

HP Service Manager

Software Version: 9.41

For the supported Windows® and UNIX® operating systems

Application Setup help topics for printing

Document Release Date: September 2015
Software Release Date: September 2015



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

© 1994-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

UNIX® is a registered trademark of The Open Group.

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

For a complete list of open source and third party acknowledgements, visit the HP Software Support Online web site and search for the product manual called HP Service Manager Open Source and Third Party License Agreements.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hp.com/>.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** 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 site at: <https://softwaresupport.hp.com>.

This website 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 website 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 to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

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

HPSW Solutions Catalog accesses the HPSW Integrations and Solutions Catalog portal website. 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 website is <https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710>.

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: Application Setup	10
Chapter 2: HP Service Manager Processes and Best Practices Guide	12
Processes	12
User Interaction Management overview	13
Incident Management overview	13
Request Fulfillment overview	14
Problem Management overview	14
Change Management overview	14
Configuration Management overview	15
Chapter 3: Adding users	16
Checklist: Adding a new user	16
Creating operator records	16
Operator records	17
Add an operator record	20
Add an operator record with the User Quick Add utility	21
Add an operator to a security group	21
Create a system default operator record	22
Define a startup menu for an operator	22
Define the distinguished name an operator uses to log in to an LDAP directory service ..	23
Delete an operator record	24
Enable an operator to see the command line	24
Set database access for an operator	25
Set the first day of week for an operator	26
Set the maximum file attachment size for an operator	27
Set the total file attachment size for an operator	28
Set the time zone for an individual operator	28
Update an operator record	29
View an existing operator record	29
Use Mass Update with operator records	30
Synchronization between contact and operator records	31
Mass create contact records from operator records	31
Mass create operator records from contact records	32
Create an operator record from a contact record	32
Create an operator record from an operator template	33
Create a contact record from an operator record	34

Operator templates	35
Create an operator record from an operator template	36
Create an operator template	37
Define the operator template applied to LDAP users	38
Chapter 4: Process Designer	39
Create a rule set	41
Clone an existing Rule Set	42
Adding a rule	42
Add a Launch a URL rule	45
Add a Run a Macro rule	45
Add a Call a Process rule	46
Add a Case Exchange rule	47
Add a Run a Wizard rule	48
Add a Clear Fields rule	49
Add a JavaScript Validation rule	50
Add a Run JavaScript rule	51
Add a Set Mandatory Fields rule	52
Add a Set Mandatory Variables rule	53
Add a Send Notifications rule	54
Add a Launch a Script rule	55
Add a Send HTML Email rule	56
Add a Start or Stop Clock rule	58
Add a Set Field rule	60
Add a Set Field from Number rule	61
Add a Validate Date rule	62
Add a Field Validation against a List rule	63
Add a Validate against Table rule	64
Add a Validate Text/Number rule	66
Add a Field Validation against a Table rule	67
Add a Popup Message Box rule	69
Add an Assignment rule	70
Add a Run Action rule	72
Add a Run Scheduled Action rule	74
Group rules	76
Using the Condition Editor	77
Launch the Condition Editor from a rule	79
Launch the Condition Editor from a workflow	79
Build a condition	80
Create a group of condition items	85

Copy a condition	86
Enable deprecated fields and system fields in the Condition Editor	86
Task Planner	87
Plan a task with Task Planner	88
Setting the input and output data in Task Planner	90
Configure the recommended maximum number of tasks	91
Configuring Task Planner	92
Add fields to Task Planner	92
Edit additional fields in Task Planner	95
Remove additional fields from Task Planner	96
Configure the status mapping between the task file and Task Planner	96
Configure the additional properties in Task Planner	97
Add an additional property	97
Edit an additional property	98
Delete an additional property	98
Process Designer workflows	99
Create a workflow	99
Copy an existing workflow	101
Export a Workflow	101
Workflow phases	102
Add a phase	102
Copy a phase	107
Workflow transitions	108
Create a manual workflow transition	109
Create an automatic workflow transition	110
Create a default workflow transition	111
Workflow Viewer	112
View a workflow in Workflow Viewer	112
View the workflow properties	113
Integrate Workflow Viewer into a new form	114
Workflow-based rule sets, actions, and transitions	116
Workflow-based rule sets	116
Workflow-based actions	118
Workflow transitions	118
Process Designer security model	119
Out-of-box role rights in the Common Configuration area	121
Multiple security roles	123
Add a security role	124
Add security roles and settings	124
Roles in the operator record	125

Assign a role or roles to an operator	125
Add an area	126
Add a setting within an area	126
Validation script for a new setting	129
Update a setting within an area	129
Localize an additional setting	130
Modify the rights for a role within an area	131
Update rights to display allowed categories and allowed statuses	132
Modify allowed categories and allowed statuses	133
Check security rights by using Java Script or variables	134
Check security rights using Java Script	134
Check record right with variables	135
Chapter 5: Controlling user access and security	136
HP proprietary records	138
Ongoing maintenance	138
Environment record	138
Service Manager record relationship models	138
Full Service Desk model	139
Status progression	140
Application profiles	142
Approval delegation	143
Administering approval delegation	144
Enabling approval delegation	145
Global variables available for approval delegation	146
What happens when I receive delegated approval authority?	146
Temporary rights of an approval delegate	147
What happens when I delegate approval authority?	148
Delegate approvals to another operator	149
Update an active approval delegation	150
Disable an active approval delegation	150
Copy an approval delegation	151
Views available for approval delegation	152
User roles	153
Add a user role record	153
Delete a user role record	154
Search for a user role record	154
Set database access for a user role	154
Capability word model	156
Capability words	156

Add a capability word	165
Delete a capability word	165
Search for capability words	165
Operator passwords	166
Change a user's password	166
Disable the password reset option	167
Enable password history	167
Enable the password reset option	168
Reset an operator's password	168
Set password format restrictions	169
Set password maximum lifetimes	170
Set password minimum lifetimes	171
License tracking	172
License types	173
Profile fields for Configuration Management license tracking	174
Profile fields for Knowledge Management license tracking	174
Profile fields for Contract Management license tracking	176
Security right fields for Service Desk license tracking	178
Security right fields for Incident Management license tracking	178
Security right fields for Problem Management license tracking	179
Security right fields for Change Management license tracking	179
Security right fields for Request Fulfillment license tracking	180
Security right fields for Service Level Management license tracking	180
Capability words for Smart Analytics license tracking	181
Disable application license tracking	181
Named users	181
Defining named users	182
Determine the number of named users available	182
Make an individual operator a named user	182
Named users for applications	183
Define named users for applications	183
Disable application license tracking	184
HP Service Manager license report	185
Generate a user license report	186
Stathistory table	186
View the stathistory table	187
Self-service licenses	187
Folder entitlement	188
Enable folder entitlement	189
Disable folder entitlement	189

Add a security folder	190
Delete a folder	191
Specify use of the default folder from the operator record	191
Add folder permissions to a security role	192
Chapter 6: Calendars	193
Holiday records	194
Add a master data record	194
Delete a master data record	195
Update a master data record	196
Create a holiday group	197
On-call schedules	198
On-call schedule exceptions	199
Create an on-call schedule	200
Work schedules	201
Add a master data record	202
Delete a master data record	203
Update a master data record	204
Chapter 7: Clocks	206
Add a clocks record	207
Add a clock to track incident record status changes	208
Enable tracking of operator times	208
Start or stop a clock from a macro	209
Start or stop a clock from format control	211
View a clock record	212
Chapter 8: Self-service	213
Working with self-service requests	213
Visible updates for self-service requests	213
Creating self-service users	214
ESS and ESSM-Approval users	214
Self-service template record	214
Create a self-service user	215
Create a self-service user from an existing contact	217
Create multiple self-service users from a contact list	218
What is a self-service power user?	218
Grant self-service access	219
Configuring the self-service working environment	220
Create a Service Desk self-service security role	222
Self-service licenses	222
Who uses self-service?	223

Choosing a configuration item for self-service requests	223
Self-service tailoring	224
Customize the self-service interface	224
Chapter 9: Views and favorites administration	226
Create a view	227
Add a view for a new table	229
Delete a view	231
Change fields in a view	232
Change roles for a view	234
Autoformatting	235
Add a new autoformatting rule	236
Adjust the order of an autoformatting rule	238
Edit an autoformatting rule	239
Remove an autoformatting rule	241
Customize current view	242
Chapter 10: ITIL Alignment	243
Access Control	243
Mandatory Fields	243
Reporting	244
Management Reporting	247
Audit Trail	249
Archiving	249
Notification and Escalation	249
Send Documentation Feedback	251

Chapter 1: Application Setup

Administrators enable users to access applications by creating security rights, security area, security role, role, and operator records. Administrators control the following application tables and related administrative tasks:

- Security rights
- Security roles
- User roles
- Capability words

- Adding users
- Purging and archiving records
- Lockouts
- Login restrictions

Chapter 2: HP Service Manager Processes and Best Practices Guide

In order for you to make optimal use of the functionality of HP Service Manager, HP has created a processes and best practices guide based on practical experience with service management implementations with many customers of various sizes.

The *HP Service Manager Processes and Best Practices Guide* provides best practices, management overviews, process flows, and workflow diagrams for different Service Manager modules.

The *HP Service Manager Processes and Best Practices Guide* documents the practice workflows that are standard with out-of-box Service Manager applications. It includes high-level process workflow diagrams, and step-by-step procedural guidelines.

You can view and search this guide using Adobe® Reader, which you can download from the Adobe Web site.

[HP Service Manager Processes and Best Practices Guide](#)

Processes

The HP Service Manager processes are based on ITIL theory and are referenced in the ITIL core.

The Service Manager best practices cover the following processes in the ITIL Service Transition and Service Operation documents. For information on these processes, see the *HP Service Manager Processes and Best Practices Guide* linked in the related topics.

ITIL core volume	process number	process reference	process reference
Service Operations	0	"User Interaction Management overview" on the next page	S00
Service Operations	2	"Incident Management overview" on the next page	S02
Service Operations	3	"Request Fulfillment overview" on page 14	S03
Service Operations	4	"Problem Management overview" on page 14	S04
Service Transition	2	"Change Management overview" on page 14	ST2

ITIL core volume	process number	process reference	process reference
Service Transition	3	"Configuration Management overview" on page 15	ST3

User Interaction Management overview

The HP Service Manager User Interaction Management process helps you handle User Interactions either reported by using Self-Service web pages or directly to your Service Desk. Though not an ITIL process, this process enables the separation between information requests and service requests. The result is that multiple user interactions may all be linked to one incident record in the tool. This process will streamline the Service Desk activities and thereby decrease the workload for second line support teams.

The Service Manager Service Desk application supports the service desk function of the Information Technology Infrastructure Library (ITIL) with its User Interaction Management processes for the IT service and the customer base. It provides a single point of entry to the other Service Manager applications and enables you to document and track all calls received by your service desk. It incorporates the essential concepts of ITIL to ensure that the best practices of IT service management in place. The Service Desk application helps you to aid end customers, ensure data integrity, and streamline communication channels in the organization.

For complete information on the User Interaction Management (Service Desk) process overview and workflows, see *HP Service Manager Processes and Best Practices Guide* in the related topics.

Incident Management overview

The HP Service Manager Incident Management process enables you to categorize and track various types of incidents (such as service unavailability or performance issues and hardware or software failures). It helps you to ensure that incidents are resolved within agreed on service level targets.

The Service Manager Incident Management application supports the Incident Management process. It incorporates the essential concepts of Information Technology Infrastructure Library (ITIL) to ensure that the best practices of IT service management in place. The Incident Management application helps you to restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

For complete information on the Incident Management process overview and workflows, see *HP Service Manager Processes and Best Practices Guide* in the related topics.

Request Fulfillment overview

The HP Service Manager Request Fulfillment process enables you to effectively manage all user requests for products and services. It provides your users a mechanism to request and receive standard services based on a pre-defined approval and qualification process. The HP Service Manager Request Fulfillment application supports the Request Fulfillment process. It incorporates the essential concepts of Information Technology Infrastructure Library (ITIL) to ensure that the best practices of IT service management in place. The Request Fulfillment application gives you an increased level of control for your organization's services and helps you source and deliver the necessary components for requested standard services. For complete information on the Request Fulfillment process overview and workflows, see the *HP Service Manager Processes and Best Practices Guide*.

Problem Management overview

The HP Service Manager Problem Management process allows you to find, fix, and prevent problems in the IT infrastructure, processes, and services. It helps you to prevent problems and their resulting incidents, eliminate recurring incidents, and minimize the impact of incidents that cannot be prevented.

The Service Manager Problem Management application supports the entire Problem Management process. It incorporates the essential concepts of Information Technology Infrastructure Library (ITIL) to ensure that the best practices of IT service management in place. The Problem Management application helps you to maximize system availability, improve service levels, reduce costs, and improve customer convenience and satisfaction.

Note: ITIL defines a Problem as the unknown cause of one or more Incidents.

For complete information on the Problem Management process overview and workflows, see *HP Service Manager Processes and Best Practices Guide* in the related topics.

Change Management overview

The HP Service Manager Change Management process enables you to control changes to baseline service assets and configuration items across the entire service life cycle. It helps you to control the process to request, manage, approve, and control changes that modify your organizational infrastructure. This includes assets, such as network environments, facilities, telephony, and resources.

The Service Manager Change Management application supports the Change Management process. It incorporates the essential concepts of Information Technology Infrastructure Library (ITIL) to ensure that the best practices of IT service management in place. The Change Management application help you to ensure that changes are requested, evaluated, and implemented according to your business processes and needs.

Note: To control changes, HP recommends that you handle all standard changes (that is, changes of predefined types) by using the Service Catalog request fulfillment process.

For complete information on the Change Management process overview and workflows, see *HP Service Manager Processes and Best Practices Guide* in the related topics.

Configuration Management overview

The HP Service Manager Configuration Management process ensures that selected components of a complete IT service, system, or product (the Configuration Item) are identified, baselined, and maintained and that changes to them are controlled. It enables you define and control the components of services and infrastructure, and to maintain accurate configuration information about the historical, planned, and current state of services and infrastructure.

The Service Manager Configuration Management application supports the Configuration Management process. It incorporates the essential concepts of Information Technology Infrastructure Library (ITIL) to ensure that the best practices of IT service management in place. The Configuration Management application supports your business and control objectives, and helps you to track your configuration items through their lifecycle.

For complete information on the Configuration Management process overview and workflows, see *HP Service Manager Processes and Best Practices Guide* in the related topics.

Chapter 3: Adding users

Each person (user) who logs onto HP Service Manager must have a personal information record stored in the operator table. Information associated with a user includes personal data, such as name, address, phone numbers, login name, and password for Service Manager. Operator records also store capability words for a given user. Without an operator record, a user cannot log onto Service Manager. A user can belong to a group with a single profile or have a unique profile.

Checklist: Adding a new user

To add a user, follow these steps:

1. Create a contact record for the user.

Caution: You cannot create an operator without a contact Id.

2. Create an operator record for the user.
3. Select security settings for the user.

Do one of the following:

- Select a user role, which includes predefined security roles, application profiles (for Knowledge Management and Configuration Management modules), and capability words.
- Select security roles, application profiles and capability words.

4. Create a startup menu for the user.
5. Create a menu record for the user.

Creating operator records

HP Service Manager provides the following methods for creating an operator record:

- Create the operator record from the operator.g form, which enables you to:
 - Create an operator record starting from a blank operator record
 - Create an operator by copying properties from an existing operator
- Create the operator record from Ongoing maintenance (CAU) User Quick Add Utility, which enables you to:
 - Create an operator record starting from a blank operator record
 - Create an operator by copying properties from an existing operator
 - Create a contact record starting from a blank contact form
 - Create a contact by copying properties from an existing contact

Service Manager includes several predefined operator records that you can use as templates to create your own users. Search your operator records to see a complete list of sample operators.

Operator records

Each HP Service Manager user must have an operator record to log on and use Service Manager applications. The operator record defines the access rights and security settings that a user has. The following fields are required for an operator record:

- Login Name
- Resource Type

You can also define the following optional information in an operator record:

Operator tab	Fields and sections	Purpose
General	<ul style="list-style-type: none"> • Login Name — Required field Full Name • Default Company • Contact ID 	Use this tab to add identifying information and application profiles to an operator record. These application profiles determine which features and views the operator can access in Service Manager applications.

Operator tab	Fields and sections	Purpose
	<ul style="list-style-type: none"> • Application Profile • User Role • Application profiles • Security Roles 	
Security	<ul style="list-style-type: none"> • Password Information • User Session Information • Login Information • User Lockout Information • LDAP Information • Template Information • Password History 	Use this tab to manage how an operator accesses Service Manager. These settings determine whether an operator can log on to Service Manager.
Login Profiles	<p>Login Profile — This section contains:</p> <ul style="list-style-type: none"> • The operators login profile • Licensing Information 	<p>The login profile includes:</p> <ul style="list-style-type: none"> • Language: Specifies the login language for the operator. • Time Zone: Specifies the time zone for the operator. • Date Format: Specifies the preferred format for the date, such as mm/dd/yy or dd/mm/yy. • First Day of Week: Specifies the first day of the week in the calendar and date picker for the operator. • Display Currency: Specifies what currency displays for catalog items when the operator orders from the Service Catalog or

Operator tab	Fields and sections	Purpose
		<p>approves catalog requests. Defaults to the basis currency in the System Information Definition record for the company when left blank.</p> <ul style="list-style-type: none"> • Message Level: Specifies the level of messages to store in the message queue for this operator. • Max Attachment Size: Specifies the maximum size of a file that the operator can insert into an attachment object. • Total Attachment Size: Specifies the maximum size of all the attachment files that the operator can insert into an attachment object.
Groups	<ul style="list-style-type: none"> • Knowledge Groups to which the operator belongs • Assignment Groups to which the operator belongs 	Use this tab to determine which groups to which the operator belong. Assignment groups are used for both work assignment and approval.
Startup	<ul style="list-style-type: none"> • Initial Application • Home Page • Queue • Dashboard • Execute Capabilities • Query Groups • Months 	Use this tab to determine which forms the operator sees at startup and also to customize the capability words the operator has in addition to those granted by a user role.
Notification	<ul style="list-style-type: none"> • Standard Notifications • Client 	Use this tab to record contact information about the operator.

Operator tab	Fields and sections	Purpose
	Printing	
Rate	<ul style="list-style-type: none"> Hourly Rate Rate Currency 	Use this tab to determine the operator's labor cost rate.
Self Service	<ul style="list-style-type: none"> Self Service Access Only Self Service Menu Self Service Starting Page 	Use this tab to authorize self service access to an operator. This gives the user access to the self service Web client.

Add an operator record

Applies to User Roles:

System Administrator

Note: To create an operator, you need to first create a contact record to match the operator record.

To add a contact record:

1. Click **System Administration > Base System Configuration > Contacts**.
2. Specify the **Contact Name**.
3. Specify the **Full Name**.
4. Add any other necessary information.
5. Click **Add**, and then click **OK**.

You are now ready to create an operator record.

To add an operator record:

1. Click **System Administration > Ongoing Maintenance > Operators**.

2. Specify a **Login Name**.

Note: HP recommends that you only use ASCII characters in **Login Name**. In Service Manager Web Service integrations, non-ASCII operator login names are not supported.

3. Specify a **Contact ID**, or select the contact name that you just created.

4. Click **Add**.

5. On the Security tab, type the name of the **Template** from which you want to create the new operator record.

The information from the template will be populated in the new operator record.

6. Add any other necessary information for this new operator record.

7. Click **Save**.

Add an operator record with the User Quick Add utility

Applies to User Roles:

System Administrator

To add an operator record with the User Quick Add utility:

1. Click **System Administration > Ongoing Maintenance > User Quick Add Utility**.

2. Fill in the required fields.

3. Click **Next**.

4. Type the name of a user to clone or use the Fill icon to find a user to clone.

5. Click **Finish**.

6. Update the new Operator record as required.

Add an operator to a security group

Applies to User Roles:

System Administrator

To add an operator to a security group:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Fill in optional search criteria, and then click **Search**.
3. Select the operator record to be changed.
4. Click the **Groups** tab.
5. In the groups array, type the names of the security groups for the new operator on separate lines.
6. Click **Save**.

Create a system default operator record

Applies to User Roles:

System Administrator

Information in the system default operator record becomes part of all operator records at the time you create the operator record and whenever you query the operator table. The operator table displays the field values in the system default record unless there is another entry that overrides it. For example, if the system default record defines the Default Company field with the value DEFAULT, then all operator records without a defined value for this field display the value DEFAULT.

To create a system default operator record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Click **Search** to select an operator from the record list.
3. Type or select the new operator information. The following fields are required for a system default record:
 - Login Name — type *SYSDEFAULTS
 - Resource Type — select the resource type to use.
4. Click **Add**.

Define a startup menu for an operator

Applies to User Roles:

System Administrator

The default home page for a HP Service Manager user is the Dashboard home page or To Do list specified for the operator or user role. You can define an old style startup menu or any other RAD application so that it is the initial application that Service Manager displays when an operator logs in. You define an initial application in the user's operator record.

Note: Specifying a Dashboard home page in a user's operator record overrides the To Do list and menus for that operator when they log in using the web client, even if the flag for menus has been set.

To define a startup menu for an operator, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the operator record to change.
5. Click the **Startup** tab.
6. In the **RAD Name** field, type the name of the startup menu or initial application to run when the operator logs on.
7. Type any parameter names and parameter values required by your startup form. For example, specify the following values for old style menus.
 - Parameter Names: `boolean1`
 - Parameter Values: `true`
8. Click **Save**.

Define the distinguished name an operator uses to log in to an LDAP directory service

Applies to User Roles:

System Administrator

To define the distinguished name an operator uses to log in to an LDAP directory service, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Click **Search** to view a list of operators.
3. Select the operator to update.
4. Click the **Security** tab.
5. In the **LDAP User DN** field, type the distinguished name you want the operator to use to bind to the LDAP directory service.
6. Click **Save**.
7. Click **OK**.

Delete an operator record

Applies to User Roles:

System Administrator

To delete an operator record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Use search or advanced search to find one or more records.
3. Select the operator record that you want to delete.
4. Click **Delete**.
5. Click **Yes** to confirm the deletion.
6. When you are prompted whether to remove a certain associated record, for example, an associated contact record, click **Yes** to delete the associated record or click **No** to keep the record.

Enable an operator to see the command line

Applies to User Roles:

System Administrator

To enable an operator to see the command line, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select an operator record from the record list.
5. Click the **Startup** tab.
6. Select **Activate Command Line on Startup**.
7. Click **Save**.

Set database access for an operator

Applies to User Roles:

System Administrator

Database access is a feature that gives you the ability to limit or grant access to database records, such as contacts, company, and regions. You can add or modify the existing out-of-box database access settings per user role or operator.

To set database access for an operator, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria, and then click **Search**.
3. Select an operator record from the record list.
4. Select the **Data Access** tab in the **General** tab.
5. To add a new Data Access record, follow these steps:
 - a. Click **Add new Data Access Record**.

The **Database Manager Data Access** form opens.

