfigure the platform server. For details, see "Setup Tool" on page 90 .
ssltool	Configures and views your SSL configuration. For details, see "SSL Tool" on page 92 .

Note: If a command requires arguments, running it without arguments displays a help screen, unless otherwise stated.

Export Tool

The **export** command enables you to export the configuration and data in the database to an image, and then import that data at a later date.

The syntax for export is:

export --image *IMAGE_NAME* [OPTIONS]

The Export Tool includes the following options:

<code>--image <i>IMAGE_NAME</i></code>	The path to the directory where the image is stored.
--	--

--components [COMPONENT]	<p>The following component options are available:</p> <ul style="list-style-type: none"> • all This is also the default if you omit --components. Exports all the configurations and data except the license. • configuration The configuration data. • content All data without the configuration and security data. • security The security configuration. User profiles, groups, and roles and the default ACLs for newly created resources.
--quiet	Execute the command without a confirmation request.
--silent	Less verbose console output.
--last-revision	Exports only last artifact revision. Last revision number will be reset to 1.
--include-generated-data	<p>Enforce export of all non-valuable data such as user event, execution, and validation data. This option also covers these options:</p> <ul style="list-style-type: none"> • --userEvents-dontSkip • --executions-flat-limit • --policyManager-validations
--executions-flat-limit <i>N</i>	<p>Export execution reports in a flat layout with a limit of <i>N</i> reports/items.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: By default, execution reports are exported in a flat layout up to a predefined number of reports and items. If the limit is exceeded a hashed layout is used instead to prevent potential excess directory errors. Use this command to define your own limit for flat layout exports.</p> </div>
--configuration-all	Export the complete configuration (not recommended).

<code>--configuration-application</code>	Export the application configuration (default).
<code>--configuration-system</code>	Export the system configuration (default).
<code>--configuration-licence</code>	Export license details.
<code>--policyManager-validations</code>	Enable the export of policy manager validation data (not exported by default).
<code>--userEvents-dontSkip</code>	Export user event data (not exported by default).

Caution: HP EM must not be running when you execute these commands.

The export creates the directory specified by `IMAGE_NAME`, containing the following, depending on the component options used:

- `image.properties`
A file containing the export execution properties and a list of the data sets exported.
- `configuration`
A directory containing the configuration properties files, including role-based UI customizations. The file also contains the license details if you use the **`--configuration-license`** option.
- `dist`
Contains properties specific to a particular distribution. Create this data with the **`--configuration-force`** option.
- `executions`
A directory containing the execution report results of asynchronous tasks such as publishing, discovery, and bulk operations.
- `lifecycle`
A directory containing the lifecycle data.
- `platform`
A directory containing the service catalog data.
- `policyManager`
A directory containing the policy data.
- `reporting`
A directory containing the reporting definitions.

- security
A directory containing the security configuration.
- userEvents
A directory user specific event information.

Import Tool

The **import** command enables you to import HP EM configuration and data to the database from an image.

Note: When importing an image with governed artifacts using the default options, lifecycle processes with identical Uuids in the image are not imported. To avoid inconsistencies in the lifecycle of artifacts use the import tool with the **--reset** option which deletes all existing artifacts and lifecycle processes.

Note: Importing a HP EM 10.00 image replaces the current group membership with group membership from the image. Importing an image migrated from HP EM 4.x, merges the imported group membership with the current group membership.

The syntax for import is:

import --image *IMAGE_NAME* [OPTIONS]

Note: HP recommends updating Oracle Database schema statistics after importing large amounts of data. Old statistics may impact the performance of some data queries. Consult your database administrator.

To Update Oracle Schema Statistics:

- Execute the following command:

```
EXEC DBMS_STATS.GATHER_SCHEMA_STATS (ownname => '&1',no_invalidate => FALSE,options => 'GATHER');
```

This command does not require database admin privileges and can be run by the schema owner (ownname).

The Import Tool includes the following options:

<code>--image</code> <i>IMAGE_NAME</i>	The path to the directory where the image is stored.
--	--