- b. Click **Fill** in the **Database Table Name** field to select a table.

- c. The operator name you initially selected is in the **Operator Name** field. If you want to add access to a different operator name than the one you selected, clear the field and click **Fill** to select a different operator name.
- d. To set the database access, select one of the following:
 - **Allow DB access:** The operator specified is granted access to the table specified.
 - **Prohibit DB access:** The operator specified is denied access to the table specified.
- e. When access has been granted to a table, click **Fill** in the **View Format** field to select the table view.
- f. Click **Add**.

The new database access record is added.

6. To modify an existing database access record, follow these steps:

- a. Select the **Data Access** tab in the **General** tab.
- b. Double-click the Table Name of the existing database access record you want to modify.

The **Database Manager Data Access** form opens.

- c. Make the necessary edits.
- d. Click **Save**.

Your changes are saved.

7. Click **OK**.

Set the first day of week for an operator

Applies to User Roles:

System Administrator

To set the first day of week for an operator, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.

3. Click **Search**.
4. Select the operator record that you want to change.
5. Click the **Login Profiles** tab.
6. In the **First Day of Week** field, select a day from the drop-down list.
7. Click **Save**.

This setting applies to the calendar and the date picker.

If you do not configure this field, the first day of the week for the operator is as follows:

- In the date picker, the first day of the week is the day that is configured by the **startDayOfWeek** parameter. For more information about the **startDayOfWeek** parameter, see ["Web parameter: startDayOfWeek" on page 1](#).
- In the calendar, the first day of the week is the day that is configured in calendar settings. For more information about the calendar settings, see ["Configure calendar settings" on page 1](#).

If you configure this field, the first day of the week in the date picker and the calendar for the operator will be the day that is specified in this field.

Set the maximum file attachment size for an operator

Applies to User Roles:

System Administrator

To set the maximum file size of a single attachment for an operator, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the operator record that you want to change.
5. Click the **Login Profiles** tab.
6. In the **Max Attachment Size** field, type the number of bytes for the maximum file attachment size.
7. Click **Save**.

You can define a file attachment maximum size limit for a particular operator from the operator record. The operator file attachment size limit supersedes the maximum file size set in the system wide company record but is itself subordinate to size limits defined for an attachment container in the Form Designer.

Set the total file attachment size for an operator

Applies to User Roles:

System Administrator

To set the total attachment size in any attachment container for an operator, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the operator record that you want to change.
5. Click the **Login Profiles** tab.
6. In the **Total Attachment Size** field, type the number of bytes for the total file attachment size.
7. Click **Save**.

You can define a total attachment size limit for a particular operator from the operator record. The total attachment size defined in the operator record supersedes the total attachment size set in the system wide company record but is itself subordinate to size limits defined for a specific attachment container in the Form Designer.

Set the time zone for an individual operator

Applies to User Roles:

System Administrator

To set the time zone for an individual operator, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.

4. Select the operator record to change from the record list.
5. In the **Time Zone** field, select the new time zone for the operator.
6. Click **Save**.

Update an operator record

Applies to User Roles:

System Administrator

To update an operator record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the operator that you want to update from the record list.
5. Type or select the new operator details. For example, change the **Application Profile** on the **General** tab, or add new capability words to the **Execute Capabilities** table on the **Startup** tab.
6. Click **Save**.
7. Click **OK**.

View an existing operator record

Applies to User Roles:

System Administrator

To view an existing operator record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select an operator from the record list to view the operator record.

Use Mass Update with operator records

Applies to User Roles:

System Administrator

Note: If you exit the **Mass Update** template form or **Complex Update** form without clicking **Execute**, all of your changes are cleared on the respective form.

To update several records at the same time, use one of the following methods:

Mass Update template

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria, and then click **Search**.
3. Select the records in the record list that you want to update.
4. Click **Mass Update**.
5. Type the value for the field in the text box or use the Find feature to display a list of potential values for the field.

Note: The value(s) you enter in the form are propagated to all of the records you selected.

6. Click **Next**.
7. Continue updating fields and click **Execute** when you complete your updates.

Simple Update:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria, and then click **Search**.
3. Select the records in the list that you want to update.
4. Click **Mass Update**.
5. Click **Simple Update**.

6. Type new values into the applicable fields on the form.
7. Click **Execute**.

Complex Update:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria, and then click **Search**.
3. Select the records in the list that you want to update.
4. Click **Mass Update**.
5. Click **Complex Update**.
6. Type the RAD code in the **Complex Update** form.
7. Click **Execute**.

Synchronization between contact and operator records

The contact and operator records are synchronized so that if you change the HP Service Manager ID field in the contacts record, it triggers the same change in the Contact ID field in the operator record. The reverse is also true. In order to make the synchronization possible, every user in the system must have both a contact record and an operator record.

Several redundant fields in the operator table were removed in order to leverage existing fields in the contacts table. See the Service Manager Upgrade Guide for a list of the fields removed from the operator table.

Mass create contact records from operator records

Applies to User Roles:

System Administrator

To mass create contact records from operator records, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.

4. In the record list, open the **More Actions** menu.
5. Click **Mass Create Contact**.
6. Follow the prompts to create the contacts.

Note: You can run the mass create function to create contact records only once. If you run the function again, it stops when it encounters the first operator record for which a contact already exists.

Mass create operator records from contact records

Applies to User Roles:

System Administrator

To mass create operator records from contact records, follow these steps:

1. Click **Support > Contacts**.
2. Type or select optional search criteria to find the contacts for which you want to create operator records.
3. Click **Search**.
4. In the record list, open the **More Actions** menu.
5. Click **Mass Create Operators**.
6. Follow the prompts to create the operators.

Note: You can run the mass create function to create operator records only once. If you run the function again, it stops when it encounters the first contact record for which an operator record already exists.

Create an operator record from a contact record

Applies to User Roles:

System Administrator

The contact and operator records are synchronized so that if you change the HP Service Manager ID field in the contacts record, it triggers the same change in the Contact ID field in the operator record. The reverse is also true. In order to make the synchronization possible, every user in the system must have both a contact record and an operator record.

To create an operator record from a contact record, follow these steps:

1. Click **System Administration > Base System Configuration > Contacts**.
2. Type or select optional search criteria to find the contact for which you want to create an operator record.
3. Click **Search**.
4. If the search returned a list of records, select the contact from the list.
5. In the contact record, click **More** or the More Actions icon.
6. Click **Create Operator**.
7. Follow the prompts to create the operator record.

Create an operator record from an operator template

Applies to User Roles:

System Administrator

Caution: Any changes that you make to an operator template automatically propagate to operator records based on that template. These automatic updates can consume substantial system resources.

To create an operator record from an operator template, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. In the **Login Name** field, type the new operator name.
3. Click the **Security** tab.
4. In the **Template** field, type the login name of the operator record to be used as an operator

template.

5. Click **Add**.

Note: Operator record login names are case sensitive.

Note: If an operator record has group1 in its security groups array when its template is NULL and group1 is in the security groups array of template_1 but not in that of template_2, when you assign template_1 to the operator record, the operator record has group1 in its security groups array; however, if you switches its template to template_2, group1 is lost in its security group array. To work around this issue, clear the template field, remove template_1L, save it, change the template to template_2, and then save.

Create a contact record from an operator record

Applies to User Roles:

System Administrator

The contact and operator records are synchronized so that if you change the HP Service Manager ID field in the contacts record, it triggers the same change in the Contact ID field in the operator record. The reverse is also true. In order to make the synchronization possible, every user in the system must have both a contact record and an operator record.

To create a contact record from an operator record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Enter and select the search criteria to find the operator for which you want to create a contact record.
3. Click **Search**.

A list of operator records is opened.

4. Select an operator from the list.
5. In the selected operator record, replace the **Contact ID** with the new contact ID.
6. Click **More** or the **More Actions** icon, and then **Create Contact** option.

7. Click **Create Contact**.
8. Follow the prompts to finish creating the contact.
9. Click **Save**.

Operator templates

System Administrators can design operator templates for creating operator records for users that share common information and settings. For example, you can design one operator template for managers and another template for first-level Service Desk Agents. An operator template is an operator record containing all the common information that applies to operator records created from the template. Typically, this includes information such as:

- Application profile
- Default Company
- Date Information
- Time Limits
- User Session Information
- LDAP Information
- Security Groups
- Security Roles

To distinguish the operator template from a user's operator record, select the **Template Operator** option in the template. Users are not attached to templates and, therefore, cannot log in to HP Service Manager using an operator template.

When you have created the new operator template with all the desired settings, you can then create the operator records you need, based on that new template. When you create operator records, fill in the **Template** field with the name of the template from the operator template, and then all the information in the template will be applied to the new operator records.

Any changes you make to an operator template automatically apply to all operator records you created from the template. If you later decide to change a setting in the template, you modify the template, and then the setting will automatically be applied to all the operator records that use the template.

Create an operator record from an operator template

Applies to User Roles:

System Administrator

Caution: Any changes that you make to an operator template automatically propagate to operator records based on that template. These automatic updates can consume substantial system resources.

To create an operator record from an operator template, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. In the **Login Name** field, type the new operator name.
3. Click the **Security** tab.
4. In the **Template** field, type the login name of the operator record to be used as an operator template.
5. Click **Add**.

Note: Operator record login names are case sensitive.

Note: If an operator record has group1 in its security groups array when its template is NULL and group1 is in the security groups array of template_1 but not in that of template_2, when you assign template_1 to the operator record, the operator record has group1 in its security groups array; however, if you switches its template to template_2, group1 is lost in its security group array. To work around this issue, clear the template field, remove template_1L, save it, change the template to template_2, and then save.

Create an operator template

Applies to User Roles:

System Administrator

System Administrators can design operator templates for creating operator records for users that share common information and settings. For example, you can design one operator template for managers and another template for first-level Service Desk Agents. An operator template is an operator record containing all the common information that applies to operator records created from the template.

To create an operator template, follow these steps:

Note: You can specify as many details in the new operator record template, as necessary.

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Enter the search criteria to find the operator record for which you want to create an operator template.
3. Fill in the necessary information, including application profiles, and proper permissions and settings.
4. In the Security tab, select the option **Template Operator**.
5. Click **Add**.

Note: Because operator templates are also operator records, they are valid log-in accounts for HP Service Manager. To prevent users from using operator templates for log-in access, you can apply a password and log-in restriction to your operator templates.

Define the operator template applied to LDAP users

Applies to User Roles:

System Administrator

To define the operator template applied to LDAP users, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. In the **Operator Template** field, specify the operator record that you want to use as the company default for LDAP users.
3. Click **Save**.

Chapter 4: Process Designer

Process Designer provides a graphical interface to develop workflows that you can use to control the flow of a single record throughout its lifecycle within Service Manager. The Process Designer enables an implementer to graphically create or update a workflow without being an expert in RAD programming.

- Define a workflow process in a graphical editor.
- Create business rules in a user-friendly interface to drive the workflow logic.
- Provide a platform to model complex processes that require branching and looping.
- Lower Total Cost of Ownership of Service Manager by enabling an intuitive and simplified configuration.
- Simplify future upgrades by enabling standardization and clarity of business logic.

Process Designer includes the following components:

- Workflow designer: Design and update a workflow using a graphical user interface.
- Rules editor: Create rules to enforce business logic in workflows and forms.
- Security model: Provide a common role-based security model.

A workflow is a collection of phases with transitions from one phase to another. Each phase represents the state of the workflow linked to a form for data capture.

Transitions

Transitions can connect phases in any manner to create a workflow with many branches and loops back to previous phases. Transitions may be manual, automatic, or default. A manual transition requires the workflow user to make a manual decision to move to the next workflow phase. An automatic transition moves the workflow to another phase based on data in the workflow record. A default transition is a special case that moves the workflow automatically, when no other automatic transition condition applies.

Rule sets

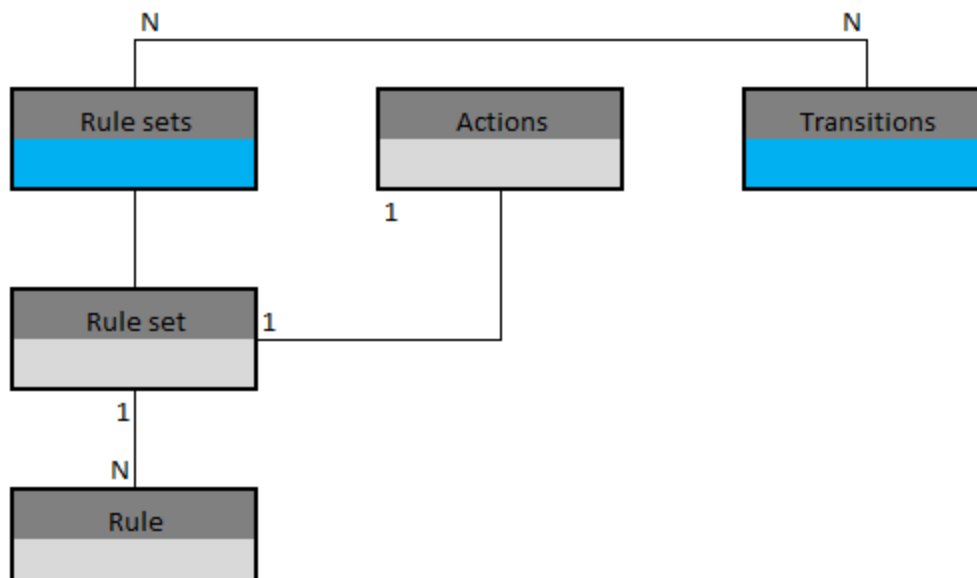
The rules editor enables administrators, such as business process owners, implementers, and developers, to add or remove the out-of-box rules and actions of a workflow to match particular business requirements. You can group individual rules into a rule set to allow their re-use within the

process. You can configure a rule set to execute on events, such as saving or updating a business table record. Rules can also be set up to run on a workflow transition.

Actions

You can also configure rules as actions, which allows operators to run rules on demand rather than wait for workflow processing. When an operator initiates an action (such as pressing a button in the system tray), the system runs the associated rule sets for that phase of the workflow.

The following diagram shows the relationship between rules, rule sets, actions, and transitions:



Condition Editor

With the Condition Editor, you can apply conditions to rules. When a rule condition is met, the rule executes. You can also edit conditions for a rule.

Process Designer security model

The Process Designer security model provides a consistent method of assigning permissions to users across all areas of the system. You can use security model to configure out-of-box rights for a specified role within an area. It also provides standardized methods to manage user rights.

Process Designer modules

Process Designer features are implemented for Knowledge Management, , Change Management, Request Fulfillment, Help Desk (which is comprised of Service Desk, Incident Management, and Problem Management) and Service Level Management. To access the Process Designer features from the system navigator, click **Tailoring > Process Designer**.

A typical Process Designer flow broadly comprises the following major tasks:

- Create rule sets with rules using out-of-the-box rule types to enforce business logic on traditional Service Manager forms.
- Create a workflow with phases and transitions to build a process flow.
- From workflow phases and transitions, associate forms, rule sets, approvals, and alerts to implement your business process.

Create a rule set

Applies to User Roles:

System Administrator

Implementer

A rule set contains a list of rules that you may run against a record. Rules implement business logic to drive a workflow or a process. Rules can help perform calculations, validate fields based on data or rule sets, set required fields, and more. A rule set uses role-based security.

You can re-use rule sets in many processes when you require the same rules in many places. rule sets simplify the effort of implementing business logic. You can apply rule sets based on conditions, or configure them to run during an action. rule sets are most often associated with specific phases of a workflow.

To create a rule set, follow these steps:

1. Click **Tailoring > Process Designer > Rule Sets > New**.
2. Type a unique ID for the rule set. For example, kmdocument_draft.

Note: The name must be unique within the rule sets records.

3. Select **Available as action** if you want to offer this rule set as an action within a workflow phase. For example, HP Service Manager interaction with an external system.
4. Type the display name for the rule set, for example, Saving a draft.
5. Select the table(s) from the Table name list that you want the rule sets to apply to, for example, select kmdocument.

Note: If the list is blank, the rule set can be applied to all tables.

6. Click **Save** to add the rule set.

Note: If you want to edit an HP Proprietary rule set, create a copy of the HP Proprietary rule set. To add Rules to a rule set, you must first save the rule set.

Clone an existing Rule Set

Applies to User Roles:

System Administrator

Implementer

You can create an editable copy of an existing Rule Set by using the cloning option. Cloning a read-only Rule Set marked as HP Proprietary creates an editable copy of the Rule Set.

To clone an existing Rule Set, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search**.
3. Select the Rule Set you want to clone.
4. Click **More > Clone**. A copy of the Rule Sets with both the ID and Name prefixed <CLONE> is displayed.
5. Rename both the ID and Name prefixed <CLONE> fields by typing something unique.
6. Click **Save**.

Adding a rule

A rule defines a singular piece of functionality, such as making a field mandatory. A rule can perform calculations, validate fields based on data or lists, set required fields, and more. Rules can also specify conditions that determine when the rule should execute or who can execute rules run in the order they appear in the rule set. The order can be changed using the **Move Up** and **Move Down** buttons. If there is an error executing a rule, rule processing will stop. It is important to order the rules such that validation

rules come first in the list, and then any rules that will perform actions. For example, to validate data and send an HTML email, place rules to validate data first and then the rule to send an HTML email. If the rules were reversed, the HTML email will be sent with invalid data or an invalid workflow state if the rules are part of a transition.

All rule sets in a phase, except the "On Enter" and "On Exit" rule sets, run before a record proceeds from one phase to another. The "On Exit" rule sets run before a transition occurs. "On Enter" rule sets run when a record moves to that phase.

The "On Exit" rules are the best place for notifications when a record leaves a phase especially when multiple transitions are used or when integration notifications are triggered. Transitions are used to add validations that are required before leaving to the current phase. For example, in a change phase, the start date and end date are entered before proceeding to the Approval phase and no input is required if you are abandoning the change. In this case, if the "On Exit" rules are run before the transition rules, you will be sending out notifications but the actual transition would not have happened. Therefore, the order of execution of rule is Transition > On Exit > On Enter.

For example, rules may run in the following situations:

- When a record enters or exits a specific phase of the workflow
- When a record is created, updated, or deleted in a certain phase of the workflow because a workflow action is invoked
- When a workflow transition occurs
- When a workflow action is invoked

The following rule types are available in out-of-box Service Manager deployments.

Rule type	Description
Assignment	Automatically distribute records (such as tasks or records) to the groups and individuals who are most able to process them
Call a process	Call a Service Manager process record
Case Exchange	Trigger certain activities for the Case Exchange integration
Clear Fields	Clear the specified field and related fields
Field Validation Against a List	Validate a field against a list (global or defined)
Field Validation Against a Table	Validate a field against a different table
JavaScript	Use JavaScript to perform actions and validations

Rule type	Description
Validation	
Launch a Script	Launch a Service Manager script
Launch a URL	Call a URL to launch a web page
Mandatory Fields	Set fields as mandatory
Mandatory Variables	Set variables as mandatory
Popup Message Box	Create and configure popup message boxes that appear to end users
Run Action	Run actions on records that have a specified relationship to the record that triggers the rule
Run JavaScript	Use JavaScript to perform actions and validations
Run Scheduled Action	Run actions on the current record after a specified length of time has passed
Run a Wizard	Run a Service Manager wizard
Send HTML Email	Send an HTML Email to users or a group
Send Notifications	Send Service Manager notifications
Set Field	Set a field value using JavaScript
Set Field from Number	Set field based on a number record
Start or Stop Clock	Start and stop a Service Manager clock
Validate against Table	Validate a field against a field in another table and fill data into other fields
Validate Date	Validate a date against a date range
Validate Text/Number	Validate a field against a range of text or a number in another field of same table

Note:

- You can edit user-defined rules only. You cannot modify the out-of-box rules because they are labeled as HP Proprietary.
- Many rules have a default description that contains tokens. The tokens are replaced with values when you define the rule. For example, the default description of the Set Mandatory

Fields rule is **<fields> are Mandatory**. When you define the rule, the **<fields>** token is replaced by the fields that you select in the rule. You can edit the default description.

- If you do not specify a condition, rules are always triggered to perform the action specified in the rule.

Add a Launch a URL rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to launch a remote web address by using its uniform resource locator (URL). This rule helps you to integrate Service Manager with other products.

To add a Launch a URL rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined Rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Launch a URL**.
4. Type a description in the **Rule Description** field.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. In the **URL** field, type the URL address of the remote resource that you want to launch, and then click **OK**.

Add a Run a Macro rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to run a HP Service Manager macro that executes a distinct action. Service Manager macros are specific actions driven by predefined conditions. For example, if you want to configure a macro to send an email, select the Service Manager macro type **Mail 1 Person**. You can configure this rule to send an email to an intended recipient when an incident record moves from one phase to another.

To add a Run a Macro rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Run a Macro**.
4. Type the description in the **Rule Description** field.
5. Click **Edit** to add a condition.

Note: If you do not specify a condition, it will default to **Always**.

6. Select a macro name from the drop-down list.

Note: The drop-down list has macros related to the current table of the rule set.

7. Click **OK** to add the new rule to the rule set.

Add a Call a Process rule

Applies to User Roles:

System Administrator

Implementer

This rule enables users to call a HP Service Manager process. You have to specify the process name and the conditions that call the process.

Caution: You cannot call a Service Manager process that expects an input, because there is no provision to pass the input through the rule. Calling a process that requires an input causes the rule functionality to fail and may generate an unrecoverable error message.

To add a Call a Process rule type, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Call a Process**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Click **Fill Field Process**, and then select the process that you want to call.
7. Click **OK** to add the new rule to the rule set.

Add a Case Exchange rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to trigger certain activities for the Case Exchange integration.

To add a Case Exchange rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Case Exchange**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. In the rule from the **Instance Name** drop-down list, select the Case Exchange integration instance that you want to apply.
7. In the **Event** drop-down list, select an event from, and then select the fields you want to add.
8. Click **Finish** to add the new rule to the rule set.

Add a Run a Wizard rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to run a HP Service Manager wizard. The form helps you to specify the wizard to run when the rule executes.

To add a Run a Wizard rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Run a Wizard**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Click **Fill Field Wizard to run**, and then select the wizard to run when the rule is executed.
7. Click **OK** to add the new rule to the rule set.

Add a Clear Fields rule

Applies to User Roles:

System Administrator

From a rule set, you can clear the value of specified fields in a record. Optionally, the rule can also clear the value in fields related to the specified fields.

To add a Clear Fields rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Clear Fields**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. In the **Field Name** column, select the fields to clear when the rule is executed.
7. In the **Clear Related Fields** column, select whether to clear the value of related fields of the specified fields.
8. Click **OK** to add the new rule to the rule set.

Add a JavaScript Validation rule

Applies to User Roles:

System Administrator

Implementer

This rule allows you to validate any JavaScript code a user enters.

To add a JavaScript Validation rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **JavaScript Validation**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note:

- If you do not specify a condition, the value defaults to **Always**.
- You may reference the current record as **record** in the JavaScript. For example, if the field in a form is a category, it may be referred to as follows: `record.category=="xyz"`
- You may reference the original copy of the record (before any changes were made by the user) as **oldRecord** in the JavaScript (that is 'oldRecord.category').
- You may set the **returnCode** variable in the JavaScript to specify whether this rule was successful or should be treated as a failed validation. A return code of 0 (zero) is considered successful (it is the default), any other code is unsuccessful. The return code must be a numeric value.

6.

Note:

- If you do not specify a condition, it will default to **Always**.
- You may reference the current record as **record** in the JavaScript. For example, if the field in a form is a category, it may be referred to as follows: `record.category=="xyz"`
- You may reference the original copy of the record (before any changes were made by the user) as **oldRecord** in the JavaScript (that is 'oldRecord.category').
- You may set the **returnCode** variable in the JavaScript to specify whether this rule was successful or should be treated as a failed validation. A return code of 0 (zero) is considered successful (it is the default), any other code is unsuccessful. The return code must be a numeric value.
- You may set the **message** variable in the JavaScript to specify a message that displays to the user if the rule is unsuccessful (returns a non-zero return code).
- You may set the **cursorPosition** variable in the JavaScript to specify a field on the current form where the cursor should be placed if the rule is unsuccessful.

7. Enter the JavaScript in the text box.

8. Click **OK** to add the new rule to the rule set.

Add a Run JavaScript rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to perform actions and validations by using JavaScript.

To add a run JavaScript rule:

1. Click **Tailoring > Process Designer** in the System Navigator.
2. Click **Rule Sets > Search** to open the Rule Set page.
3. Select the Rule Set to which you want to add the rule.
4. Click **Add Rule** to open the Select Rule Type page.
5. Click **Run JavaScript**.
6. Type the Rule Description.
7. Click **Edit** to add a condition.

Note: If you do not specify a condition, it will default to **Always**.

8. Type the JavaScript to run in the text box.
9. Click **OK** to add the rule.

Add a Set Mandatory Fields rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to make one or more fields mandatory and to specify a default value for each field, which will be set if the mandatory fields are empty.

To add a JavaScript Validation rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the

rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Set Mandatory Fields**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select the error message type (**Pop-up** or **Screen**) that is displayed during validation.
7. Click the **Show All Error Messages Together** check box if you want to display all error messages together during validation.
8. Select the field name you want to set as mandatory.
9. You can choose a default value, which will be set if the mandatory fields are empty.
10. Click **OK** to add the new rule to the rule set.

Add a Set Mandatory Variables rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to set global and thread variables as mandatory. If mandatory variables are empty, then a default value is set if specified in the Rule.

Global or thread variables begin with the \$ symbol. However, the rule does not accept local variables beginning with \$. Global variables are set when the operator logs on and the server automatically cleans them up when the session ends.

Thread variables do not have a consistent naming scheme. They are only valid for the current RAD thread. If the RAD thread terminates, the server automatically cleans up all thread variables.

To add a Mandatory Variables rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Set Mandatory Variables**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select the error message type (**Pop-up** or **Screen**) that is displayed during validation.
7. Click the **Show All Error Messages Together** check box if you want to display all error messages together during validation.
8. Select a global or thread variable.

Note: If a mandatory variable is empty, then the rule sets it to a default value.

9. Type the variable of the default value.
10. Click **OK** to add the new rule to the rule set.

Add a Send Notifications rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to send notifications using a HP Service Manager notification record. The rule is typically mapped to a workflow or workflow phase. For example, you can use the rule to send a notification when a phase is entered. The rule type links to an existing notification record.

To configure a notification, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Send Notifications**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Click **Fill Field Notification Name**, and then select the existing notification record that you want to send when this rule is executed.
7. Click **OK** to add the new rule to the rule set.

Add a Launch a Script rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to launch a Service Manager script. Scripts enable you to interrupt the normal screen flow and gather the prerequisites before the form is displayed. For example, you can use a script to automatically close an incident in five days. The script closes the incident.

To add a Launch a Script rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Launch a Script**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Click the **Fill Field Script** icon in the **Script text** box to select a Service Manager script.

Note: If you type an invalid script name, an error message appears.

7. Click **OK** to add the new rule to the rule set.

Add a Send HTML Email rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to send a formatted HTML email to intended recipients using pre-configured HTML templates. Recipients can be particular users or a group, either explicitly named or based on data in the form. This rule is used to send emails at specific points in a workflow as opposed to create a general Service Manager notification outside of Process Designer that, for example, would apply for all Change Requests.

To add a Send HTML Email rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP

Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Send HTML Email**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. In the **HTML Template** field, enter an HTML template.
7. Select one of the four recipient options: **Users**, **Group**, **Set Using JavaScript**, or **Current Record**. Then, follow the appropriate steps to configure the recipient:
 - **Users:** Select a user type (**Operators** or **Contacts**), and then select the operators or contacts accordingly.
 - **Group:** Select one of the following group types: **Assignment Group** (assignment), **Change Management Group** (cm3groups), **Knowledge Management Group** (kmggroup), or **Request Management Group** (ocmggroups). Then, follow the appropriate steps to configure the group:
 - **Assignment Group:** Enter a group name in the **Group** field, and then select **Operators**, **Manager**, or **All** in the **Send To** drop-down list.
 - **Change Management Group:** Enter the group name in the **Group** field, and then select **Members**, **Approvers**, or **All** in the **Send To** drop-down list.
 - **Knowledge Management Group:** Enter the group name in the **Group** field, and then select **Operators**, **Manager**, or **All** in the **Send To** drop-down.
 - **Request Management Group:** Enter the group name in the **Group** field. Also, select **Operators**, **Manager**, or **All** in the **Send To** drop-down list.
 - **Set Using JavaScript:** In the script field that appears, set the recipients in the **users** array variable by using valid operator login names or contact names. For example, you type the following:

```
var users = new Array ();  
users [0] = "jennifer";
```

- **Current Record:** Choose a field from the current record, and then specify if the field is the ID of an operator, contact, assignment, cm3groups, kmgroup, or ocmgroup in the **Field Type** drop-down list.

If you select any field type apart from **Operator** or **Contact**, you have to select from **Send To** field. For example, if you select **Assignment Group**, you have to select **Operators, Manager**, or **All** from the **Send To** drop-down list.

8. Click **OK** to add the new rule to the rule set.

Add a Start or Stop Clock rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to start or stop an HP Service Manager clock to measure elapsed time. For example, if you want to know the time taken for an incident record to move from the Validation phase to the Risk and Impact Analysis phase, configure a rule to start a clock when the record enters the Validation phase. Then, configure another rule to stop the same clock when the incident record moves to the Risk and Impact Analysis phase. The time difference is stored in the clocks table along with start and stop times.

To add a Start or Stop Clock rule to start a clock, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Start or Stop Clock**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select **Start Clock**, and then click **Next**.
7. In the **Name of Clock** pane, choose one of the following methods to define the clock name:
 - Select the **Fixed Name** option to identify a specific clock. Type a clock name to add a new clock, or select an existing clock name from the drop-down list.
 - Select the **Set Using JavaScript** option to set a clock name by using a JavaScript. The following is an example of setting a clock by using a JavaScript:

```
clockName = "New Clock";
```

8. In the **Use this schedule** pane, select a predefined schedule or configure a schedule by using a JavaScript.
9. In the **Using this time zone** pane, select the time zone that the clock uses. Options include the location of the system server, technician, customer, or CI. You can also enter a fixed value (a specific time zone) or configure the time zone by using a JavaScript.
10. Click **Finish** to add the new rule to the rule set.

Once that you have created a rule to start a clock, you can add another rule to stop the clock. To do this, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.
3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Start or Stop Clock**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select **Stop Clock**, and then click **Next**.

7. In the **Name of Clock** pane, choose one of the following methods to define the clock name:
 - Select the **Fixed Name** option to identify a specific clock. Type a clock name to add a new clock, or select an existing clock name from the drop-down list.
 - Select the **Set Using JavaScript** option to set a clock name by using a JavaScript.

Note: The name of the stop clock rule should be the same as the corresponding start clock rule.

8. Click **Finish** to update the rule.

Add a Set Field rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to set a field with a value that is determined by a JavaScript. From a rule set, you can select a common field from multiple tables and set its value based on a JavaScript expression.

Note: Make sure that the field is set to the contents of the **value** variable. If it is not set to the **value** variable, the JavaScript cannot be processed.

To configure a field based on a JavaScript, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Set a Field**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select an applicable field name from the drop-down list.
7. Type the JavaScript that sets the variable **value** to the desired value for the field in the text box.
8. Click **OK** to add the new rule to the rule set.

Add a Set Field from Number rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to set a field based on an HP Service Manager number record. When this rule is executed, unique sequential numbers for the records in the database are generated.

When a new record is added, the unique sequential number is incremented or decremented based on the prefix or suffix provided. For example, you can create a number record for the cm3r class with **Increment By** as **+1**, **Prefix** as **C**, and **Last Number** as **10**. Whenever a new change request is added in the system, it assigns the change request with a unique change ID C10, the next change request you add will have the change ID C11.

To add a Set Field from Number rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Set Field from Number**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select the field from the **Field Name** drop-down list.
7. Select the class from the **Class of Number Record** drop-down list.

Note: You can select the **Overwrite When Record Is Saved** check box to overwrite the number when you save a record.

8. Click **OK** to add the new rule to the rule set.

Add a Validate Date rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to validate a date field against an absolute date or a range of relative dates. For example, you can add a rule to validate whether a document expiration date is greater than or equal to the document creation date.

To add a Validate Date rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Validate Date**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select the error message type: **Pop-up** or **Screen** to display during validation.
7. Select the field to validate from the drop-down list.

Note: The drop-down list displays all fields with the Date data type from the current table.

8. Select the comparison operator from the drop-down list.
9. Select the **Not** option if you want to negate the comparison.
10. Click **Relative Date/Time** or **Absolute Date/Time** to validate against date field.

Note:

- If you select **Relative Date/Time**, select a date field or Current Date/Time from the drop-down list.
- An offset time of days, hours, and minutes can be added or subtracted from the relative date/time by selecting **+** or **-**. For instance, an offset of **+04:03:02** indicates the relative date/time is ahead by 4 days, 3 hours, and 2 minutes.
- If you select **Absolute Date/Time**, click the **Calendar** icon to select the date and time.

11. Click **OK** to add the new rule to the rule set.

Add a Field Validation against a List rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to select a field to validate against a list of values. This list may be global or manually defined.

To add a Field Validation against a List rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Validate against List**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select **Pop-up** or **Screen** to set the type of error message that is displayed during validation.
7. In the **Field to Validate** drop-down list, select the field to validate.
 - If you select **Global List**, select the global list from the drop-down list.
 - If you select **Manual List**, type the manual list names in the Value table.
8. Click **OK** to add the new rule to the rule set.

Note: If the field value does not match a value in the specified list, the system displays a message and sets the cursor to that field when the rule is not followed.

Add a Validate against Table rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to validate a field against a field in another table and fill data into other fields. You can also filter the data you are validating against, and fill data into other fields.

Note: If the field value does not match a value in the specified table, the system displays a pop-up

message and sets the cursor to that field when the rule is not followed.

To add a Validate against Table rule:

1. Click **Tailoring > Process Designer**.
2. Click **Rule Sets > Search**.
3. Select the Rule Set to which you want to add the rule.
4. Click **Add Rule** to open the Select Rule Type page.
5. Click **Validate against Table**.
6. Type the Rule Description.
7. Click **Edit** to add a condition.

Note: If you do not specify a condition, it will default to **Always**.

8. Select the error message type: **Pop-up** or **Screen** to display during validation.
9. Select the field to validate from the drop-down list.
10. Select the name of the table you want to validate against.
11. Select the name of the field you want to validate against.
12. You can filter the data you are validating against using a standard RAD query.

For Example: The following field entries will validate only for cm3r with the current field name (Demo String2 in this example) of the workflow:

Current Field Name field: **Demo String2**

Validate Against Table field: **ModuleStatus**

Validate Against Field field: **Status**

Filter field: **module="cm3r"**

13. Click **Here to Add Fill Information** to enter Fill From and Fill To fields.

Note: The **Fill From** field represents the fields of the validation table against which it validates. The **Fill To** field represents the fields in the current table being validated.

14. (Optional) If you want the field to be validated whether its value changes or not, select the **Always Check Validity** check box.

If this option is not selected, the system validates the field only when its value changes.

15. Click **OK** to add the rule.

Add a Validate Text/Number rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to validate a field against a range of text or a number in another field of same table. You can define fixed values or select a field from the current table to validate against a field. For example, the field to validate is **Demo Number**, field to validate against is **Demo String 1**, and the comparison operator is **Is greater than or equal to**.

Note: If the field to validate against is blank, the rule is ignored. If you need to enforce the rule, then use a Set Mandatory Fields rule on the field you need to validate against.

To add a Validate Text/Number rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Validate Text/Number**.
4. In the **Rule Description** field, type a description of your new rule.

5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select **Pop-up** or **Screen** to set the type of error message that is displayed during validation.
7. Select the field to validate from the drop-down list.
8. Select the comparison operator from the drop-down list.
9. Select the **Not** check box if you want to negate the comparison.
10. To validate against a field or manually defined value, follow the appropriate steps:
 - To validate against a field, select **Field** under **Values**, and then select the field you want to validate against from the drop-down list.
 - To validate against a manually defined value, select **Custom** under **Values**, and then type the value to validate against the selected field. For example, to validate whether the “Risk Assessment” value is between 1 and 5, select the **Is between** comparison operator, and then type 1 and 5 in the **Custom** text box.
11. Click **OK** to add the new rule to the rule set.

Add a Field Validation against a Table rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to validate a field against a field in another table and fill data into other fields. You can also filter the data you are validating against, and fill data into other fields.

Note: If the field value does not match a value in the specified table, the system displays a message and sets the cursor to that field when the rule is not followed.

To add a Field Validation against a Table rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Validate Against Table**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select the field to validate from the drop-down list.
7. Select the name of the table you want to validate against.
8. Select the name of the field you want to validate against.
9. You can filter the data that you are validating against by using a standard RAD query.

For example, the following field entries will validate only for cm3r with the current field name ("Demo String2," in this example) of the workflow:

Current Field Name field: **Demo String2**

Validate Against Table field: **ModuleStatus**

Validate Against Field field: **Status**

Filter field: **module="cm3r"**

10. Click **Click Here to Add Fill Information** to enter Fill From and Fill To fields.

Note: The **Fill From** field represents the fields of the validation table against which it validates. The **Fill To** field represents the fields in the current table being validated.

11. Click **OK** to add the new rule to the rule set.

Add a Popup Message Box rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to create and configure popup message boxes that appear to end users.

To add a Popup Message Box rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Popup Message Box**.
4. In the **Rule Description** field, type a description of your new rule.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. In the **Using this message** section, select whether you want to set a fixed message or to configure the message text by using a JavaScript. Then, enter the message or JavaScript in the relevant text box.

Note: If you select a fixed message, you can additionally enter localized versions of the message. If you select to set the message text by using a JavaScript, the JavaScript implementation handles the message localization.

To localize a fixed message, first save the rule, and then open it for editing. An **Edit localized labels** button is now displayed next to the **Fixed Message** field. Click the button to configure the language code, message ID, and text of the localized message.

7. Select the message box type. The following options are available:

- **Ok only**

This type of message box provides end users with the option to click "Ok" only. When you select this rule type, you must select the message level and set the behavior when the user clicks "Ok."

- **Yes, No**

This type of message box provides end users with the option to click "Yes" or "No." When you select this rule type, you must set the behavior when the user clicks "Yes" or "No."

- **Yes, No, Cancel**

This type of message box provides end users with the option to click "Yes," "No," or "Cancel." When you select this rule type, you must set the behavior when the user clicks "Yes," "No," or "Cancel."

8. Click **OK** to add the new rule to the rule set.

Add an Assignment rule

Applies to User Roles:

System Administrator

Implementer

This rule enables you to automatically distribute records (such as tasks or records) to the groups and assignees who are most able to process them.

To add an Assignment rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Assignment**.

4. Type a description in the **Rule Description** field.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select one of the following assignment types:
 - **Automatic - take first:** Service Manager automatically assigns the record to the first group or assignee that is identified in the **Group Assignment** and **Individual Assignment** panes (see step 7 and step 8).
 - **Manual - let the user choose:** Service Manager presents a list of potential assignment groups and assignees to the user who has triggered the rule.
7. In the **Group Assignment** pane, configure the group to whom the record is assigned when the rule is triggered (that is, the value that is inserted into the field which you specified in the **Group Field Name** field). To do this, follow these steps:
 - a. In the **Group Field Name** field, enter the name of the field in which the name of the group that you want to assign the records to is stored.
 - b. In the **Default Group** field, enter the group to which the record is assigned if the remaining rules do not return a specific group.
 - c. Select one of the following options to configure the assignment rule:
 - **Service Based:** Returns the groups that are defined in a specified service
 - **Fixed:** Automatically inserts a fixed value into the field that you specified in the **Group Field Name** field
 - **Set Using JavaScript:** Determines the group to whom the record is assigned based on a JavaScript
8. In the **Individual Assignment** pane, configure the assignee to whom the record is assigned when the rule is triggered.

Note: Assigning tasks or records to specific assignees is optional. If you want to assign records to a group only, select the **None** option.

To do this, follow these steps:

- a. select one of the following options to configure the assignment rule:
 - **Assign To Group Member:** Automatically assigns the record to a member of the configured group. Records can be assigned on a round robin basis or to the assignee who is currently assigned the lowest number of records.
 - If you select the **Round robin** option, enter the field in which the time used for the calculation is stored in the **Assignment Time Field Name** field. Then, select the number of days that are taken into consideration when the assignment is calculated. The default value is 60 days.
 - If you select the **Number of Assigned Tickets** option, click **Edit Query** to open the condition editor and create the filter that determines the assignee.
 - **Assign To Coordinator:** Assigns the record to a coordinator of your choice in the specified group
 - **Fixed:** Automatically inserts a fixed value into the field that you specified in the **Assignee Field Name** field
 - **Set Using JavaScript:** Determines the assignee to whom the record is assigned based on a JavaScript
- b. In the **Assignee Field Name** drop-down list, select the field in which the name of the assignee to whom you want to assign the record is stored.

9. Click **OK** to add the new rule to the rule set.

Add a Run Action rule

Applies to User Roles:

System Administrator

Implementer

This rule automatically runs actions (defined by rule sets and/or backend transitions) on records that have a specified relationship to the record that triggers the rule. For example, you can use this rule to change the workflow phase of related records under specific conditions.

To add a Run Action rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Run Action**.
4. Type a description in the **Rule Description** field.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

6. Select the type of record on which you want to run the action.
 - Select **Related Records** to change the workflow status of records related to the record that triggers the rule.
 - Select **Other Records** to change the workflow status of records that have a relationship with the current record that is built by a manually-defined query string.
 - Select **Current Record** to change the workflow status of the record that triggers the rule.

Note: This option enables you to run a backend transition directly on the current record.

7. Configure the relationship between the records on which you want to run the action and the record that triggers the rule.
 - If you selected the **Related Records** option, select a relationship type from the **Relation Type** drop-down list.
 - If you selected the **Other Records** option, select a table from the **Table Name** drop-down list.
 - If you selected the **Current Record** option, there is no need to define a relationship.
8. Click **Edit Query** if you want to define a subset of the related records on which the actions will be

run.

Note:

- If you select the **Other records** option but do not specify a query, no records are queried. This prevents the rule from running the action on every record in the defined table.
- This step does not apply if you selected to run the actions on the current record only.
- The Query Editor widget functions similarly to the Condition Editor. However, note the following differences:
 - In the left-hand side (LHS) of the query, you can only select a field in the record on which you want to run the action. Cross table fields are not supported.
 - Only the following data types are supported on the right-hand side of the query:
 - Blank/Nul
 - Value
 - Variable
 - Current Record
 - Saved Record

9. In the **Run Rule Set** field, select the rule set that is applied to the target records when this rule is triggered.
10. In the **Action after Rule Set** field, select the action that is performed on the target records after the rule set is applied. You can select to do nothing, save the record, or apply a backend transition. The list of available backend transitions is retrieved from the workflows of the target record's table name (depending on the Relation Type that you selected).
11. Click **OK** to add the new rule to the rule set.

Note: This rule does not take locked records into account. If a record is locked when the rule is run, the action is not automatically rescheduled.

Add a Run Scheduled Action rule

Applies to User Roles:

System Administrator

Implementer

This rule automatically runs an action (defined by rule sets and/or backend transitions) on records after a specified length of time has passed. For example, you can use this rule to automatically close incident records that have been in a Resolved state for a certain number of days.

To add a Run Scheduled Action rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then click **Run Scheduled Action**.
4. Type a description in the **Rule Description** field.
5. Click **Edit** to add conditions to the rule.

Note: If you do not specify a condition, the value defaults to **Always**.

When these conditions are met, a schedule instance is created and monitored by a backend scheduler.

6. Select one of the following options to set the calculation method of the schedule instance:
 - **Use field in record + interval:** Enables you to configure when the rule is triggered by setting a time and an interval. To do this, you must specify a field in a record (to set the time) and a length of time (to set the interval). Enter the interval time in the **Calc Interval** field, and use the following time format:
 - ddd hh:mm:ss

Note: This option supports negative intervals. That is, you can specify the length of time before a time that is set in a field.

- **Use javascript to set variable actionExecutionTime:** Enables you to use a JavaScript to set the time when the backend schedule is executed.
- 7. Click **Edit** to set a further set of conditions that are applied once the time that is defined in the schedule instance is reached.
- 8. In the **Run Rule Set** field, select the rule set that is applied to the current records when the backend schedule is executed.
- 9. In the **Action after Rule Set** field, select the action that is performed on the current records after the rule set is applied. You can select to do nothing, save the record, or apply a backend transition. The list of available backend transitions is retrieved from the workflows of the current record's table name.
- 10. Click **OK** to add the new rule to the rule set.

Note: This rule takes locked records into account. If a record is locked when the rule is run, the action is automatically rescheduled.

Caution: A scheduled action is triggered based on the interval that is configured in the rule. If a user manually updates a field that the scheduled action will update later, the user's update will be overwritten by the scheduled action. For example, the `im.schedule.unlinkAllChild` Rule Set defines a scheduled action that will clear the Parent Incident field of all child incidents. If you click **Unlink All** in a parent incident, this scheduled action is triggered; before the scheduled action is completed, if a user manually changes the Parent Incident value of a child incident, the user's update will be cleared later.

Group rules

Applies to User Roles:

System Administrator

Implementer

You can group multiple rules into a rule group with an overall condition. The system runs all the rules in the rule group if the condition matches.

To group rules, follow these steps:

1. Click **Tailoring > Process Designer**.
2. Click **Rule Sets > Search** to open the **Rule Set** form.
3. Select the rule set to which you want to add a group, and then click **Add Group**.
4. Type a rule group name. For example, `kmrules`.
5. Click **Edit** to add a condition.