<code>--components [COMPONENT]</code>	<p>The following component options are available:</p> <ul style="list-style-type: none"> • <code>all</code> <p>This is also the default if you omit <code>--components</code>. Imports all the data without the configuration.</p> <ul style="list-style-type: none"> • <code>configuration</code> <p>The configuration data.</p> <ul style="list-style-type: none"> • <code>content</code> <p>All data without the configuration and security data.</p> <ul style="list-style-type: none"> • <code>security</code> <p>The security configuration. User profiles and groups and the default ACLs for newly created resources.</p>
<code>--quiet</code>	Execute the command without a confirmation request.
<code>--silent</code>	Less verbose console output.
<code>--reset</code>	Executes the reset command first deleting all existing artifacts and lifecycle processes, with matching component options.
<code>--passphrase <i>PASSPHRASE</i></code>	Use the master passphrase entered during installation if password encryption is enabled.
<code>--configuration-passphrase <i>IMAGE_PASSPHRASE</i></code>	If image was exported from a server having a different passphrase than the current one; specify using this parameter to decrypt the configuration data in image.
<code>--force</code>	If an imported service catalog resource is already in the database, it is overwritten.
<code>--platform-bootstrap</code>	Import the service catalog data in bootstrap format.
<code>--platform-update-blacklist</code>	Append imported service catalog resources to the migration blacklist. Useful for bootstrap installation.
<code>--platform-rest-blacklist</code>	Save imported service catalog resources to the migration blacklist.
<code>--platform-ignore-sdm-merge-warn</code>	Continue service catalog data import if the SDM merge check only reports warnings.
<code>--executions-force</code>	If an imported execution report or item is already in the database, it is overwritten.

<code>--configuration-all</code>	Import the complete configuration (not recommended).
<code>--configuration-application</code>	Import the application configuration (default).
<code>--configuration-system</code>	Import the system configuration.
<code>--configuration-licence</code>	Import license details.
<code>--userEvents-dontSkip</code>	Import user event data (not imported by default). Existing user event data is deleted before this data imports.

Caution: HP EM must not be running when you execute these commands.

The import checks the directory specified by `IMAGE_NAME`, which contains the following depending on the image:

- `image.properties`
A file containing the export execution properties and a list of the data sets exported.
- `configuration`
A directory containing the configuration properties files, including role-based UI customizations. The file also contains the license details if the export used the **--configuration-license** option.
- `dist`
Contains properties specific to a particular distribution. Use the **--configuration-force** option to import this data.
- `executions`
A directory containing the execution report results of asynchronous tasks such as publishing, discovery, and bulk operations.
- `lifecycle`
A directory containing the lifecycle data.
- `platform`
A directory containing the service catalog data.
- `policyManager`
A directory containing the policy data.
- `reporting`
A directory containing the reporting definitions.

- security
A directory containing the security configuration.
- userEvents
A directory user specific event information.

Note: If specific components are specified, the other component folders are ignored. If a specified component is not present, the import fails.

Rebrand Tool

The rebrand tool enables you to extract the images, text, and libraries from HP EM used to identify and brand it as an HP product. You can then modify these files and reapply your own corporate image to HP EM.

The command for rebranding is:

rebrand [OPTIONS]

The Rebrand Tool includes the following options:

<code>--extract</code>	Extract the current branding image.
<code>--apply</code>	Apply a new branding image.
<code>--image IMAGE</code>	The path to the image archive file (--apply) or a path to directory to export the extracted image to (--extract).
<code>--imageconf FILE</code>	Custom path to create an image configuration XML file (--extract only).
<code>--quiet</code>	Execute with no confirmation queries.
<code>--silent</code>	Less verbose console output.
<code>--force</code>	Ignore branding image consistency check errors, for example missing files, (--extract option only).
<code>--passphrase PASSPHRASE</code>	Specify the master passphrase entered during installation or setup if password encryption is enabled.

Caution: HP EM must not be running when you execute these commands.

Reset Tool

The **reset** command enables you to reset the HP EM data in the database and import the default image.

Note: All artifacts and lifecycle processes are deleted prior to the import. This resolves any conflicts with identical artifacts or process UUIDs between existing and imported data.

The syntax for reset is:

reset [OPTIONS]

The Reset Tool includes the following options:

<pre>--components [COMPONENT]</pre>	<p>The following component options are available:</p> <ul style="list-style-type: none"> • all This is also the default if you omit --components. Resets all data. • content Resets all data excepting security. • security Resets only security configuration. User security profile, groups, roles and default ACL's for newly created resources.
<pre>--quiet</pre>	<p>Execute the command without a confirmation request.</p>

Caution: HP EM must not be running when you execute these commands.

SDM to Database Mapping Tool

Artifacts in the Catalog are stored in the form of XML documents. Their structure is defined by the System Data Model (SDM). Artifacts are serialized into a database over a standard serialization layer. The serialization of data may differ from the norm, based on customer specific extensions or modifications.

The `sdm2dbmap` tool is a mapping tool that generates a report containing the mapping between your SDM and database tables.

To generate the report, execute the following command:

EM_HOME/lib/sdm/bin/sdm2dbmap

The mapping report is output to the following file:

`EM_HOME/lib/sdm/build/sdm2dbmap.html`

The output consists of the following parts:

- A top level 1:1 mapping between SDM artifacts and DB tables. Each artifact listed, maps directly to one table.