Note: If you do not enter a condition, it will default to **Always**

6. Click **OK** to add the group name.
7. Highlight the group by selecting it.
8. Click **Add Rule**.
9. Select a rule.
10. Type the attributes in the Rule form.
11. Repeat steps 8 to 11 if you want to add more rules.
12. Click **OK** to create the rule group.

Note: You can add one or more rule groups within another rule group.

Using the Condition Editor

The HP Service Manager Condition Editor enables you to build a condition or set of conditions without any programming language knowledge. Conditions always evaluate to True or False. When a condition evaluates to True, the system runs the rule or applies an action that the condition controls. For example, you can use conditions to determine if a workflow transition should occur or if a rule should be executed.

A condition item is an expression built from fields, operators, and values. A condition item has a Left-Hand-Side (LHS) and a Right-Hand-Side (RHS), which are separated by an operator. There can be a combination of variables, types, and values on either side of the condition item. The Condition Editor

uses a tabular format in which you populate each element of the condition item (RHS, LHS, and operator) by using a series of drop-down lists.

You can also build complex conditions with the Condition Editor. Complex conditions are composed of groups of condition items that are connected by logical operators.

After you build a condition, HP Service Manager displays it in a user-readable form, such as the following example:

```
((description in Category = 100 OR display.name in Category = "Test") AND
((assoc.published.doc in CurrentFile
!=true AND activity.mandatory.msg in Object <=20) OR error in SavedFile Starts
With 101 OR ((the
"edit.adaptive.learning" value in the "Knowledge Document" Security Area <= 123 AND
the "update" value in the
"Tailoring" Security Area = "always") OR test!=12)))
```

You can use the Condition Editor to perform the following tasks:

- Build a condition

For more information, see ["Build a condition" on page 80](#).

- Create a group of condition items

For more information, see ["Create a group of condition items" on page 85](#)

- Edit a condition

To do this, open the Condition Editor and click on the condition item that you want to edit. You can then edit the existing values.

- Delete a condition item or group of condition items

To do this, open the Condition Editor, and then click the Delete Condition icon (-) beside the condition item or group of condition items that you want to delete.

- Clear all condition items and groups

To do this, open the Condition Editor, click the More Actions icon (...), and then click **Clear**.

Launch the Condition Editor from a rule

Applies to User Roles:

System Administrator

Implementer

The Condition Editor enables you to build a condition without any programming language knowledge.

Note: You can launch the Condition Editor in the web client only.

To launch Condition Editor from a new rule, follow these steps:

1. In the System Navigator, click **Tailoring > Process Designer > Rule Sets**.
2. Click **Search** to open the **Rule Set** form, and then select the rule set to which you want to add the rule.

Note: You can edit user-defined Rule sets only. Out-of-box rule sets are labeled as HP Proprietary and cannot be modified.

3. Click **Add Rule** to open the **Select Rule Type** page, and then select the type of rule that you want to open.
4. Type a description in the **Rule Description** field.
5. Click **Edit** to open the Condition Editor and add conditions to the rule.

Launch the Condition Editor from a workflow

Applies to User Roles:

System Administrator

Implementer

The Condition Editor enables you to build a condition without any programming language knowledge.

Note: You can launch the Condition Editor in the web client only.

To launch the Condition Editor from a workflow, follow these steps:

1. Click **Process Designer** > **Workflows** in the System Navigator.
2. Select an existing workflow or create a new workflow.
3. You can launch the Condition Editor from workflow phases and workflows transitions.
 - To launch the Condition Editor from a phase, select a phase, and then use one of the following methods:
 - In the **Details** tab, click the **Form Edit Condition** field.
 - In the **Actions** tab, click **Add**, and then click the **Action Condition** field.
 - In the **Approvals** tab, click the **Reset Condition** or **Recalculate Condition** field.
 - In the **Alerts** tab, click the **Reset Condition** or **Recalculate Condition** field.
 - To launch the Condition Editor from a transition, select a transition, and then click the **Condition** field in the **Details** tab.

Note: To close the Condition Editor, click **Cancel**.

Build a condition

Applies to User Roles:

System Administrator

Implementer

A condition has a Left-Hand-Side (LHS) and a Right-Hand-Side (RHS) that are separated by an operator. There can be a combination of variables, types, and values on either side of the condition.

Note: The data type in the RHS must match the data type in the LHS. For example, if you select a field that has a Boolean data type in the LHS, you must select a matching Boolean field in the RHS. Service Manager automatically validates the data types in conditions. If you do not enter matching

data types, an error message is displayed in the appropriate drop-down list, and you cannot save the condition until you correct the issue.

If you decide to choose a value rather than a field in the RHS, Service Manager provides you with the option to type or select a value that is the same data type as the field in the LHS.

To build a condition, follow these steps:

1. Open the Condition Editor.

For example, click **Edit** in the **Condition** field to open the Condition Editor when you create or edit a rule.

2. Select the logical operator for the conditions. The following operators are available:

- **Match all** (this option corresponds to an AND operator)
- **Match any** (this option corresponds to an OR operator)
- **Not match all** (this option corresponds to negating all conditions)
- **Not match any** (this option corresponds to negating any of the specified conditions)

Match all is selected by default. To select another operator, click **Match all** to display the other operators, and then select another operator.

3. In the left-most drop-down list, select a data type for the LHS. The following table describes the available data types for the LHS.

Field	Description
Category	<p>A field in the associated category definition of the current record</p> <p>Note: Only displayed when the category table is defined in the object record.</p>
CurrentRecord	A field in the name of the current record
CurrentRecord Authorization	<p>A field in the name of the current record</p> <p>Note: Only listed in the condition editor in the workflow editor.</p>

Field	Description
CurrentWorkflowPhase	A field in the associated workflow phase definition of the current workflow
Object	A field in the Object definition of the current record
Phase	<p>A field in the associated phase definition of the current record</p> <p>Note: Only displayed when the phase table is defined in the object record.</p>
SavedRecord	A field in the original copy of the current record (before the user made any changes)
SavedWorkflowPhase	A field in the associated workflow phase definition of the original copy of the current workflow (before the user made any changes)
RAD Expression	<p>Evaluates a RAD expression typed in the text area. For example:</p> <pre>evaluate(cls.control in \$L.phase) and evaluate (\$L.tableAccess.delete) and open in \$L.file=true and nullsub(\$G.ess, false)=false and approval.status in \$L.file="approved" and (category in \$L.file~="KM Document" or category in \$L.file="KM Document"</pre> <p>Note: You cannot combine this condition with any other type of condition. Therefore, once you enter a RAD expression, click Done to build the condition. You can ignore all remaining steps.</p>
Security	An operator's security rights. You can choose rights from the drop-down list of defined values, such as: Change, Change Management Configuration, Change Tasks, Knowledge Management, Knowledge Administration, Security, or Tailoring.
UserOption	<p>A user-selectable option for a Service Catalog item</p> <p>Note:</p> <ul style="list-style-type: none"> You must type the name of the user option. The User Options field only supports string and boolean values.
Variable	Evaluates the value of a global, local, or thread variable condition. For example:

Field	Description
	\$G.test
	\$L.testNumber

4. Select the field for comparison.

Note:

- If a "one to one" or "many to one" cross table relationship is defined for a field, the cross table fields are available for selection in a second-level drop-down list. If relationships are defined with more than one field in the same table, the second-level drop-down enables you to specify the relationship, and a third-level drop-down list enables you to select the field.
- To quickly navigate to a field, move the focus to the field drop-down list, and then type the name of the desired field. To quickly navigate to a field in a second-level list, move the focus to the first-level item in the drop-down list, and then type the name of the desired field.

5. Select an operator. The following operators are available:

- **Equals**
- **Not Equals**
- **Greater Than**
- **Greater Than or Equals**
- **Less Than**
- **Less Than or Equals**
- **Starts With**

Note: For Boolean conditions that evaluate to !=true, you can use the following RAD expression:

```
( nullsub(Boolean in $L.file,false) != true)
```

6. Select a value type for the RHS. The following table describes the available value types for the RHS.

Field	Description
Blank/NULL	A blank or null value
Category	A field in the associated category definition of the current record
CurrentUser	The user currently logged in to Service Manager
CurrentRecord	A field in the name of the current record
CurrentWorkflowPhase	A field in the associated workflow phase definition of the current workflow
Object	A field in the Object definition of the current record
Phase	A field in the associated phase definition of the current record
SavedRecord	A field in the original copy of the current record (before the user made any changes)
SavedWorkflowPhase	A field in the associated workflow phase definition of the original copy of the current workflow (before the user made any changes)
Security	<p>An operator's security rights. You can choose rights from the drop-down list of defined values, such as: Change, Change Management Configuration, Change Tasks, Knowledge Management, Knowledge Administration, Security, or Tailoring.</p> <p>Note: The Knowledge Management value is displayed as "Knowledge Document" in the back-end RDBMS and after you build the condition.</p>
UserOption	<p>A user-selectable option for a Service Catalog item</p> <p>Note:</p> <ul style="list-style-type: none"> You must type the name of the user option. The User Options field only supports string and boolean values.
Value	<p>Allows you to type a value that is appropriate for the data type on the LHS.</p> <p>Note: If a Global List is defined for the field that you specified on the LHS, a drop-down list of values is available for selection on the</p>

Field	Description
	RHS. These values are defined in the Value List field of the Global List.
Variable	Evaluates the value of a global, local, or thread variable condition.

7. Select the field for comparison.

Note: To quickly navigate to a field, move the focus to the field drop-down list, and then type the caption of the desired field. To quickly navigate to a field in a second-level list, move the focus to the first-level item in the drop-down list, and then type the caption of the desired field.

8. Click **Done** to create the condition. Once you add a condition, Service Manager displays a user readable version.

Note:

- To edit an existing condition, open the condition by using the Condition Editor, and then click anywhere in the Condition Editor to enable editing.
- To delete an existing condition, click the Delete Condition icon (-) beside the condition that you want to delete.
- To cancel the creation of a condition, click **Cancel** to exit the Condition Editor.

Create a group of condition items

Applies to User Roles:

System Administrator

Implementer

You can create complex conditions by grouping condition items. A separate logical operator applies to each group. You can add child and sibling groups to a complex condition.

To add a group of condition items, click the Add Condition Group icon in the Condition Editor. To add a child group of condition items, click the Add Condition Group icon in the parent group.

To remove a group of condition items, click the Delete Condition icon (-) in the group.

Note: This action deletes all condition items within the group.

You can easily edit complex conditions by dragging groups and condition items. You can drag a condition item into any group within the complex condition. You can drag a group into any other group, apart from its own child.

Copy a condition

Applies to User Roles:

System Administrator

Implementer

You can copy and paste conditions between Condition Editors. This saves you time if you have a complex condition that you need to use multiple times within your environment.

To copy a condition, follow these steps:

1. Open the Condition Editor in the rule or workflow that contains the condition that you want to copy.
2. Click the More Actions icon (...), and then select **Copy**.
3. Close the Condition Editor, and then open the Condition Editor in the rule or workflow in which you want to paste the condition.
4. Click the More Actions icon (...), and then select **Paste** to copy the condition into the rule or workflow.

Note: You can copy whole conditions only. You cannot copy the individual simple conditions or groups of conditions that comprise a complex condition.

Enable deprecated fields and system fields in the Condition Editor

User Roles: System Administrator

A deprecated field is a field that is assigned the `Deprecated` usage type in the data policy. A system field is a field that is assigned the `System` data type in the data policy.

To display deprecated fields and system fields in the Condition Editor, follow these steps:

1. Click **Tailoring > Process Designer > Configuration > Settings** to display the Condition Editor Settings screen.
2. Select the **Display Deprecated Fields in Current Record** check box if you want to display deprecated fields in Current Record. This option is selected by default.
3. Select the **Display System Fields in Current Record** check box if you want to display system fields in Current Record. This option is selected by default.
4. Click **Save**.

The selected field types will now appear in the drop-down lists in the Condition Editor.

Task Planner

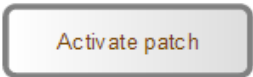
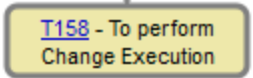
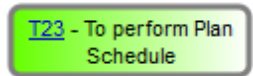
Task Planner enables you to schedule tasks in HP Service Manager modules such as Change Management and Request Fulfillment.

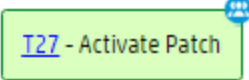
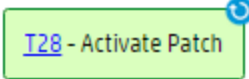

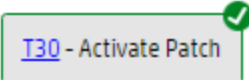
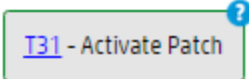
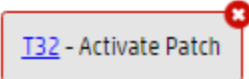
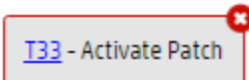
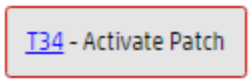
Task Planner graphical interface

Task Planner graphical interface supports panning and zooming.

- To zoom in or zoom out Task Planner graphical interface, click **Zoom in** or **Zoom out** in the toolbar.
- To reposition the workflow within the graphical interface, move the outline box at the top right of the graphical interface, or click and drag the workflow background.

The following table describes the various statuses of a task and their appearance in the graphical interface.

Task status	Graphic style	Remarks
0-Waiting		
0-Planned (opened)		This style appears when a task is created but still in Planned status because it is dependent on another task.
1-Ready		

Task status	Graphic style	Remarks
2-Assigned		
3-In Progress		
4-Blocked		
20-Completed		
21-Completed with problem		
30-Canceled		
31-Withdrawn		
32-Failed		

Plan a task with Task Planner

Applies to User Roles:

System Administrator

Implementer

You can use Task Planner to plan tasks for current or future phases of records that support tasks.

To plan a task by using Task Planner, follow these steps:

1. Open the record for which you want to plan a task.

For example, click **Change Management** > **Change Queue**, and then select a Change record from the queue. Or, click **Request Fulfillment** > **Search Requests**, enter your search criteria, and then click **Search**.

2. Click the **Tasks** tab in the record, and then click **Edit** in the Planned Tasks pane to open Task Planner.

Note: If you open Task Planner before a record is created (that is, a new record that you have not yet saved) or after a record is closed, Task Planner is read-only. In this situation, the **Add Task** and **Save** buttons are invisible.

3. Click **Add Task**, and then do the following:

- a. Type the task title in the **Description** text box.
- b. Select task category from the **Task Category** drop-down list.
- c. Select a phase to start the task from the **Open In Phase** drop-down list.

Note:

- If you plan a large number of tasks for a single phase in a workflow, you may experience slow performance. Therefore, we recommend that you do not create more than ten tasks that start in the same phase.
- If the start phase in the task is the same as the current phase of the parent record, the task is created with a task number assigned. Otherwise, the task remains in the planned status until the parent record reaches the start phase (the "open in" phase) defined for this task.

- d. Select a phase to end the task from the **Close By Phase** drop-down list.

Note: The end phase must be no earlier than the start phase. If left blank, the end phase matches the start phase.

4. To add another task, click **Add Task**. To add a dependent task, hover the mouse on an existing task until you see a hand symbol, and then drag the mouse pointer to add the new sequential task.

5. Click **Save** to save the planned tasks.

Note:

- After you finish adding tasks, you can click **Auto Layout** to automatically arrange the tasks and dependencies in the workflow.
- Once the task record is created, you cannot delete the task or modify its properties in Task Planner. You can click the task number in the graphical interface to modify the details of a created task record.
- The **Mark as required/Set properties as read-only in change** field can only be set for tasks that are defined in Task Planner in the change model and request model. These fields are read-only in Task Planner, and are displayed for your reference.
- If a task is not marked as required in a change model or request model and has not been created, you can modify the properties of this planned task, or you can click **Delete** to remove the task. However, you cannot move the "open in" phase of a planned task to a phase prior to the current phase of the record.

Setting the input and output data in Task Planner

The Input and Output fields in Task Planner enable you to configure the information that is pulled from the parent record into a task record, or pushed from the task record to the parent record.

Task Planner shares the following types of information between the parent and task records:

- Values in fields in the parent record
- User options
- Additional properties

Information that is pulled into the task record from the parent record ("input") is displayed in a read-only field in the **Additional Properties** tab of the task record. If you configure "output" (information that is pushed from the task record to the parent record), an editable field is displayed in the **Additional Properties** tab of the task record. Values that you enter into this field are shared with the parent record.

To configure the input and output of planned tasks, follow these steps:

1. Open the record for which you want to plan a task.

For example, click **Change Management > Change Queue**, and then select a Change record from the queue. Or, click **Request Fulfillment > Search Requests**, enter your search criteria, and then click **Search**.

2. Click the **Tasks** tab in the record, and then click **Edit** in the Planned Tasks pane to open Task Planner.
3. Select the task for which you want to configure input or output, and then open the **Input-Output** tab.

Note: You cannot configure the input and output of active tasks.

4. To configure input, click the icon at the right of the **Input** field, and then select one or more values from the drop-down list. If the value that you require does not appear in the list, you must create it as an additional property. For more information about how to do this, see the "Related tasks" section.

To configure output, click the icon at the right of the **Output** field, and then select one or more values from the drop-down list.

Note: The output field supports additional properties only.

5. Click **Save** in the toolbar to save your changes.

Configure the recommended maximum number of tasks

HP Service Manager processes planned tasks sequentially. Therefore, if you plan a large number of tasks for a single phase in a workflow, you may experience slow performance when a record moves to that phase and the tasks are processed.

To help prevent users from planning too many tasks and degrading the system performance, you can configure the recommended maximum number of tasks for phases. When a record that has more than the maximum recommended number of tasks is saved, a warning message is displayed to the current user.

To configure the recommended maximum number of tasks, follow these steps:

1. Click **Tailoring > Process Designer > Configuration > Settings**.
2. In the **Suggested Maximum Task Number in Task Planner** field, enter the desired maximum number of tasks for each phase. By default, the value is 10.

Note: We do not recommend that you configure a value over 10.

3. Click **Save** in the toolbar to save your changes and exit.

Configuring Task Planner

You can perform the following tasks to configure Task Planner to your requirements:

- ["Add fields to Task Planner" below](#)
- ["Edit additional fields in Task Planner" on page 95](#)
- ["Remove additional fields from Task Planner" on page 96](#)
- ["Configure the status mapping between the task file and Task Planner" on page 96](#)
- ["Configure the additional properties in Task Planner" on page 97](#)

Add fields to Task Planner

You can add fields to Task Planner, and determine whether they are mandatory or not. Additional fields are associated with a specific type of task file (for example, the change task file), and can be configured at both the file and task category level. This determines whether the additional field is displayed whenever Task Planner is started for that type of task file, or whether the field is displayed once the user has entered a value in the Task category field.

Note: You cannot remove or modify the fields that are present by default (that is, the Title, Task Category, Open In Phase, Close By Phase, Task template, Task Condition, and Assignment Rule fields).

The following example adds the **Assignment Group** field in the **requestTask** table to Task Planner.

To add a field to Task Planner, follow these steps:

1. Click **Tailoring > Process Designer > Configuration > Predefined Additional Task Fields**.
2. Select **requestTask** from the **File Name** drop-down list, and then click the **New** icon.
3. If you want to configure an additional field at the file level, leave the **Task Category Name** field empty. If you want to configure an additional field that applies only to a specific task category, click **Fill** to select a task category in the **Task Category Name** field.

Note: If one field is defined at both the file and category levels, the setting in the category level overrides the setting in the file level.

4. Click **Add Field**.
5. In the **Field Name** drop-down list, select the field that you want to add to Task Planner. For example, select **Assignment Group**.
6. If you want this additional field to be mandatory, select the **Mandatory** option.
7. If this field has a link definition defined, select the **Is Record in Table?** check box. For example, a link definition exists for the **Assignment Group** field because the values of this field should be retrieved from the **assignment** table.

The Record Information area appears. If only one relationship record of this field exists in Relationship Manager, this area is automatically populated with the relationship information. If multiple relationship records exist, you need to click the Fill icon in the **Relationship Id** field to select the correct relationship record. If no relationship records of this field exist in Relationship Manager, no relationship information is displayed.

See the following table for more information.

Field	Description	Example value
Relationship Id	This is the Id of the relationship record, which you can find in Relationship Manager through a search. For example, for the Affected CI (logical.name) field in cm3t, enter table name cm3t and field name logical.name, and then click Search .	5914
Table	This is the name of the other table in the relationship record.	assignment
Field	This is the name of mapping field in the other table.	name

You can define a query by clicking **Edit Query** so that only values that meet the specified conditions will be available for selection in Task Planner. For example, you can specify this query:

```
( Time Zone = "US/Pacific" )
```

Caution: If you want to add an array field (for example, Affected CI) to Task Planner, do not select the **Is Record in Table** option. Additionally, in Task Planner, you cannot select values for the field by clicking Fill; instead, you can only manually enter values by using one of the following formats depending on the array type:

- array character {"a","b"}
- array number {1,2}
- array datetime {'09/02/15 13:35:42'}
- array boolean {true, false}

8. Click **OK**. The field is now added.

Tip: You can click **Edit Field** to edit the field or click **Delete Field** to delete the field. You can also click **Add Field** to add more fields.

9. Click **Save** to save the record.
10. Verify that the field is added to Task Planner.
 - a. Go to **Request Fulfillment > Configuration > Request Models**, and open a request model record through a search. For example, open the out-of-box Application Access request model.
 - b. Go to the Task section and click **Edit** to open Task Planner.
 - c. Select a task. For example, select the out-of-box Enable Access task. The field you added (Assignment Group in this example) is displayed on the **Task-Properties** tab. If you click Fill in this field, a list of values based on the query conditions you set is displayed.

Task-Properties Input-Output

Title* Enable Access

Task Category* Labor

Open In Phase* Fulfillment Close By Phase Fulfillment

Task Template

Task Condition

Assignment Rule

☐ Mark as required/Set properties as read-only

Assigned Group* Application
ASSET MANAGEMENT

- d. If you select a value for the field and then save the request model record, the task record is automatically populated with this field value when created later.

Edit additional fields in Task Planner

Note: You cannot remove or modify fields in Task Planner that are present by default (that is, the Title, Task Category, Open In Phase, Close By Phase, Task template, Task Condition, and Assignment Rule fields).

To edit an additional field in Task Planner, follow these steps:

1. Click **Tailoring > Process Designer > Configuration > Predefined Additional Task Fields**.
2. Select a task file type from the **File Name** drop-down list, and then click the **Search** icon to display the additional fields that are configured for that type of task file.
3. In the table of additional fields, select the row that describes the field that you want to edit, and then click **Edit Field**.
4. Make your desired changes, and then click **OK**.
5. Click **OK** in the toolbar to save your changes.

Remove additional fields from Task Planner

Note: You cannot remove or modify fields in Task Planner that are present by default (that is, the Title, Task Category, Open In Phase, Close By Phase, Task template, Task Condition, and Assignment Rule fields).

To remove an additional field from Task Planner, follow these steps:

1. Click **Tailoring > Process Designer > Configuration > Predefined Additional Task Fields**.
2. Select a task file type from the **File Name** drop-down list, and then click the **Search** icon to display the additional fields that are configured for that type of task file.
3. In the table of additional fields, select the row that describes the field that you want to remove, and then click **Delete Field**.
4. Click **OK** in the toolbar to save your changes.

Configure the status mapping between the task file and Task Planner

The different statuses through which tasks in HP Service Manager pass do not correspond exactly to the different statuses that Task Planner uses to describe the progress of tasks. In order for the Task Planner graphical interface to display the correct status for each task, you must map the statuses of each task file type to the statuses in Task Planner.

Tip: Mapping records for both Change Tasks and Request Tasks are included in out-of-box Service Manager systems.

For more information about the Task Planner graphical interface and a list of the task statuses, see ["Task Planner" on page 87](#).

To create a new map between the statuses of a task and the statuses displayed in Task Planner, follow these steps:

1. Click **Tailoring > Process Designer > Configuration > Task Planner Mapping**.
2. Click **New** in the toolbar.

3. In the **Parent File Name** drop-down list, select the type of record with which the task is associated. For example, select **request**.
4. In the **Model File Name** field, select the model level for the task. For example, **requestModel**.
5. In the **Task File Name** field, select the name of the task file. For example, **requestTask**.
6. In the **Task Status Field Name**, select the field in the task record that contains the task status. For example, select **Status**. The left-hand **Task Status** column in the table is populated with all the values that are defined in the global list for that field.
7. In the right-hand **Task Planner Status** column, select the Task Planner status to which you want to map the corresponding task status. For example, map the **CMDB Update** task status to the **In Progress** Task Planner status. Repeat this until you have mapped all task statuses to a Task Planner status.
8. Click **Save** in the toolbar to save your changes.

Configure the additional properties in Task Planner

The additional properties in Task Planner enable you to share information between task records and parent records, and also between task records. When you configure the input and output of a planned task, the options available for selection are typically user options or fields in the parent record. In order to make other options available, you must configure the additional properties.

Add an additional property

To add an additional property, follow these steps:

1. Open the record for which you want to plan a task.

For example, click **Change Management > Change Queue**, and then select a Change record from the queue. Or, click **Request Fulfillment > Search Requests**, enter your search criteria, and then click **Search**.

2. Click the **Tasks** tab in the record, click **Edit**, and then click **Additional Properties** to open the Additional Properties information page.
3. In the toolbar, click **Add Additional Properties** to open the New Additional Property page.
4. In the **ID** field, type an identifier for the additional property.

Note: The identifier cannot start with either a number or a punctuation mark.

5. In the **Display Label** field, type the name of the field as you want it to appear in the Additional Properties tab of the task record.
6. In the **Type** drop-down list, select the type of data that you want to share, and then click **Next**.

Note: Depending on the type of data that you choose, you may have to enter further information. For example, if you select **Record**, you must then specify the table and the field in which the record is located.

7. (Optional) If the additional property requires validation, enter the validation script into the **Validation Script** field.
8. Click **Finish** to save your changes.

The additional property is now available for selection when you configure input and output values in Task Planner.

Edit an additional property

To edit an additional property, follow these steps:

1. Open the record for which the task that contains the additional property is configured.

For example, click **Change Management > Change Queue**, and then select a Change record from the queue. Or, click **Request Fulfillment > Search Requests**, enter your search criteria, and then click **Search**.

2. Click the **Tasks** tab in the record, click **Edit**, and then click **Additional Properties** to open the Additional Properties information page.
3. In the toolbar, click **Edit Additional Properties** to open the New Additional Property page.
4. Make the required changes to the additional properties definition.
5. Click **Finish** to save your changes.

Delete an additional property

To delete an additional property, follow these steps:

1. Open the record for which the task that contains the additional property is configured.

For example, click **Change Management > Change Queue**, and then select a Change record from the queue. Or, click **Request Fulfillment > Search Requests**, enter your search criteria, and then click **Search**.

2. Click the **Tasks** tab in the record, click **Edit**, and then click **Additional Properties** to open the Additional Properties information page.
3. In the toolbar, click **Edit Additional Properties** to open the New Additional Property page.
4. Click **Remove This Additional Property**, and then click **Yes** to confirm the deletion.

Process Designer workflows

A workflow is a collection of phases with transitions from one phase to another. Each phase represents the state of the workflow linked to a form for data capture. Transitions can connect phases in any manner such as creating parallel branches or loop backs to previous branches.

A workflow enables an implementer to graphically layout the entire lifecycle of a process or record without any programming knowledge. The end user of the workflow views the same graphical workflow to see the current phase and past transitions.

Before you create a new workflow, you must add rules and rule sets to the phases and transitions of your intended workflow.

Create a workflow

Applies to User Roles:

System Administrator

Implementer

Note: You can create a workflow only in the web client.

After you have a basic workflow, you can then modify it by adding additional phases, transitions, rules, and actions to match the business process.

You can click **Zoom in** or **Zoom out** in the toolbar either to zoom in or zoom out in the workflow page.

To create a workflow, follow these steps:

1. Click **Tailoring > Process Designer > Workflows**.
2. Click **New**.
3. Type a name for the workflow. For example, `demo_Workflow`.

Note: You cannot modify a workflow name once it is set.

4. Type a description for the workflow.
5. Select an HP Service Manager table from the drop-down list to associate the table with the new workflow, for example `kmdocument`.

Note: You can use the `kmdocument` table to manage the Knowledge Management document process. You can use the `WorkflowDemo` table to explore Process Designer capabilities.

6. Click **OK**. The new workflow **demo_Workflow** appears in the Workflows list.

Note:

- HP Proprietary workflows are accompanied by an HP logo in the workflow list. Non-HP Proprietary workflows are not accompanied by a logo.
- If you want to edit an HP Proprietary workflow or use it as a model, create a copy of the HP Proprietary workflow.

After you created a basic workflow, modify the Object record of the table for the new workflow.

Note: Modifying the Object record is only required for the Knowledge Management module. All other modules that use Process Designer set the workflows in each of the Category records. For other modules using Process Designer, update the category record.

To modify the object record, follow these steps:

1. Click **Tailoring > Document Engine > Objects**.
2. Under File name, provide the table name of the associated workflow. For example, "`kmdocument`."
3. Select **In Object in Workflow Location** drop-down list.

4. Select the workflow name in Workflow drop-down list.
5. Click **Save**.

Copy an existing workflow

Applies to User Roles:

System Administrator

Implementer

You can clone an existing workflow to use it in another business process or if you need to make changes to a HP Proprietary workflow. You also have an option to copy the rule sets of the existing workflow.

To copy an existing workflow, follow these steps:

1. Click **Tailoring > Process Designer > Copy Existing Workflow**.
2. In the Clone a Workflow form, select the workflow that you want to copy.
3. Type a new workflow name.
4. Click **Copy rule sets** check box if you want to copy rule sets.
5. Type a rule set prefix.
6. Click **Next**.
7. Click **Workflows** . The newly-copied workflow is displayed.

Export a Workflow

You can export a workflow from Process Designer into a Service Manager unload file. You can then use that unload file to import the workflow into another Process Designer-based Service Manager system.

Note: The export only includes the related records in the Workflow, WorkflowPhase, and RuleSet tables. Processes and Java Scripts called from rules sets cannot be exported.

To export a workflow to an unload file, follow these steps:

1. Navigate **Tailoring > Process Designer > Export Workflow**.
2. In the Export/Unload a Workflow tab, select a Process Designer Table from the **Table** drop-down.
3. Select the workflow from the **Workflow Name** field.
4. Enter an appropriate name in the **External File Name** box.
5. Select or clear the **Append to file** check box as appropriate.

Note: If you wish to append this workflow to an existing unload file, enter the unload file name, and make sure that the **Append to file** check box is checked. You can use this mechanism to build a single unload file that contains multiple workflows that you can later import into another Process Designer-based Service Manager system.

6. Click **Ok**.

After the file is created, save the file to an appropriate location. You can then import the generated unload file to in another Process Designer-based Service Manager system.

Workflow phases

Workflow phases show the state of a record in the workflow and provide processing that must occur for the record to move to the next phase. Phases use transitions to move from one phase to another phase. Some of this processing can be manual, or it can be triggered by the rules or actions specified for that specific phase.

Within a workflow, you can specify a form to display when that phase is active. Use different forms on different phases to allow different information to be displayed and captured at various stages of the workflow.

Rule sets are defined in the phase or transition to enforce business logic, such as checking if the user has entered the required data or has proper security to perform a transition.

Add a phase

Applies to User Roles:

System Administrator

Implementer

You can add a phase to an existing workflow by using the graphical interface of the workflow editor.

Note: After you add a phase and click **Save**, you cannot modify its name. You can modify only its display name.

To add a phase to a workflow, follow these steps:

1. Click **Tailoring > Process Designer > Workflows** from the System Navigator to display the workflows list.
2. Select the applicable workflow for which you want to add a phase.
3. Click **Add phase**.
4. Drag the mouse to add a new transition and a phase.
5. Enter the details described in the table.

Details	
Phase Order	<p>The Phase Order field gives a numerical order number to each phase of a workflow. These numbers are used in calculations for Service Level Targets (SLTs) and similar metrics, so that the number and timestamps of entries and exits from specific phases can be tracked. For example, an SLT calculation can determine the time of entry to the final phase and therefore determine whether a breach has occurred.</p> <p>As best practice, you should specify your starting phase as 1, and your closing phase as the highest number. We also recommend that these numbers should be roughly sequential from phase to phase. However, some workflows may loop multiple times through a sequence or take divergent paths.</p>
Name	Type the name of the tab.
Display name	Type the display name of the tab.
Table name	The selected table name during workflow creation. You cannot modify it.
Form Edit condition	If the condition evaluates to true for a user, who will be able to edit the form. If it does not, the form will be read-only.
Records in this phase are active	Select the check box if you want the records in this phase to be active.
Make this the first phase	Click Make this the first phase if you want it to be the first phase.
Make this the default	Click Make this the default phase if you want it to be the default phase. Click Save .

phase	<p>Note: If the current phase of a record is set to a phase that does not exist in the current workflow, it will be moved to the default phase. This may occur if a phase is removed from a workflow or if data is imported from another source that did not share the same workflow.</p>
Additional Phase Information	<p>Click Additional Phase Information to open the Extended Phase Information page to modify phase information.</p> <p>Note:</p> <p>Only the Change Management module supports this feature.</p> <p>You cannot edit or delete a phase name from the Extended Phase Information page or the cm3rcatphase.main form.</p> <p>Change Management workflows have unique workflow phases but they will share change phases if the workflow phases have the same name. For example, if the Workflow1 and Workflow2 each have a phase named 'Build and Test' they will share the same change phase record.</p>
Description	Enter a description of the workflow phase. This field supports hyperlinks.
Forms	
Display form	<p>The display form is the primary method to capture and display data. If you do not specify a form, the system will look for a form that has the same name as the current table name.</p> <p>To add a display form, follow these steps:</p> <ol style="list-style-type: none"> 1. Select the display form from the Default Display form drop-down list. 2. Click Save. <p>To add a display form that is selected by a condition or set of conditions, follow these steps:</p> <ol style="list-style-type: none"> 1. In the Additional/Display forms section, click Add. 2. In the Name drop-down list, select the form name. 3. In the Description field, type a description of the form. 4. Click the Form Condition field and use the condition editor to enter a condition. 5. In the Type drop-down list, select Display Form. 6. Click Update to add the additional form. <p>Note: You may also specify a form in a RAD expression, for example "display.form"</p>

	in \$L.category”.
Additional Forms	<p>You can add, edit, and delete additional forms for a workflow phase.</p> <p>To add an additional form to a workflow record, follow these steps:</p> <ol style="list-style-type: none"> 1. Click Add. 2. In the Name drop-down list, select the table name. 3. In the Description field, type a description of the form. 4. Click the Form Condition field and enter a condition. 5. In the Type drop-down list, select Additional Form. 6. Click Update to add the additional form.
Rule sets	
Add	<p>To add rule sets at various stages:</p> <ol style="list-style-type: none"> 1. Click the On enter, After successful enter, On exit, Initialization, On display, On update, or After successful update tab. For more information, see the note after step 4. 2. Click Add. 3. Select the appropriate rule sets check box you want to add. 4. Click Save. <div> <p>Note: You may also specify a form in a RAD expression, for example “display.form in \$L.category”.</p> <ul style="list-style-type: none"> • On enter – Runs when the record tries to move from another phase into this phase. For example, the rule set can set the time at which the record first entered the phase or send notifications that the record has entered the phase. • After successful enter – Runs after the record successfully moves from another phase into this phase. • On exit – Runs when the record moves out of this phase. For example, the rule set can set the time at which the record left the phase or send notifications that the record has left the phase. • Initialization – Runs once just before the record is displayed to the user. For example, the rule set can set up variables for display that are not meant to change while the user is viewing the record. </div>

	<ul style="list-style-type: none"> • On display – Runs each time the record is displayed after a user action. For example, if the user uses the “fill” function to populate a field, the display rules will run after the action is completed and before the form is displayed. A possible use may be to populate a variable that is displayed on the form, which is calculated based on other values in the form. • On update – Runs immediately before the record is updated in the database (or created if this is a new record). For example, the rule set can validate field data (the record will not be updated if validations fail), set default values, or perform calculations on existing fields. • After successful update – Runs immediately after the record is updated in the database (or created if this is a new record). For example, the rule set can send notifications of the record update or update related records based on changes to this record.
Actions	
Add	<p>Actions perform a task for the phase. In Knowledge Management, Actions are used to preview the document. Actions refer to rule sets that are marked as Available as Action.</p> <ol style="list-style-type: none"> 1. Click Add to add an action, which runs associated rule sets for that phase of the workflow. 2. Type the identification name, which is how the action will appear in the Tray, More Options List, or on the button. 3. Select the action from the drop-down list. 4. Select the location of the action: Tray, More Options List, or Button. <p>Note: If you select Button, then manually add a button to the form with the option number of the action specified.</p> <ol style="list-style-type: none"> 5. Click Action Condition to add a condition if required. 6. Select Add, Save, or Delete for action when complete. 7. Select Requires lock check box if you want to lock the record before the action can be performed. <p>Note: If another user has the record locked, you will not be able to perform the action.</p> <ol style="list-style-type: none"> 8. Click Save.

Approvals	
Reset condition or Recalculate condition	<ol style="list-style-type: none"> 1. Click Reset Condition or Recalculate Condition. 2. Click Save.
Add approvals	<ol style="list-style-type: none"> 1. Click Add to add approvals. 2. Select desired approvals for the phase. 3. Click Save.
Alerts	
Reset condition or Recalculate condition	<ol style="list-style-type: none"> 1. Click Reset Condition or Recalculate Condition. 2. Click Save.

- To reposition the phase, select the phase, hover your mouse until you see a crosshairs symbol, and then move the phase to the desired location on the workflow page.
- To delete a phase, select the phase and either click the trashcan symbol next to the phase or **Delete** from the toolbar. You cannot delete default or first phases.
- To move multiple phases at the same time, press **Ctrl** and select multiple phases, and then move the phases or section of the workflow to new location.
- In the **Rule Sets** tab, select a rule set and either double-click the rule set or click the **View** icon to open the rule set page.
- In the **Approvals** tab, select an approval name and either double-click the approval name or click the **View** icon to open the Approval Definition page.
- In the **Alerts** tab, select an alert name and either double-click the alert name or click the **View** icon to open the Alert Definition page.

Copy a phase

Applies to User Roles:

System Administrator

Implementer

You can copy a phase in an existing workflow by using the graphical interface of the workflow editor. Every attribute of the phase is copied, apart from the name and display name. This feature enables you to create workflow phases that have similar attributes quickly.

To copy a phase in a workflow, follow these steps:

1. Click **Tailoring > Process Designer > Workflows** from the System Navigator to display the workflows list.
2. Open the workflow in which you want to copy a phase.
3. Select the phase that you want to copy, click **Copy** in the toolbar, and then click **Paste**. Alternatively, you can press Ctrl+C and Ctrl+V after you select the phase to copy.

The duplicate phase appears overlapping the copied phase. By default, the name of the new phase is "*<copied phase name>_copy*."

4. Modify the attributes of the phase as required.
5. Drag the copied phase to a convenient location in the workflow, and then add the necessary transitions.
6. Click **Save** to save your changes.

Workflow transitions

Process Designer workflow transitions occur when a record moves from one phase to another phase. Transitions can happen manually, automatically, or by default. An automatic transition is taken when its condition is met. For example, the condition might check if a field value is a specific value. In this case, the transition is taken automatically when the record is saved. An example of a manual transition is when an operator clicks the "Request Validation" button in the toolbar of a form. A default transition is a special transition type that moves the workflow automatically only when no other automatic transition conditions are satisfied.

Note: Transitions govern the flow of the workflow. However, in Change Management processes, an operator with Administrator rights can use the "Change Phase" menu option to bypass the workflow and jump to any phase.

After you add a transition, you can reposition it to avoid transitions overlapping with phases or other transitions. To reposition the transition, select the transition and move the green rectangular dot to achieve a desired layout.

You can also move a transition from one phase to another. To move the transition, select the transition, hover your mouse near the blue rectangular dot to see a hand symbol, and then move it to another phase.

Tip: Workflow phases are connected by transitions to move from one phase to another phase. However, if you want to move to another phase from the current phase, you can use backend transitions. For more information, see the ["Process Designer Tailoring Best Practice Guide" on page 1](#).

Create a manual workflow transition

Applies to User Roles:

System Administrator

Implementer

When you set up a workflow, you can require an operator action to move a record from one phase to another. This type of transition, in which an operator must press a button or otherwise trigger an action, is a manual transition.

To create a manual workflow transition, follow these steps:

1. Click **Tailoring > Process Designer > Workflows**.
2. Open the applicable workflow from the Workflows list.
3. Click the phase where the manual transition will begin.
4. Hover your mouse until you see a hand symbol and then drag the mouse to add another phase.
5. Enter the following information.

Field	Description
Transaction Type	Evaluates to one of the following transition types: Manual , Automatic , or Default . Select the Manual transition type.
Command Name	Evaluates to command location: Tray , More Options List , or Button .
Description	Type a description of the transition. This description is displayed when you hover the mouse over the transition in the Workflow Viewer.
Condition	Evaluates to a condition that you can add to the transition.

Field	Description
Rule Sets	Evaluates to the rule sets you created for the transition. a. Click Add and then select the ID of the rule set you want to add. b. Click OK .
Save record prior executing the transition	Select this option if you want the record to be saved before the transition occurs.

6. Click **Save**.

You have added a manual transition.

Note: Click the **Localize Command Label** icon in the **Command Name** text box to open the **HP Service Manager Message** form of a transition. In this page, you can add a message record for a new transition or view the message record of an existing transition.

Create an automatic workflow transition

Applies to User Roles:

System Administrator

Implementer

An automatic transition moves the workflow to another phase based on data in the workflow record.

Note: You can add a condition and rule sets to the automatic transition.

To create an automatic workflow transition, follow these steps:

1. Click **Tailoring > Process Designer > Workflows**.
2. Open the applicable workflow from the Workflows list .
3. Click the phase where the automatic transition will begin.
4. Hover your mouse until you see a hand symbol and then drag the mouse to add another phase.

5. Enter the following information.

Field	Description
Transition Type	Evaluates to one of the following transition types: Manual , Automatic , or Default . Select the Automatic transition type.
Description	Type a description of the transition. This description is displayed when you hover the mouse over the transition in the Workflow Viewer.
Condition	Evaluates to a condition that you can add to the transition.
Rule Sets	Evaluates to the rule sets you created for the transition. a. Click Add and then select the ID of the rule set you want to add. b. Click OK .

6. Click **Save**.

You have added an automatic transition.

Create a default workflow transition

Applies to User Roles:

System Administrator

Implementer

A default transition moves the workflow automatically only when no other transition conditions are satisfied.

Note: You can add rule sets to the default transition.

To create a default workflow transition, follow these steps:

1. Click **Tailoring > Process Designer > Workflows**.
2. Open the applicable workflow from the Workflows list.
3. Click the phase where the default transition will begin.
4. Hover your mouse until you see a hand symbol and then drag the mouse to add another phase.

5. Enter the following information.

Field	Description
Transition Type	Evaluates to one of the following transition types: Manual , Automatic , or Default . Select the Default transition type.
Description	Type a description of the transition. This description is displayed when you hover the mouse over the transition in the Workflow Viewer.
Rule Sets	Evaluates to the rule sets you created for the transition. <ol style="list-style-type: none"> Click Add and then select the ID of the rule set you want to add. Click OK.

6. Click **Save**.

You have added a default transition.

Workflow Viewer

The following sections explain the workflow viewer and how to integrate it into a knowledge document.

View a workflow in Workflow Viewer

Applies to User Roles:

System Administrator

Implementer

The Workflow Viewer enables you to view a graphical layout of the entire lifecycle of a process or record. The phases and transitions of the workflow are color-coded as follows.

Phase/transition	Color property used
Current phase	Green highlight
Past phase	Green border
Future phase	Blue border
Inactive phase	Grey border
Past transition	Dotted green line
Future transition	Blue line arrow

If a phase in a workflow contains approvals, an Approvals icon is displayed in the phase in the Workflow Viewer.

You can view information about specific parts of the workflow by hovering the mouse over that component in the Workflow Viewer. For example, hover the mouse over a transition between two phases to display the description of that transition. Or, hover the mouse over the Approvals icon to display the approval definition list (in future phases), the approvals information in the Approval table (in the current phase), or the approval history (in past phases).

To view a workflow, open a record, and then click the **Workflow** tab.

Note: In order to view a workflow in the Workflow Viewer, you must integrate a Workflow widget into any form that is associated with a Process Designer-enabled table. This is currently available for Knowledge Management (`kmdocument`), Change Management (`cm3r` and `cm3t`), and WorkflowDemo, Service Desk (`incidents`), Incident Management (`probsummary` and `imTask`), Problem Management (`rootcause` and `rootcausetask`), and Request Fulfillment (`request` and `requestTask`).

The procedure to integrate the viewer into each module is very similar.

View the workflow properties

Applies to User Roles:

System Administrator

Implementer

You can use the Workflow Properties button to view the properties that are related to an entire workflow. You can see all the workflow-based Rule Sets, Actions, and Backend Transitions that are related to that workflow.

To view the Workflow properties, follow these steps:

1. Click **Tailoring > Process Designer > Workflows**. Or, from within a Process Designer module, click **Configuration** and then **Workflows**.
2. Double-click on any workflow.
3. After the Workflow tab opens, click the **Workflow Properties** button.
4. Click on any of the following tabs:

- **Workflow Properties**
- **Workflow Based Rule Sets**
- **Workflow Based Actions**
- **Workflow Backend Transitions**

Caution: If you modify a rule set that you have accessed through the Workflow Properties button, those changes are applied to the rule set directly. Therefore, any other workflow that also uses this rule set will also be affected.

Integrate Workflow Viewer into a new form

Applies to User Roles:

System Administrator

Implementer

The Workflow Viewer icon is available in Forms Designer. The following example will help you integrate the Workflow Viewer widget into the `kmdocument.document` form. After the integration, you can see a graphical view of the workflow in the **Contribute Knowledge > External > Workflow** tab. Using similar steps, you can integrate the Workflow Viewer with other forms.