- A list of artifacts. Each artifact in the report maps each SDM property to a specific column in the table. There are also associated tables and foreign keys, joined using the primary key of the artifact table.
- A report documenting the DB schema for all database tables coming from the SDM. Tables with names ending in `_Rev` are used to store older revisions.

Setup Tool

Included with HP EM is the Setup Tool. You can use it for the following functions, which you select as **Scenarios** when running the tool.

To access the Setup Tool user interface, execute the following command:

EM_HOME/bin/setup

The Setup GUI opens at the Welcome screen.

Click **Next** to be presented a set of scenarios, as described in the following sections:

- ["Changing the License Key" below](#)
- ["Applying Extensions" on the next page](#)
- ["Updating HP EM" on the next page](#)
- ["Advanced Setup Tool Options" on the next page](#)

The Setup Tool can also be used in command line mode.

For details, see ["Setup Tool Command-Line Options" on page 92](#).

Note: By default, the Setup Tool does not allow you to import data or apply extensions while there is a server running in order to protect data consistency. In some environments (for example, behind a load balancer proxy or using Siteminder) there is always something running at the server endpoint. To enable the Setup Tool in these environments set the `install.ignore.running.platform` property to `TRUE`. For details, see ["How to Manage System Settings" on page 59](#). Alternatively, execute the Setup Tool with the following command option: **-Dinstall.ignore.running.platform=true**

Changing the License Key

The Setup Tool enables you to change the license.

To Change the License Key with the Setup Tool:

- a. In the Scenario Selection page, select **Change License Key**, and then click **Next**.

The License Information page opens.

- b. In the License Information page, do one of the following:
 - o Select **Install a 60 day evaluation license**.
 - o Select **Enter license details**, and input the license details provided by your sales representative.

Click **Next**.

- c. Click **Next** through each confirmation and progress page, and when the setup is complete, do one of the following:
 - o Click **Setup Again** to return to the Scenario Selection page.
 - o Click **Finish** to exit the Setup Tool.

Note: The Administration Tab also provides support for changing the license key. For details, see *Installation and Deployment Guide*, section *License Management*.

Applying Extensions

For details see *Installation and Deployment Guide*, section *Apply Custom Extensions* .

Updating HP EM

The Setup Tool enables you to install updates to HP EM, which are downloaded or copied to the EM_HOME/updates directory.

Advanced Setup Tool Options

The Advanced scenario enables you to select specific parts of the configuration procedure to suit the needs of a specific task.

To Select Specific Configuration Processes:

- In the Scenario Selection page, select **Advanced**, and then click **Next**.

The Custom Scenario Selection page opens and enables you to select which parts of the configuration you want to execute.

Every part of the configuration process is listed as an individual step. The steps required for a particular process vary depending on what configuration you want to change.

Setup Tool Command-Line Options

The Setup Tool can also be executed as a command line tool.

The setup command is:

EM_HOME/bin/setup [OPTIONS]

The following options are available:

- **-h, --help [scenarios|steps]**

Display the available options or list the available scenarios or steps in the console.

- **-c, --console**

Execute the Setup Tool in console mode.

- **-a, --dbadmin-mode**

Enables DB administrator mode. The setup stops after creating the DB scripts, allowing the administrator to execute them manually. Continue installation after script execution with **setup -c**.

- **-n, --scenarios SCENARIO**

Execute only the specified steps in the installation. Use **--help scenarios** to view a list of available scenarios.

- **-p, --steps [comma separated list of steps]**

Execute only the specified steps in the installation. Use **--help steps** to view a list of available steps.

- **-u, --use-config FILE**

Use the properties in the specified file to override the default or current configuration properties.

- **--passphrase PASSPHRASE**

If password encryption is enabled, specify the passphrase to use for encryption.

- **-d, --debug**

Execute the setup in debug mode. All properties, SQL statements, and installation details are output to EM_HOME/log/setup.log.

SSL Tool

The SSL Tool is a combined tool enabling you to setup client-side SSL for a deployed HP EM application. It also enables you to print SSL server certificates, as well as to download the SSL server

certificate chain.

The SSL Tool has the following basic actions:

- **serverInfo**

Prints the SSL requirements for the specified HTTPS URL, and saves the server certificate to a file.

- **keystoreEI**

Exports or imports SSL certificates to the HP Enterprise Maps database keystore or truststore.

- **customize**

Change the effective SSL customization.

The syntax for `ssltool` is:

EM_HOME/bin/ssltool [ACTION] [options]

Execute `ssltool` with no action or options to view the help with some examples.

Execute `ssltool [ACTION] --help` to view specific help for each type of action with the available options.