To integrate the Workflow Viewer widget into the `kmdocument` form:

1. Log on as a System Administrator and open Forms Designer in the Windows client (In the System Navigator, click **Tailoring > Forms Designer**). For information on accessing Forms Designer and updating a form, see the following topics in the Help server: "Access Forms Designer" and "Update a form".
2. In the Form field, type `kmdocument.external` and click **Search**. The Contribute Knowledge form opens with the External Document Upload tab selected.
3. Add 'Workflow' tab in the form.
4. Set the visible condition to `[$showWF]=true` in the Workflow tab.

Note: The condition hides the tab in the Windows client, but is visible in the Web client.

5. Add the Workflow Viewer component to the new Workflow tab.
6. In the Workflow Viewer component, set the following variables in the properties.

Workflow Name: \$L.wfgWFName

Workflow Table: \$L.wfgWFTable

Workflow RecordID: \$L.wfgWFRecId

Workflow Current Phase: \$L.wfgWFPhase

7. Add four text boxes at the bottom of the Workflow Viewer.
8. Set their input values in the properties to:

\$L.wfgWFName

\$L.wfgWFTable

\$L.wfgWFRecId

\$L.wfgWFPhase

Note: The four text boxes display workflow name, table name, document id, and phase of the record.

9. Set the Workflow Viewer variables in the **Main > Initialization** tab of display screens for kmdocFlow.open and kmdocFlow.view:

\$L.wfgWFName=workflowName in \$L.wfPhase

\$L.wfgWFTable=tableName in \$L.wfPhase

\$L.wfgWFPhase=phaseName in \$L.wfPhase

\$L.wfgWFRecId=id in \$L.file

if (sysinfo.get("environment")~="scguiwswt") then (\$showWF="true") else (\$showWF="false")

Note: To go to display screen, type ds in Service Manager command prompt and search for

the kmdocument.document form.

10. Follow steps 1 through 7 to add Workflow View in the other Knowledge Management forms: kmdocuments (kmdocument.probsol, kmdocument.howto, kmdocument.reference and kmdocument.errormsg)

Workflow-based rule sets, actions, and transitions

Applies to User Roles:

System Administrator

Implementer

Process Designer allows you to apply rule sets, actions and transitions to a workflow as a unit, which are collectively referred to as workflow-based rule sets, actions and transitions. You can access the workflow-based rule sets, actions, or transitions by following the steps in ["View the workflow properties" on page 113](#).

The following sections describe special considerations when you apply a rule sets, actions or transitions to an entire workflow.

Workflow-based rule sets

Applies to User Roles:

System Administrator

Implementer

You can add workflow-based rule sets to an entire workflow by viewing the **Workflow Properties**.

A workflow-based rule set is invoked on each phase of the workflow as long as the triggering events are triggered in the back-end.

A workflow-based rule set is comprised of six sub-rule sets.

Sub-rule set	Triggering action	Execution Order
On Add	Record Creation (Adding Record)	<ol style="list-style-type: none"> 1. Add (before record is created in the database) 2. After Successful Add (after

		<p>record is created in the database)</p> <ol style="list-style-type: none"> 3. Initialize 4. On Display
After Successful Add	Record Creation (Adding Record)	<ol style="list-style-type: none"> 1. Update (before record is updated in the database) 2. After Successful Add (after record is created in the database) 3. Initialize 4. On Display
On Enter	Phase Change	<ol style="list-style-type: none"> 1. From phase On Exit 2. To phase On Enter 3. To phase After successful Enter
After Successful Enter	Phase Change	<ol style="list-style-type: none"> 1. From phase On Exit 2. To phase On Enter 3. To phase After successful Enter
On Exit	Phase Change	<ol style="list-style-type: none"> 1. From phase On Exit 2. To phase On Enter 3. To phase After successful Enter
Initialization	Search and access existing record	<ol style="list-style-type: none"> 1. Initialize 2. On Display
On display	Current page refresh (caused by link execution or other action that still keeps at current format)	<ol style="list-style-type: none"> 1. On Display
On Update	Record Update	<ol style="list-style-type: none"> 1. Update (before record is updated in the database) 2. After Successful Update 3. Initialize

		4. On Display
After Successful Update	Record Update	<ol style="list-style-type: none"> 1. Update (before record is updated in the database) 2. After Successful Update 3. Initialize 4. On Display

Workflow-based actions

Applies to User Roles:

System Administrator

Implementer

In earlier versions of Process Designer, actions were applied to individual phases. In certain circumstances, the same actions had to be duplicated in each phase. For example, in cases where a certain button needed to be present in each phase, the workflow designer had to add the button manually to each phase.

In the current version of Process Designer, you can add workflow-based actions to an entire workflow by viewing the **Workflow Properties**.

A workflow-based action appears in each phase of the workflow when its condition is satisfied.

Workflow transitions

Process Designer workflow transitions occur when a record moves from one phase to another phase. Transitions can happen manually, automatically, or by default. An automatic transition is taken when its condition is met. For example, the condition might check if a field value is a specific value. In this case, the transition is taken automatically when the record is saved. An example of a manual transition is when an operator clicks the “Request Validation” button in the toolbar of a form. A default transition is a special transition type that moves the workflow automatically only when no other automatic transition conditions are satisfied.

Note: Transitions govern the flow of the workflow. However, in Change Management processes, an operator with Administrator rights can use the “Change Phase” menu option to bypass the workflow and jump to any phase.

After you add a transition, you can reposition it to avoid transitions overlapping with phases or other transitions. To reposition the transition, select the transition and move the green rectangular dot to achieve a desired layout.

You can also move a transition from one phase to another. To move the transition, select the transition, hover your mouse near the blue rectangular dot to see a hand symbol, and then move it to another phase.

Tip: Workflow phases are connected by transitions to move from one phase to another phase. However, if you want to move to another phase from the current phase, you can use backend transitions. For more information, see the ["Process Designer Tailoring Best Practice Guide" on page 1](#).

Process Designer security model

The Process Designer security model provides a consistent method of assigning permissions to users across all facets of Service Manager data and accounts for out-of-box rights that can be configured for a specified role within an area. It also provides standardized methods to manage user rights.

Note: Process Designer security model is implemented for Knowledge Management, Change Management, Service Desk, Incident Management, Problem Management, Request Fulfillment, and Service Level Management modules. For all other areas and modules, the traditional security features for Service Manager still apply.

The Process Designer security model includes the following components:

- **Area:** An area defines a specific functional area or module within Service Manager, such as Knowledge Management or Knowledge Management administration. Each area definition includes default rights that are copied to the role whenever a new role is created. In addition to the out-of-box areas, system administrators are able to define additional areas.

In an out-of-box system, the following three security areas are shared by several modules: Tailoring, Common Configuration, and Security. These areas contain the default security rights and settings that apply to the Change Management, Service Desk, Incident Management and Problem Management modules:

- The Tailoring area is used to set the permissions that control operator access to Workflows.
- The Common Configuration area is used to set the permissions that control access to common configurations, including Alert Definitions, Approval Definitions, Assignment Groups, Service Desk/Problem Solution Matching, and Environment.
- The Security area is used to set the permissions that control operator access to Security configurations.

Note: The rights to access Settings are controlled by the separate Configuration area in each module.

- **Rights:** The system includes a set of rights such as view, new, update, and delete that control an operator's data access. When an administrator creates a role, the default rights from each area are used to set the rights for that role. Rights can be modified for a specific area and role by an administrator that has update rights for the area and role. Each combination of role and area creates a collection of rights.

Security Rights also include the following components:

- **Allowed Statuses:** This field displays the list of statuses that are available to operator when they access records. A System Administrator specifies the allowed statuses for a role within an area. When this list is populated, the role may only update the records that are in one of the listed statuses. If a record has a status that is not in the list, the role will not be able to modify it. However, when the role updates records, the statuses that are available for selection are not limited to the list. If no statuses are listed, the role may modify records in any status.
- **Allowed Categories:** This field displays the list of categories that are available to the operator when they access category data. A System Administrator specifies the allowed categories for a role within an area. When this list is populated, only the listed categories are available for selection when the role creates a new record or updates a record in the Category field. If no categories are listed, all categories are available for the role within the area.
- **Settings:** Settings are configurable security extensions such as an initial view, a format to display a list, or an approval check box. Settings are added for an area. The types of settings include number, string, Boolean, date/time, global list, manual list, record, and condition.
- **Security Folders:** If Folder Entitlement is enabled in the system, a System Administrator must select the security folders that each security role can access. If a role is not granted rights to a specific

folder, operators associated with that role will not be able to access records in that folder.

- **Roles:** A role has a set of rights and settings assigned to it. Each operator is assigned a role or roles which, along with area, determine the access rights for the operator. Whenever the roles on an operator record are updated, the operator must log out and then log in for the changes to take effect.

Note: The out-of-box system includes a default role for the Security area that cannot be deleted.

- **Data Policy records:** The data policy records include an Area field used to specify the area associated with the table. An area needs to be associated with a Data Policy record in order to access the information from the table.

Out-of-box role rights in the Common Configuration area

The Common Configuration area is used to set the permissions that control access to common configurations, including Alert Definitions, Approval Definitions, Assignment Groups, Service Desk/Problem Solution Matching, and Environment.

Based on the mapping rules, the rights and settings in previous security profiles are mapped to the rights and settings in the Common Configuration area specified in the corresponding security roles. See the table below for the out-of-box security rights in the Common Configuration area. This table only lists the new security roles that have different settings with the default rights.

Area	Role	View	New	Update	Delete/Close	Modify Template	Expert	Admin
Common Configuration	change analyst change	True	True	Always	Always	False	False	False
	change analyst tasks	True	True	Always	Always	False	False	False
	change approver	True	True	Always	Always	False	False	False
	change coordinator change	True	True	Always	Always	False	False	False
	change coordinator tasks	True	True	Always	Always	False	False	False
	change	True	True	Always	Always	False	False	False

Area	Role	View	New	Update	Delete/Close	Modify Template	Expert	Admin
	manager							
	configuration auditor	True	True	Always	Always	False	False	False
	emergency group	True	True	Always	Always	False	False	False
	incident analyst	True	True	Always	Always	False	False	False
	incident coordinator	True	True	Always	Always	False	False	False
	incident manager	True	True	Always	Always	False	False	False
	initiator	True	True	Always	Always	False	False	False

Area	Role	View	New	Update	Delete/Close	Modify Template	Expert	Admin
	operator	True	True	Always	Always	False	False	False
	problem analyst	True	True	Always	Always	False	False	False
	problem coordinator	True	True	Always	Always	False	False	False
	problem manager	True	True	Always	Always	False	False	False
	reviewer	True	True	Always	Always	False	False	False
	SD agent/manager	True	True	Always	Always	False	False	False
	service desk agent	True	True	Always	Always	False	False	False
	service desk manager	True	True	Always	Always	False	False	False
	system administrator	True	True	Always	Always	True	True	True
	Requestor	True	False	Never	Never	False	False	False
	Request Approver	False	False	Never	Never	False	False	False
	Request Coordinator	True	False	Never	Never	False	False	False
	Request Analyst	False	False	Never	Never	False	False	False
	Request Manager	True	True	Always	Always	False	False	False
	Request Process Owner	True	True	Always	Always	False	False	False
	Stock Manager	False	False	Never	Never	False	False	False

Multiple security roles

When an operator has multiple security roles, the operator's data access rights are combined to give the operator the greatest data access.

When the rights do not include specific allowed statuses and allowed categories, all statuses and categories are available for the role within the area. Refer to the following examples:

- If an operator has view rights for one role in an area and update rights for another role in that area, then the operator has view and update rights for the area.
- If an operator has allowed statuses and allowed categories specified in one role and not in another role, then the operator is able to access all categories and statuses for the area.
- If an operator has multiple roles that include different allowed statuses and allowed categories, the allowed statuses and allowed categories are merged so that the operator has all allowed categories and allowed statuses. No allowed statuses and allowed categories are duplicated.
- If an operator has multiple settings because the operator has been assigned multiple roles, the operator only has the actual settings for the first settings in the operator record .

Add a security role

Applies to User Roles:

System Administrator

When you create a security role, the rights from each area defined in the system are used to set the rights for that role record.

To add a role record, follow these steps:

1. Click **System Administration > Security > Roles**.
2. Click **New**.
3. Type the name of the role.
4. Type a description for the role.
5. Click **Save & Exit**.

Add security roles and settings

Applies to User Roles:

System Administrator

To create a security role and assign rights and settings, follow these steps:

1. Click **System Administration > Security > Roles**.
2. Click **New**. The **Security Role** form opens.
3. Type the security role name in the **Name** field.
4. Type the security role description in the **Description** field.
5. Click **Save**.
6. Select the security area.

The **Security Rights and Settings** form opens.

7. Under **Rights**, select the rights to be assigned to the security role. For example, set **Expert** rights for the security role. The **Expert** security right enables the operator to view alert log, opened tasks, affected services, and clocks of change request. It also enables you to set reminders, send notifications, create hot news, and associate change request to changes, incidents, interactions, requests, and know errors.
8. Under **Settings**, add required settings.
9. Under **Folders**, add folder permissions to the security role.

The out-of-box security folders available in Service Manager are **DEFAULT** and **advantage**. You can also create security folders to meet your business needs. By default, all security folders are assigned to a new security role created. Once a role is created and rights are configured, you can modify the security rights for a role within an area.

Roles in the operator record

System Administrators assign roles to an operator in the Security Roles field of the operator record. When a System Administrator creates an operator record, the system assigns the default role to the operator if the System Administrator does not add a role for the operator. The System Administrator can update the operator record to change a role or add additional roles.

When an operator has multiple roles, the operator has the rights that provide the greatest data access. However, if each role has additional settings, the rights from the first role listed in the Security Rights field is used to determine an operator's access rights.

Assign a role or roles to an operator

Applies to User Roles:

System Administrator

You assign a role or multiple roles to an operator to provide the operator access to HP Service Manager data. You can also update the operator's role in the operator record.

To assign a role or roles to an operator record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Enter the applicable search criteria to find an operator record and then click **Search**.
3. In **Security Roles**, select the role or roles you want to assign to the operator.
4. Click **Save**.

Add an area

Applies to User Roles:

System Administrator

When you create an area and define the rights and settings for the area, all roles will inherit the rights and settings for the area.

To add an area, follow these steps:

1. Click **System Administration > Security > Areas**.
2. Type the name for the role.
3. Click **New**.
4. Select the module for the area.
5. Type a description for the area.
6. Define the rights for the area.
7. Define the settings for the area.
8. Click **Save** to add the record.

Add a setting within an area

Applies to User Roles:

System Administrator

You can add a new setting, such as record or format, in the area. A role inherits the new setting from the area when the new setting for the area is not already defined in the role. For example, this is useful when you want to have role within an area to have additional access to system data or another form.

When you add a new setting, it is only inherited when you add a new role.

To add a setting within an area, follow these steps:

1. Click **System Administration > Security > Areas**.
2. Add optional search criteria and then click **Search**.
3. Click the area to update.
4. Click **More** or the More Actions icon and then select **Administration > Add New Setting**.
5. In the **New Setting Info** wizard, provide the following:
 - **Id**: Uniquely identifies the setting so that it can be referenced programmatically.
 - **Display Label**: Defines display label for the setting.
 - **Description**: Describes the setting.
 - **Type**: Select the type of data used by the setting to match the type of setting you are creating. For the type selections, the format of the field on the form depends on the type you select. For example, if you choose boolean, then the setting displays a check box and if you select record, the setting displays as a text field. When you select some of the types, the system prompts you for additional information. For example:
 - If you select **Record**, you are also prompted to specify the table and field name for the record.
 - If you select **Manual List**, you are prompted to provide a display type and a name - value pair to display in the list. The Value is the field name in the table and Display Value provides the list of items in the drop-down list for the field.
 - If you select **Global List**, you are prompted to provide a Global List and Display Type for the Global List.
6. Specify whether or not the setting is mandatory. When checked, a value is required for the setting you are adding.
7. Click **Next**.

8. In Adding Settings Validation, add an optional validation script.

9. Click **Finish**.

Validation script for a new setting

When you add an additional setting you have the ability to create simple or complex validations for the setting using JavaScript. The JavaScript automatically sets up an XML variable named `result`, which has a child node named `message`. If the value of the result node is 0 (zero), the validation has succeeded. Any non-zero result is interpreted as a failure. When a validation fails, the contents of the message node display. The value of the setting being validated is set to a variable named `value`.

Example:

This example validates that the setting is a number between 1 and 10.

```
if ( value < 1 || value > 10 )
{
    result.setValue( -1 );
    message.setValue("The value must be between 1 and 10.");
}
```

Update a setting within an area

Applies to User Roles:

System Administrator

Once you create a setting for an area, you can update the definition of the setting or delete it. You can also edit any labels that have been localized.

When you add a new setting to an area, it is only inherited when you add a new role.

To edit a setting within an area, follow these steps:

1. Click **System Administration > Security > Areas**.
2. Add optional search criteria and then click **Search**.
3. Click the area to update.
4. Click **More** or the **More Actions** icon and then select **Administration > Edit/Delete Setting**.
5. Select the setting to edit or delete.
6. On the **Edit Setting Info** wizard, update the following:

- **Id:** Uniquely identifies the setting so that it can be referenced programmatically.
- **Display Label:** Defines a display label for the setting.
- **Description:** Describes the setting.
- **Type:** Select the type of data used by the setting to match the type of setting you are creating. For the type selections, the format of the field on the form depends on the type you select. For example, if you choose boolean, then the setting displays a check box and if you select record, the setting displays as a text field. When you select some of the types, the system prompts you for additional information. For example:
 - If you select **Record**, you are also prompted to specify the table and field name for the record.
 - If you select **Manual List**, you are prompted to provide a name-value pair to display in the list. You must also enter Display Type (Radio Button or Drop Down List).
 - If you select **Global List**, you are prompted to provide a Global List and Display Type for the Global List.

7. Specify whether or not the setting is mandatory.
8. Click **Edit localized labels** to update localized labels.
9. For each language available, you can localize the label text. After you localize the text, click **Save** and then **OK** to return to the wizard.
10. Click **Next**.
11. As an option, you can add or edit a validation script for the setting in Adding Settings Validation.
12. Click **Finish**.

Localize an additional setting

Applies to User Roles:

System Administrator

Once you add a new setting, such as record or format, you can localize the setting for all of the languages that are active in the system.

To add a setting within an area, follow these steps:

1. Click **System Administration > Security > Areas**.
2. Add optional search criteria and then click **Search**.
3. Click the area to update.
4. Click **More** or the More Actions icon and then select **Administration > Edit/Delete Setting**.
5. In the **Edit Setting Info** wizard, click **Edit localized label**. A list of the messages displays for the user's current language.
6. Click the item you want to localize and then type the applicable text to localize the label you created for the setting.
7. Click **Save**.
8. Continue selecting items until you have localized all the labels for the languages active in the system.
9. To localize the data in the settings for global lists or manual lists, use the record tag localization utility.

Modify the rights for a role within an area

Applies to User Roles:

System Administrator

Once a role is created and rights are configured, an administrator updates the rights for a role within an area.

To modify the rights for a role within an area, follow these steps:

1. Click **System Administration > Security > Roles**.
2. Add optional search criteria and then click **Search** to find the role you want to modify.
3. Select the role, and then select the area that you want to modify.
4. Make the changes you want for default rights, folders, and settings.

Note: The values for the "update" and "delete/close" rights of security areas are given the following priorities (from highest to lowest):

- Always
- When assigned to workgroup
- When assigned
- Never

Higher values include the permissions of lower values. For example, if you select "When assigned to workgroup," the role will also have the permissions associated with "When assigned."

If you are assigned two security roles, and if these two roles have different values for the same right in the same area, the higher value will override the lower one. For example, if one role has a right set to "When assigned to workgroup" and another role has the same right set to "When assigned," then you have the "When assigned to workgroup" permissions for this right.

5. Click **Save & Exit**.
6. For any other area, repeat steps 3 through 5 to update the rights for the selected role.

Update rights to display allowed categories and allowed statuses

Applies to User Roles:

System Administrator

A System Administrator can add additional rights to a role within an area by adding the **Allowed Categories** and **Allowed Statuses** fields for an area. Once these fields are available, an administrator can then specify the particular categories and statuses for which the role has rights. If an area has multiple tables that support category and status, the drop-down list in **Allowed Categories** and **Allowed Statuses** will have a combination of all categories and statuses from all tables.

The example below uses the data policy record for the cm3r table for Change Management to demonstrate how to display the **Allowed Categories** and **Allowed Statuses** fields.

Note: When you add a new setting, it is only inherited when you add a new role.

To add a setting within an area, follow these steps:

1. Click **Tailoring > Data Policy**.
2. Use search to find the data policy record for the cm3r table.
3. Select an area from the drop-down list in the **Area** field. This list displays all the areas available for the selected data policy record.
4. Click **Save**. The **Allowed Categories** and **Allowed Statuses** fields now appear in the **Default Rights** section for the roles within the area you specified in step 3.

Modify allowed categories and allowed statuses

Applies to User Roles:

System Administrator

For both roles and areas, an administrator can specify in the Allowed Categories and Allowed Statuses fields the categories and statuses for which a role has rights within an area. Before you can do this, you must first update the applicable data policy record. These rights give a role in combination with the other rights access to the specific categories and statuses selected. When no selections are made for Allowed Categories or Allowed Statuses, the role has access to all categories or statuses within the area.

You must first ensure that the data policy record for the role within an area has been updated to include the **Allowed Categories** and **Allowed Statuses** fields.

Note: When you add a new setting, it is only inherited when you add a new role.

To modify Allowed Categories and Allowed Statuses, follow these steps:

1. Click **System Administration > Security > Roles**.
2. Use search to display a list of roles.
3. Select the role to update.
4. Select the area you want to update.
5. Select the allowed categories and the allowed Statuses from the drop-down lists.
6. Click **Save**.

Check security rights by using Java Script or variables

Applies to User Roles:

System Administrator

In the Process Designer security framework, you can use Java Script functions or use variables to check the security rights of an operator.

Check security rights using Java Script

In the Process Designer security framework, you can use the “security.getRights” Java Script function to check security rights for an operator. For how to use this function, see the following description and examples.

security.getRights(<area>, <right>)

This function checks and returns the specific right (or setting) of the current role in a given Area. The return value is a string.

<area> - The Security Area that is to be checked, such as Incident or Change.

<right> - The right to check, such as new or update.

Example 1

```
var temp = lib.security.getRights("Change", "update")
```

Depending on the specific right that the current user has, the function may return one of the following values: "always", "never", "assigned" or "workgroup".

If the current user has no update right for the Change module, the return value is "false".

Example 2

```
var temp = lib.security.getRights("Change", "allowCategory")
```

The return value is a group of specific categories. For example: {"Emergency Change", "CI Group"}

Example 3

```
var temp = lib.security.getRights("Change", "view")
```

It returns "true" if the current user has the view right for the Change module. Otherwise, it returns "false" if the current user does not have the view right for the Change module.

Note: You can also use the “security.getToken(<area>, <right>)” function to check rights (or

settings).

The `security.getToken` function is an alias of `security.getRights`.

Check record right with variables

You can use the following variables to check whether a user can access a record. The variables are calculated based on new, view, update, delete, allowed status, and folder setting from `secRights` with each record.

- `$L.tableAccess.new`
- `$L.tableAccess.view`
- `$L.tableAccess.update`
- `$L.tableAccess.delete`
- `$L.tableAccess.expert`
- `$L.tableAccess.admin`

Chapter 5: Controlling user access and security

The System Administrator can control user access to HP Service Manager in the following five ways:

1. Setting individual access restrictions in operator records

- Assigning capability words to operators
- Assigning operators to application profiles
- Assigning roles to operators
- Assigning Security Roles to operators for Process Designer enabled modules
- Assigning operators to assignment groups
- Assigning operators to security groups
- Assigning operators to user role descriptions
- Creating a login profile
- Modifying field-level rights
- Enabling application time limits
- Enabling file attachment restrictions
- Enabling password requirements
- Enabling printing restrictions
- Enabling user session restrictions

2. Setting access restrictions by tailoring the application layer

- Creating displayoptions and displayscreens
- Creating document engine objects, states, and processes
- Creating formatctrl

- Creating menus
- Defining DVD controls
- 3. Setting global access restrictions in the System Wide Company record
 - Enabling account expiration times
 - Enabling active integrations to external applications
 - Enabling application time limits
 - Enabling login restrictions
 - Enabling password requirements
- 4. Setting global access restrictions to application tables in Mandanten
 - Defining security group access to database tables
 - Filtering records visible to users by security groups
 - Limiting access to records by adding security group restricting queries
- 5. Setting global access restrictions in the initialization file:
 - Defining named users and restricting login to these named users only
 - Enabling Secure socket layer (SSL) connections between the server and clients
 - Enabling shared Mandanten file restrictions

In some cases, these five levels of access restrictions describe the same settings. In such cases, Service Manager uses the following precedence to determine what access restrictions apply:

1. Settings in the initialization file override all other security settings
2. Tailoring settings override security settings in individual operator records and the System Wide Company Record
3. Settings in an individual operator records and Mandanten override security settings in the System Wide Company Record
4. Settings in the System Wide Company Record apply to all operators that have no other security settings

HP proprietary records

Some HP proprietary records in HP Service Manager are identified by the words **HP Proprietary** and are read-only. Having these records as read-only will help future Service Manager upgrades.

Ongoing maintenance

The Ongoing Maintenance menu enables a System Administrator to access an operator record to view user and contact information, application profile privileges, and the Mandanten utility. If you use the ongoing maintenance menu and have administrative rights, you can also access and control several users or a group from a single application.

As an Application Administrator, you can add or edit users and manage user profiles from within HP Service Manager applications. You can restrict certain user rights and control the forms that users see when they access different parts of an application.

Environment record

Each application has an Environment record, which defines options that affect the functionality of an application for all users. Some of the typical options stored in the Environment record include:

- Relationship model
- Access rights
- Default category

Service Manager record relationship models

HP Service Manager Service Desk relationship models are methods to control the relationships between records inside Service Manager. The Service Desk relationship models affect four record types: Service Desk interaction records, Incident Management incident records, Change Management change records, and Request Fulfillment records. A Service Desk Agent can:

- Open an incident, complaint, or request for information in Incident Management
- Open a request for change in Change Management

- Open a Request Fulfillment record to order a product or service

For example, if a user complains that a printer has stopped working and the Service Desk Agent determines that an older printer is not compatible with a new laptop, the agent can open a Request Fulfillment record to order a new printer for the user. Once the order is placed, the Service Desk Agent can close the interaction record and add the Request Fulfillment record number for the new printer to the resolution note of the interaction. The Request Fulfillment record is also associated to the interaction record, so that even though the interaction is at a closed status the agent can refer back to the closed interaction to check the status of the related Request Fulfillment record.

The following can be set in the Service Desk Environment Profile record and are models for managing Service Desk record relationships:

- **Full Service Desk Model:** In this model, the state of a Service Desk interaction record changes when each related record closes. The closed state of an interaction record depends on the notification value chosen for the "Notify By" field in the interaction record. For example, if the notification value is "Telephone," the interaction record has a required action before it is closed. This action describes why the customer must be contacted. It also prevents the interaction record from closing until all required actions are complete. In this case, the interaction record goes into the Callback state before it is closed. For more information, see [Full Service Desk model](#).
- **All Records close Independently:** In this model, all Service Desk interaction records close independently. The state of related records does not affect closing an interaction record, and closing the interaction record does not affect related records.
- **Close Interactions when Related Record closes:** In this model, when the last related record closes, the Service Desk interaction record closes.
- **Cannot close Related Record until Interactions are closed:** In this model, records related to a Service Desk interaction cannot close until the interaction record is closed.
- **Cannot close Interactions until Related Records are closed:** In this model, a Service Desk interaction record cannot close until all related Incident Management records, Change Management records, and Request Management records are closed.

Full Service Desk model

In this model, the state of a Service Desk interaction record changes when each related record closes, depending on the value of the **Notify By** field in the interaction record. The following notification options are available.

Option	Description
None	The interaction record closes.
E-mail	Service Desk sends an email to the contact listed in the interaction record. The email informs the contact that the related record is closed. Service Desk closes the interaction record.
Page	Service Desk sends a page to the contact listed in the interaction record. Service Desk closes the interaction record.
Telephone	The interaction record has a required action. This action describes why the customer must be contacted. It also prevents the interaction record from closing until all required actions are complete. The interaction record goes into the Callback state.

Status progression

HP Service Manager applications have a logical status progression as a Service Desk Interaction, Change, Change Task, Problem, Problem Task, Request, or Request Task moves through its individual life cycle. The following table describes the out-of-box status values that Service Manager assigns to these applications.

Application	Status progression
Change Management (Change)	Initial Closed
Change Management (Change Task)	Planned Ready Assigned In Progress Completed Completed with Problems Canceled Withdrawn Failed Blocked
Incident Management	Categorize Assign Work In Progress

Application	Status progression
	Pending Customer Pending Evidence Pending Vendor/Supplier Pending Other Resolved Suspended Closed
Problem Management (Problem)	Open Categorize Assign Work In Progress Deferred Pending Resolved Closed
Problem Management (Problem Task)	Planned Ready Assigned Work In Progress Pending Pending Review Closed
Service Desk	Open Categorize Assign In Progress Dispatched Resolved Suspended

Application	Status progression
	Withdrawal Requested Closed
Request Fulfillment	Open In Progress Pending Customer Suspended Fulfilled Closed Ordering Closed
Request Fulfillment (Request Task)	Planned Ready In Progress Pending Customer Pending Vendor/Supplier CMDB Update Pending Review Canceled Closed

Application profiles

Note: Application profiles are not used for modules using Process Designer (other than Knowledge Management). For more information, see ["Process Designer security model" on page 119](#).

Application profiles are security settings that determine which features a user can access from a particular HP Service Manager application. Each of the seven Service Manager applications has a set of application profiles that determine which features a user can see. An application profile defines the access settings that a particular business function or role has to the application. Typically, System Administrators assign application profiles as part of user role descriptions, but the administrator can also assign an individual application profile that overrides the default settings of a user role.

Users must have an application profile in their operator record to access any application. Each out-of-box application has a profile record named Default to use when a profile does not exist. Each application also has a setting to enable access to the application using only the Default profile.

For example, records in the smenv table store Service Desk rights and privileges information, such as whether a user can close a service desk interaction record. Profiles also store information that may affect the way an application looks and behaves, such as defining a personal search form for a user.

Application profile authentication

When a user attempts to access one of the applications, Service Manager does the following:

1. Retrieves the profile name from the operator record and accesses the profile record for the specific application.
2. If Service Manager cannot find a user profile, it uses the Default profile.
3. If Service Manager cannot find a user profile, and the setting to use the Default profile is disabled, the user is denied access to the application.

Approval delegation

Approval delegation is an optional feature that enables users with approval rights to temporarily delegate their approval authority to another qualified operator. Operators with the **Delegate Approvals** or **Can Delegate Approvals** option enabled in their application profiles can delegate some or all of their approvals by using the Approval Delegation wizard.

Using the **Approval Delegation** wizard, an operator can grant another qualified operator the right to temporarily view and act on items in his or her approval queue. The wizard offers the following delegation options:

- Delegate all approvals to another qualified operator
- Delegate approvals from a particular application to another qualified operator
 - Delegate approvals directly assigned to you as an operator
 - Delegate approvals assigned to you as a member of an approval group
- Delegate approvals from a specified start date to a specified end date

The **Approval Delegation** wizard enables an operator to create any number of approval delegation combinations, including delegating the same approvals to multiple operators at the same time.

Delegators can also update an existing approval delegation to change the delegation start and end dates, as well as change the delegate's name.

Note: HP Service Manager tracks all changes to approval delegations using the standard field auditing capability.

When delegates log on to Service Manager, they see both their own and any delegated approvals in their approval list. For security reasons, delegates always retain their original application profiles and operator records. Service Manager determines what temporary rights delegates have when they view or act on an approval.

Administering approval delegation

HP Service Manager supports approvals, and thus approval delegation, for the following applications:

- Change Management
- Request Fulfillment
- Service Catalog

To enable approval delegation for one of these applications, an Administrator must edit one of the application's security role records and select the **Can Delegate Approvals** option. Next, the Administrator must grant this security role to the operators who will be given approval delegation authority.

Note: If you want to support approval delegation for an application that does not support approvals out-of-box, you must first enable and customize approvals for the application.

Approval delegation never changes a delegate's original security role or operator record. Service Manager only changes a delegate's approval groups in memory when the following conditions occur.

- When the system notifies the delegate
- When a delegate views or acts on an approval

By default, Service Manager sends an email notification to the approval delegate when the following conditions occur:

- A new approval delegation is assigned to the delegate
- A new approval arrives in the approval owner's queue

Note: Service Manager also sends an email notification to the approval owner when a new approval arrives in the owner's queue. System Administrators can change the notification behaviors for approval delegation directly from the notification engine.

A delegated approval always retains its original operator assignment. Service Manager records the delegate's actions separately from the owner in the following new fields:

Field name	Label in approval record	Description
approved.by	Operator	The name of the operator who acted on the approval.
approved.for	Approved For	The name of operator who delegated the approval.

Note: Delegators and delegates can view these fields from the approval record and the approval log. However, in some cases, only a delegator may have the approval group necessary to view the records in the approval log. A delegate's temporary rights do not include viewing approvals in the log. In order to view approvals in the approval log, a delegate's application profile must include the required approval groups.

Enabling approval delegation

The **Can Delegate Approvals** security role setting controls whether an operator can view the **Approval Delegation** wizard.

Note: It is a best practice to only enable the **Delegate Approvals** or **Can Delegate Approvals** option for operators who can also view and approve objects in the application.

Refer to the following example for how to enable approval delegation for Change Management.

1. Log on to HP Service Manager as a System Administrator.
2. Click **System Administration > Security > Roles**.
3. In the **Name** field, type the name of the security role you want to grant approvals. For example, `change approver`.
4. Click **Search**. The **Security Roles** form opens.
5. Click **Change** in the **Area** column.

6. Under **Settings**, select the **Can Delegate Approvals** check box.

7. Click **Save**.

Global variables available for approval delegation

HP Service Manager provides global variables for approval delegation. Administrators can use these global variables to create their own custom queries or views.

Global variable	Description
\$G.delegated.cm3r.groups	Stores the assignment groups that are associated with Change Management changes that the current operator can view and act on as an approval delegate.
\$G.delegated.cm3t.groups	Stores the assignment groups that are associated with Change Management tasks that the current operator can view and act on as an approval delegate.
\$G.delegated.ocmq.groups	Stores the assignment groups that are associated with Request Management that the current operator can view and act on as an approval delegate.
\$G.delegated.svc.groups	Stores the assignment groups that are associated with Service Catalog that the current operator can view and act on as an approval delegate.

What happens when I receive delegated approval authority?

If an operator delegates his or her approval authority to you, HP Service Manager sends an email to notify you of the new approval delegation. You are also notified when a new approval arrives in your approval queue.

Viewing approvals

When you log on to Service Manager, you will see both your own and any delegated approvals in your approval queue.

- To view approvals that another operator has delegated to you, you can use the **Active approval delegations assigned to me** view.
- To view approvals delegated to you in the past, you can use the **Past approval delegations assigned to me** view.

- To see which items in the approval queue are due to an active approval delegation, you can open the **Approve Requests** view from the System navigator. In this view, Service Manager indicates which approvals are in the queue due to an active delegation by displaying a value of **YES** in the As Delegate? column. You can use this view to view, approve, or deny approval requests.

Tracking approval actions

As a delegate, when you act on an approval, Service Manager tracks your actions by adding both your operator name and the delegator's operator name to the approval record.

- Service Manager lists your name in the Operator column of the Completed Approval Actions table.
- Service Manager lists the delegator's name in the Approve For column of the Completed Approval Actions table.

After the approval delegation expires

When an approval delegation expires, you are no longer considered a temporary member of the delegator's approval groups. This means that you can no longer view or act on items that belong exclusively to the delegator's approval groups. The restriction includes any approvals that you previously acted on during the delegation period. In some cases, this may mean that only the delegator can see a particular approval record.

Temporary rights of an approval delegate

An approval delegate temporarily gains the rights for the assignment group of the delegating operator while the approval delegation is active. After the approval delegation period ends, the delegate's temporary rights for the assignment group revert to their original status.

Approval delegation never changes a delegate's original application profile or operator record. HP Service Manager only changes a delegate's assignment group rights in memory when the following conditions occur.

- When the system notifies the delegate
- When a delegate views or acts on an approval

For example, a manager wants to delegate approval authority to a technician. When the manager delegates approval authority to the technician, the technician temporarily becomes a member of all of the assignment groups that the manager is an approver of.

What happens when I delegate approval authority?

When you delegate approval authority to a qualified operator, the delegate receives an email notification. Delegates are also notified when a new approval arrives in their approval queues.

As a delegator, you always retain your normal approval authority. Both you and any delegates you authorize have the ability to approve items while an approval delegation is active.

Viewing approvals

As a delegator, when you log on to HP Service Manager, you will see both your own and any delegated approvals in your approval queue.

- To view your active approval delegations, you can use the **Approval Delegation** wizard or the **My active approval delegations** view.
- To view your past delegations, you can use the **Copy Approval Delegation** wizard or the **My past approval delegations** view.

Tracking approval actions

When a delegate acts on an approval, Service Manager tracks the delegate's actions by adding both the delegate's operator name and your operator name to the approval record.

- Service Manager lists the delegate's name in the Operator column of the Completed Approval Actions table.
- Service Manager lists the delegator's name in the Approve For column of the Completed Approval Actions table.

After the approval delegation expires

When an approval delegation expires, a delegate is no longer considered a temporary member of your approval groups. This means that the delegate can no longer see or act on items that belong exclusively to your assignment groups. The restriction includes any approvals that the delegate previously acted on during the delegation period. In some cases, this may mean that only you as delegator can see a particular approval record.

Delegate approvals to another operator

Applies to User Roles:

System Administrator and other users with approval delegation authority

You can only delegate approvals to another operator if a System Administrator enables the **Delegate Approvals** or **Can Delegate Approvals** option for you in your security role.

To delegate approvals to another operator, follow these steps:

1. Click **Approval Delegation**. The **Approval Delegation** wizard opens and displays any active approval delegations assigned to you.
2. To create a new approval delegation, click **Add New Delegation**.
3. Select whether to delegate all your approvals or to select approvals.
4. If you are selecting approvals, make the following choices:
 - a. Choose which application's approvals you want to delegate.
 - b. Choose how you want delegate approvals assigned to you:
 - Assigned as part of an assignment group
 - Assigned directly to you as an operator

Note: You can select multiple assignment groups or operators as needed.

5. Select the delegate to whom you want to grant approval authority.

Note: HP Service Manager only displays operators who are eligible approval delegates. If you do not see a particular operator listed as a potential delegate, it means that the operator does not have one or more of the rights required to be eligible for approval delegation. Consult your System Administrator if you want to assign additional rights to a particular operator.

6. Select the date range during which the approval delegation will be active.

Update an active approval delegation

Applies to User Roles:

System Administrator and other users with approval delegation authority

You can change the delegate, the start date, or the end date of any currently active approval delegation by using the Approval Delegation wizard. If you want to use a delegation as a template for a new delegation, use the Copy Approval Delegation wizard.

Note: To change approvals delegated by a specified assignment group or operator name, you must disable the current delegation and create a new one with the new assignment groups and operator names. HP Service Manager requires a new delegation in order to determine which operators are qualified to be delegates.

To update an active approval delegation, follow these steps:

1. Click **Approval Delegation**. The **Approval Delegation** wizard opens and displays any active approval delegations assigned by you.
2. Select the approval you want to edit from the list of active delegations.
3. Click **Edit Current Delegation**.
4. Select the new start and end dates for the approval delegation.

Note: Service Manager dates always default to midnight (00: 00: 00) of the selected day. If you want to set a different start time, manually type in the new start time using the twenty-four hour: minute: second format notation. For example 23 : 59 : 59 represents 11: 59 PM and 59 seconds.

5. Click **Next** to save your changes and close the wizard.

Disable an active approval delegation

Applies to User Roles:

System Administrator and other users with approval delegation authority

You can disable any currently active approval delegation. You cannot disable an inactive past delegation.

To disable an active approval delegation, follow these steps:

1. Click **Approval Delegation**.

The **Approval Delegation** wizard opens and displays any active approval delegations assigned by you.

2. Select the approval you want to disable from the list of active delegations.
3. Click **Edit Current Delegation**.
4. Clear the **Enabled** check box.
5. Click **Next** to save your changes and close the wizard.

Note: To view your past delegations or delegations assigned to you, use one of the default approval delegation views.

Copy an approval delegation

Applies to User Roles:

System Administrator and other users with approval delegation authority

You can use an existing approval delegation as a template to create a new approval delegation. The wizard copies the values from the existing delegation and allows you to change the delegate and the delegation dates. You cannot change the application module, delegated approval groups, or operator when copying an approval delegation. If you want to change these values, you must create a new approval delegation.

To copy an approval delegation, follow these steps:

1. From the **To Do** view, select **Approval Delegation** from the **Queue** list. HP Service Manager displays the Approval Delegation view.
2. From the **View** list, select either **My active approval delegations** or **My past approval delegations**.
3. Select the approval you want to copy from the list of approval delegations.
4. Click **Copy Approval Delegation**. Service Manager displays the Copy Approval Delegation wizard and automatically fills in the delegate name, the delegated module, approval groups, and operator.

5. Select the new delegate if needed.
6. Select the new delegation start and end dates.
7. Select **Enabled**.
8. Click **Next** to create a new approval delegation.

Views available for approval delegation

HP Service Manager provides default views for delegators and delegates to manage approval delegations. Administrators can also view approval delegation records directly from the Database Manager by viewing the ApprovalDelegation table.

View	Description	Available Actions
My active approval delegations	A list of the currently active approvals that you delegated to other operators. This view does not display future delegations because they are not currently active.	<ul style="list-style-type: none"> • Start the Approval Delegation wizard • Export • Print
My past approval delegations	A list of the inactive approvals that you delegated to other operators in the past.	<ul style="list-style-type: none"> • Start the Copy Approval Delegation wizard • Export • Print
Active approvals assigned to me	A list of the currently active approvals delegated to you. This view only displays approvals where you are the active delegate. Use the other views to display your past or pending delegations.	<ul style="list-style-type: none"> • Export • Print
Past approvals assigned to me	A list of the inactive approvals that other operators have delegated to you in the past.	<ul style="list-style-type: none"> • Export • Print

Note: If you create or update an approval delegation record you may need to use the Service Manager **Refresh** option in order for the views listed above to display the new delegation record.

User roles

The Service Management process can meet best practices when employees involved in the process are assigned user roles in your IT organization. For information on the Service Management organizational model of user roles for best practices, see *HP Service Manager Processes and Best Practices Guide* in the related topics.

A user role is a template that combines a collection of application profiles, security roles, and capability words into a single record. Service Manager provides out-of-box user role descriptions with appropriate capability words and application profiles that define a variety of business functions or roles. By defining and assigning user role descriptions, a System Administrator can grant an operator the capability words and application profile required for a particular job.

The Service Management process consists of the following user roles:

Add a user role record

Applies to User Roles:

System Administrator

A user role defines a set of application profiles, capability words, and query groups that you can apply to any operator record. For example, the self-service role enables the self-service user to open, view, update, and close service requests.

To add a user role record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > User Roles**.
2. Enter a User Role or click **Search** to select a role from a record list.
3. Add optional information to the form. If necessary, press **Ctrl + H** to view help for each field.
4. Click **Add**.

Note: Service Manager provides an out-of-box self-service user role record.

Delete a user role record

Applies to User Roles:

System Administrator

To delete a user role record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > User Roles**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the user role that you want to delete.
5. Click **Delete**.
6. Click **Yes** to confirm the deletion.

Search for a user role record

Applies to User Roles:

System Administrator

To search for a user role record, follow these steps:

1. Click **System Administration > Ongoing Maintenance > User Roles**.
2. Click **Search** to select a role from a record list.

Set database access for a user role

Applies to User Roles:

System Administrator

Database access is a feature that gives you the ability to limit or grant access to database records, such as contacts, company, and regions. You can add or modify the existing out-of-box database access settings per user role or operator.

To set database access for a user role, follow these steps:

1. Click **System Administration > Ongoing Maintenance > User Roles**.
2. Type or select optional search criteria, and then click **Search**.
3. Select a user role from the record list.
4. Select the **Data Access** tab.
5. To add a new Data Access record, follow these steps:

- a. Click **Data Access Records**.

The **Database Manager Data Access** form opens.

- b. Click **Fill** in the **Database Table Name** field to select a table.
- c. The user role you initially selected is in the **User Role** field. If you want to add access to a different user role than the one you selected, clear the field and click **Fill** to select a different user role.
- d. To set the database access, select one of the following:
 - **Allow DB access:** The user role specified is granted access to the table specified.
 - **Prohibit DB access:** The user role specified is denied access to the table specified.
- e. When access has been granted to a table, click **Fill** in the **View Format** field to select the table view.
- f. Click **Add**.

The new database access record is added.

6. To modify an existing database access record, follow these steps:

- a. Select the **Data Access** tab.
- b. Double-click the Table Name of the existing database access record you want to modify.

The **Database Manager Data Access** form opens.

- c. Make the necessary edits.

- d. Click **Save**.

Your changes are saved.

7. Click **OK**.

Capability word model

Capability words provide a security mechanism to control access to HP Service Manager applications by enabling or disabling parts of the interface. You can add capability words to a user role or individual operator to control access to Service Manager. In some cases capability words are redundant to the privileges and views that are already provided by application profiles. In cases where capability words and application profiles overlap, capability words take precedence.

Service Manager stores capability words in the capability table, which you can access by opening the capability form in Database Manager, or by clicking **System Administration > Ongoing Maintenance > Capability Words**. To limit access, choose a subordinate capability word. To grant a broad range of permissions, choose a parent capability word, such as SQLAdmin or SysAdmin. If you create your own capability words or modify the default permissions, you can use the JavaScript functions `checkPermission()` and `checkExclusivePermission()` available in the script library to determine if an operator has a particular capability word. You must use these functions to enforce the capability word model.

Capability words

HP Service Manager provides a hierarchy of out-of-box capability words.

Note: Capability words are case-sensitive.

Capability	Primary subordinate	Secondary subordinate	Application	Description
EditContacts			Any application mainly for admins to edit contacts (Administration)	Enables editing of contact records.
EditOperators			Any application mainly for	Enables editing of the password in

Capability	Primary subordinate	Secondary subordinate	Application	Description
			admins to edit operators (Administration)	operator records. If you are not SysAdmin, without this capability word even if you could edit some other operator information you wouldn't be able to change the password.
fscfull			Calendar	Enables full access and the ability to open and update change records from the web
fscread			Calendar	Enables read capability to FSC web calendar
ODBC			Server Access	Grants access via ODBC32.DLL for reporting.
SOAP API			Web Services	Enables the user to login to Service Manager and execute a SOAP API request.
SQLAdmin			SQL	Enables SQL administrator authority.
	Db2Admin		DB2	Enables DB2 administrator capability.
SysAdmin			All Applications	Enables system administrator capability (i.e., everything).
	system.build		Administration	Grants access to old binary text format unload options.

Capability	Primary subordinate	Secondary subordinate	Application	Description
				These are used to create a Service Manager file system from scratch and must always be available to someone.
	programmer		RAD	Grants access to the application generator (ag).
		Debug	Debugger	Enables a non-sysadmin user to do debugging for testing purposes. Normal users should not have this capability word unless there is debugging being done for that user.
	AlwaysAdmin		Database Manager	Defaults administration mode to true when using the Database Manager.
	ChMAdmin		Change Management	Grants access to Change Management administration.
		change request	Change Management	Grants access to Change Management requests.
		change task	Change Management	Grants access to Change Management tasks.
		expedite change	Change Management	RFC management: this person may expedite changes.
	GUIAdmin		User Interface	Grants access to GUI

Capability	Primary subordinate	Secondary subordinate	Application	Description
				administration.

Capability	Primary subordinate	Secondary subordinate	Application	Description
		chart.breakdown	Charts	Enables the charting capability in the Service Manager client.
		public.favorites	Favorites	Enables public favorites in the Windows / and Web client.
		user.favorites	Favorites	Enables the user favorites in the Windows / and Web client.
	menu.commands		Command line	Grants command line access to functions from menu.
	ICMAdmin		Configuration Management	Grants access to Configuration Management administration.
	inventory management		Configuration Management	Grants access to Configuration Management.
	help		Help	Enables the user to add or update help records
	IncidentAdmin		Incident Management	Grants access to Incident Management administration.
		amend suspension	Incident Management	Enables the capability to amend the Incident Management profile rights for suspend/unsuspend.
		incident management	Incident Management	Grants access to Incident Management.

Capability	Primary subordinate	Secondary subordinate	Application	Description
	KMAdmin		Knowledge Management	The KMAdmin capability word enables a user to perform all Knowledge Management and Knowledge Centered Support (KCS) tasks for all document categories including the administrative tasks associated with maintaining the Knowledge Management system.
	knowledge engineer		IR Expert	Enables the capability to modify the adaptive learning records.
	mobile.admin		Mobile	Grants access to the HP Portal for mobile user administration.
		mobile.user	Mobile	Grants access to the HP Portal for mobile users.
	ProbAdmin		Problem Management	Grants access to Problem Management administration.
		problem management	Problem Management	Grants access to Problem Management.
	query.window		Queries	Grants access to query window function in query.window application.
	QueryAdmin		Queries	Enables query administrator

Capability	Primary subordinate	Secondary subordinate	Application	Description
				capability. Full access to query options/maintenance. Includes: query window, stored query usage and editing, etc. This is intended to be used like sysadmin, as an administrator, not for general usage. Please use caution assigning this as it gives access to create/modify stored queries, which can adversely affect system performance if not done correctly.
		mod.time.limit	Queries	Enables the user to modify the default time limit for a partial key query entered in either Database Manager or Change Management.
		partial.key	Queries	Enables the user to execute a partial key query in Database Manager or Change Management.
		partial.key.msg.skip	Queries	Enables the user to skip the partial key query message in Database Manager.
		query.stored	Queries	Enable user to execute stored queries when F6 (query) key is pressed, from any application. The user

Capability	Primary subordinate	Secondary subordinate	Application	Description
				will be able to perform any stored query assigned to him/her or a group he/she belongs to (allowable groups in operator record).
		query.stored.mod	Queries	Enable user execute/modify access of stored queries when F6 (query) key is pressed from any application.
	OCMAdmin		Request Fulfillment	Allows access to Request Fulfillment administration, such as the approval delegation application.
		OCML	Request Fulfillment	Allows access to the legacy Request Management Line Item applications. Since Line Item is not supported in Request Fulfillment in Server Manager Codeless mode, it can be considered obsolete if you do not use it anywhere else.
		OCMO	Request Fulfillment	Allows access to Request Fulfillment order records.
		OCMQ	Request Fulfillment	Allows access to Request Fulfillment request records in the approval delegation application.

Capability	Primary subordinate	Secondary subordinate	Application	Description
	svcCatAdmin		Service Catalog	Grants access to Service Catalog administration.
		service catalog	Service Catalog	Enables users to request items from catalog.
		svcCatDeptRequester	Service Catalog	Enables a department to request items from catalog.
		svcCatEmployeeRequester	Service Catalog	Enables an employee to request items from catalog.
		svcCatManagerRequester	Service Catalog	Enables a manager to request items from catalog.
		svcCatTechRequester	Service Catalog	Enables a technician to request items from catalog.
		svcCatRequestOnBehalf	Service Catalog	Enables an employee self-service (ESS) user to submit a service catalog request on behalf of another user.
	SDAdmin		Service Desk	Grants access to Service Desk administration.
		service desk	Service Desk	Grants access to Service Desk.
	data administrator		Service Desk, Incident Management	Enables save, add and update on supporting tables from within Service Management and Incident Management.
	user		User	Grants basic access

Capability	Primary subordinate	Secondary subordinate	Application	Description
				to an end user but does not grant the ability to add, delete, or reset.

Add a capability word

Applies to User Roles:

System Administrator

To add a capability word, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Capability Words**.
2. Type the information for your new capability word.
3. Click **Add**.

Delete a capability word

Applies to User Roles:

System Administrator

To delete a capability word, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Capability Words**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the capability word that you want to delete.
5. Click **Delete**.
6. Click **Yes** to confirm the deletion.

Search for capability words

Applies to User Roles:

System Administrator

To search for capability words, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Capability Words**.
2. Type or select optional search criteria.
3. Click **Search**.

Operator passwords

Passwords play a major part in controlling system security within HP Service Manager. To protect your system from unauthorized access, you can require passwords for every operator.

A System Administrator can change any operator password. Users can also change their own passwords, unless the System Administrator denies operators password modification privileges.

A System Administrator can also set password format restrictions and time limits from the System Information Record. The System Administrator can set the following password options:

- Format requirements
- Maximum and minimum lifetimes
- Default password for reset passwords

Change a user's password

Applies to User Roles:

System Administrator

Note: A System Administrator can both change and reset a user password. Changing an operator password permanently changes the password. Resetting an operator password temporarily changes the password until the operator next logs in at which time HP Service Manager prompts the operator to change the password.

To change a user password, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.

3. Click **Search**.
4. Select the operator with password to be changed.
5. Click the **Security** tab.
6. In the **Password** field, type the new password for the operator.
7. Click **Save**.

Disable the password reset option

Applies to User Roles:

System Administrator

To disable the password reset option, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **Passwords** tab.
3. Select the **Prevent Pwd Resets** option.
4. Click **Save**.

Enable password history

Applies to User Roles:

System Administrator

To enable password history, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **Password Standards** tab.
3. Select the **Keep Password History** option.
4. Click **Save**.

Enable the password reset option

Applies to User Roles:

System Administrator

The **Reset Operators Password** option provides temporary passwords. However, when you reset an operator password, HP Service Manager does not verify that the new password conforms to any of the password standards that you can define in the company record.

To enable the password reset option, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **Password Standards** tab.
3. Select one of the following options.

Password reset option	Description
Prevent Pwd Resets	Select this option to remove Reset Operators Password from the More Actions menu. You can still manually change operator passwords from the operator record.
Reset to User Name	Select this option to reset the operator password to the log-in name whenever an administrator chooses Reset Operators Password from the More Actions menu.
Prompt for Value	Select this option to display a dialog box where an administrator can enter a new password whenever the administrator chooses Reset Operators Password from the More Actions menu.
Reset to Value	Select this option to reset an operator password to the value you type in the text field whenever the administrator chooses Reset Operators Password from the More Actions menu.

4. Click **Save**.

Reset an operator's password

Applies to User Roles:

System Administrator

To reset an operator password, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Use search or advanced search to find one or more records.
3. Select the operator record from the record list.
4. Click **More** or the **More Actions** icon, and then select **Reset Operators Password**.
5. Click **Yes** to confirm the operation.

When you reset an operator password, HP Service Manager does not verify that the new password conforms to the password standards that you defined in the company record. Therefore, use the **Reset Operators Password** option to provide only temporary passwords.

Set password format restrictions

Applies to User Roles:

System Administrator

To set password format restrictions, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **Password Composition** tab.
3. Type or select the following options:
 - **Min Password Length**: type the minimum number of characters a password can contain.
 - **Max Password Length**: type the maximum number of characters a password can contain.
 - **Allow Alpha Characters**: select this option to allow users to create passwords with alphabetical characters.
 - **Allow Numeric Characters**: select this option to allow users to create passwords with numeric characters.
 - **Allow Symbolic Characters**: select this option to allow users to create passwords with symbolic characters.

Note: HP Service Manager prevents users from creating passwords that start with the following symbolic characters: pound (#), equal sign (=), tilde (~), greater than (>), and less than (<).

- **Always Require a Password:** select this option to require all users to have a password defined in their operator record. This option is the only way to prevent users from having blank passwords.

Caution: Users who currently have blank passwords defined in their operator record can still log in until they are required to change their passwords.

- **Require Alpha Chars:** select this option to require users to create passwords that contain at least one alphabetical character.
 - **Min Required:** type the minimum number of alphabetical characters a password must contain. This value must be a positive integer if you select the **Require Alpha Chars** option.
- **Require Mixed Case:** select this option to require users to create passwords that contain both upper case and lower case alphabetical characters.
- **Require Non-Alpha Chars:** select this option to require users to create passwords that contain at least one numerical or symbolic character.
 - **Min Required:** type the minimum number of numerical characters a password must contain. This value must be a positive integer if you select the **Require Non-Alpha Chars** option.
- **Prohibit Space Character:** select this option to prohibit users from creating passwords that contain the space character.

4. Click **Save**.

Caution: The only way to prevent users from defining blank passwords is to select the **Always Require a Password** option.

Set password maximum lifetimes

Applies to User Roles:

System Administrator

To set password maximum lifetimes, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **Password Lifetime** tab.
3. Type or select the following options:
 - **No Max Lifetime**: select this option to disable password expiration.
 - **Use Time Period**: select this option to have passwords expire after a set time period.
 - **Max Pwd Lifetime**: type the number of days, hours, minutes, and seconds before user passwords expire.
Type the time period in the following format: *Dayshours: minutes: seconds*. For example, 4 03: 02: 01 expires user passwords after 4 days, 3 hours, 2 minutes, and 1 second.
 - **Use Number of Logins**: select this option to have passwords expire after a set number of user logins.
 - **Max before change**: type the number of logins before user passwords expire.
 - **Notify by Email on Password Change**: select this option to notify users by email whenever another user, such as a System Administrator, changes their password.
4. Click **Save**.

Set password minimum lifetimes

Applies to User Roles:

System Administrator

To set password minimum lifetimes, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **Password Lifetime** tab.
3. Type or select the following options:

- **No Min Lifetime:** select this option to disable password expiration.
- **Use Time Period:** select this option to have passwords expire after a set time period.
 - **Min Pwd Lifetime:** type the number of days, hours, minutes, and seconds before user passwords expire.

Type the time period in the following format: *Dayshours: minutes: seconds*. For example, 4 03: 02: 01 expires user passwords after 4 days, 3 hours, 2 minutes, and 1 second.

- **Use Number of Logins:** select this option to have passwords expire after a set number of user logins.
 - **Min before change:** type the number of logins before user passwords expire.
- **Notify by Email on Password Change:** select this option to notify users by email whenever another user, such as a System Administrator, changes their password.

4. Click **Save**.

License tracking

HP Service Manager tracks floating and named licenses on the application level for reporting purposes.

The logon process determines which applications are authorized for each user, allocates a floating or named license for the duration of the session, and records usage information in the stathistory file. When the user logs out or ends the session, Service Manager deallocates the license. Because Service Manager tracks the highest daily license usage for each application, administrators can use this information to determine how many licenses are being used and when peak usage times occur. They can enable or disable user license tracking at any time.

The license tracking feature tracks the named and floating licenses on an application basis. Service Manager refreshes the license usage information whenever the user logs out, or the session terminates by inactivity or administrator action.

Authorized applications

The following applications monitor licenses:

- Contract Management
- Change Management

- Incident Management
- Configuration Management
- Request Fulfillment
- Problem Management
- Service Desk
- Knowledge Management
- Service Level Management
- Smart Analytics

The Database Administrator can enable and disable the application license tracking feature. Service Manager applications contain logic to ensure license usage accuracy.

License types

There are two types of license: login license (named or floating, which just controls the initial login), and the application license for individual module access.

License type	Description
Login license	Controls the initial login: <ul style="list-style-type: none">• Floating: Users are not on the Named user list for the application and they have update capabilities.• Named: Users are on the Named user list for the application and they have update capabilities.
Application license	Controls individual module access. Logging in as any user with update capacity for an application consumes a license for that application. Update capacity includes permission to add, update, or delete any record associated with the application.

Login licenses are tightly controlled so that the product will not allow you to log in if you exceed your login licenses. Application licenses are lightly controlled, and you can exceed the licenses with only a warning message.

If the Named Application field in the operator record is empty and the operator logging in is a Named user, the user will consume one named login license and floating licenses for application license. If the

Named Application field in the operator record is only filled with, for example, Incident Management, the same user will consume one named login license, one floating license for each other application/module, and one named license for the Incident Management application/module. In other words, by default the Application Licenses are floating licenses regardless of whether the operator is a named or floating user.

Login licensing has been separated from Module licensing to provide more flexibility. It is possible to change the default behavior to ensure the Named user consumes a Named license, instead of a Floating license for the Modules. To do so, follow these steps:

1. Open the Operator record.
2. Click the **Login Profiles** tab, add the Modules required for the Named user in the **Named Applications** field.

Profile fields for Configuration Management license tracking

Users who have the capability to update records in Configuration Management will consume either a Floating or Named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Configuration Management security profile (icmenv) will consume a Configuration Management license.

Label	Field Name in icmenv
New	new
Delete	delete
Update	update
Change device type	change.devtype
Template Mass Update	db.template
Complex Mass Update	db.complex
Mass Delete	mass.delete

Profile fields for Knowledge Management license tracking

Users who have the capability to update records in Knowledge Management will consume either a Floating or Named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Knowledge Management security profile (kmprofile) will consume a Knowledge Management license:

KCS I

Label	Field Name in kmprofile
Contribute New Knowledge	contribute
Save a Draft Copy	save.draft
Edit working copy documents in Knowledge Management	edit.in.workflow

KCS II

Label	Field Name in kmprofile
Publish internal immediately	int.immediate
Retire / Archive a document	retire
Publish a working copy document internally	internal
Unretire a retired document	unretire
Modify a published document	modify
Delete a retired document	delete.doc
Revert a working copy to the published version	revert
Delete Feedback	delete.feedback

KCS III

Label	Field Name in kmprofile
Publish internal and external immediately	ext.immediate
Publish a working copy document internally and externally	external

Admin

Label	Field Name in kmprofile
Manage document types and views	doctype
Manage Categories	manage.categories
Manage knowledgebases	knowledgebases
Integration Mapping	integration.mapping
Manage shared content	shared.content
Configure hit list	configure.hit.list
Manage environment and profiles	environment.profiles

Admin, continued

Label	Field Name in kmprofile
Review/publish any draft	any.draft
Search in all categories	admin.search.all
Edit Adaptive Learning	edit.adaptive.learning

Profile fields for Contract Management license tracking

Users who have the capability to update records in Contract Management will consume either a Floating or Named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Contract Management security profile (ctenv) will consume a Contract Management license.

General Privileges

Label	Field Name
Mass Add	mass.add
Mass Update	mass.update
Mass Delete	mass.delete

Contracts

Label	Field Name
Add Contract	add.contract
Update Contract	update.contract
Cancel Contract	cancel.contract
Renew Contract	renew

Payments

Label	Field Name
Schedule Payment	sched.payment
Gen Payment Sched	gen.payment.sched
Update Payment	update.payment
Submit Payment	submit.payment
Cancel Payment	cancel.payment

Payments, continued

Label	Field Name
Delete Payment	delete.payment

Contract Templates

Label	Field Name
Create Template	create.template
Update Template	update.template
Delete Template	delete.template

Asset Allocation

Label	Field Name
Add Asset	add.items
Gen Asset Allocation	gen.item.allocation
Update Asset	update.items
Delete Asset	delete.items

Software Counters

Label	Field Name
Create Counter	add.counter
Update Counter	update.counter
Delete Counter	delete.counter
Compliance Check	compliance.check

Terms and Conditions

Label	Field Name
Add Term/Condition	add.term
Update Term/Condition	update.term
Delete Term/Condition	delete.term

Security right fields for Service Desk license tracking

Users who have the capability to update records in Service Desk will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Service Desk security rights will consume a Service Desk license.

Area	Tab	Label of Settings	Value
Service Desk	Rights	New	true
Service Desk	Rights	Update	Always/When assigned/When assigned to work group
Service Desk	Rights	Delete/Close	Always/When assigned/When assigned to work group

Security right fields for Incident Management license tracking

Users who have the capability to update records in Incident Management will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Incident Management security rights will consume an Incident Management license.

Area	Tab	Label of Settings	Value	Can do
Incident Incident Tasks	Rights	New	true	New
Incident Incident Tasks	Rights	Update	Always/When assigned/When assigned to workgroup	Update
Incident Incident Tasks	Rights	Delete/Close	Always/When assigned/When assigned to workgroup	Close/Inactivate/Mass Inactivate
Incident Incident Tasks	Rights	Expert	true	Can suspend/ Can unsuspend

Security right fields for Problem Management license tracking

Users who have the capability to update records in Problem Management will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Problem Management security rights will consume a Problem Management license.

Area	Tab	Label of Settings	Value
Problem Problem Tasks	Rights	New	true
Problem	Rights	Create Known Error	true
Problem Problem Tasks	Rights	Update	Always/When assigned/When assigned to workgroup
Problem Problem Tasks	Rights	Delete/Close	Always/When assigned/When assigned to workgroup

Security right fields for Change Management license tracking

Users who have the capability to update records in Change Management will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Change Management security rights will consume a Change Management license.

Area	Tab	Label of Settings	Value	Can do
Change/Change Task	Rights	New	true	Copy and Open/New
Change/Change Task	Rights	Expert	true	Update when closed/Can Mass Approve
Change/Change Task	Rights	Admin	true	Change Category/Change Phase/Can override Approvals
Change/Change Task	Rights	Update Delete/Close	Always/When assigned/When assigned to workgroup	Update/delete/Close

Area	Tab	Label of Settings	Value	Can do
Change/Change Task	Settings	Reopen/Can Approve	true	Reopen/Can Approve

Security right fields for Request Fulfillment license tracking

Users who have the capability to update records in Request Fulfillment will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Request Fulfillment security rights will consume a Request Fulfillment license.

Area	Tab	Label of Settings	Value	Can do
Request/Request Tasks	Rights	New	true	New
Request/Request Tasks	Rights	Expert	true	<ul style="list-style-type: none"> Update Mass Approve
Request/Request Tasks	Rights	Admin	true	Override (Approve.Override)
Request/Request Tasks	Rights	Update Delete/Close	Always/When assigned/When assigned to workgroup	Close
Request	Settings	Can Approve	true	Can Approve
Request	Settings	Reopen	true	Reopen

Security right fields for Service Level Management license tracking

Users who have the capability to update records in Service Level Management will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have update capabilities for any of the following fields in the Service Level Management security rights will consume a Service Level Management license.

Area	Tab	Label of Settings	Value
Service Level Management	Rights	New	true

Area	Tab	Label of Settings	Value
Service Level Management	Rights	Update	Always/When assigned/When assigned to workgroup
Service Level Management	Rights	Delete/Close	Always/When assigned/When assigned to workgroup
Service Level Management	Settings	Manage SLT Catalog Records	true

Capability words for Smart Analytics license tracking

Users who have the capability to update records in Smart Analytics will consume either a floating or a named license. HP Service Manager tracks these licenses for reporting purposes.

Users who have the **SysAdmin** or **idol.assistant** capability word will consume a Smart Analytics license. If there is no Help Desk license, Smart Analytics cannot work.

Disable application license tracking

Applies to User Roles:

System Administrator

You must have administrative access to the database to perform this procedure.

To disable application license tracking, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **General** tab.
3. Select the **Disable Application License Tracking** check box.
4. Click **Save**.

Named users

HP Service Manager uses the software license agreement, which provides for two types of licensed users: named users and floating users.

Named users are users who are always authorized to log on to the Service Manager system when either floating user licenses or named user licenses are available. Floating users are limited to a maximum

number of concurrent logins as defined by the floating user license. The Service Manager license key password file encodes the number of named users and floating users in the system as separate values. You can define as many named users as you want. If the number of named users logged on exceeds the limit of named user licenses, the surplus named users consume floating licenses to log on to the Service Manager system. Floating users also consume floating licenses when they log on. If all of your floating licenses have been used, Service Manager denies access to any additional unique floating users. Unique named users will still be able to log in if Named licenses are available. If all named licenses and floating licenses are used, no additional unique users (named or floating) will be able to connect.

Defining named users

You can use the following method to define named users on your HP Service Manager system:

- Define each named user in the user's operator record

Determine the number of named users available

Applies to User Roles:

System Administrator

You must have access to the HP Service Manager server to perform this procedure.

To determine the number of named users available, follow these steps:

1. Open a Windows command prompt window.
2. Change directories to the RUN folder of your Service Manager installation.
3. Type the following command:

```
sm -reportlic
```

4. Press **Enter**.

Service Manager displays a report of your licensed features and your current usage. The Named Users field lists the number of named users that are active and inactive on your system.

Make an individual operator a named user

Applies to User Roles:

System Administrator

To make an individual operator a named user:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select the operator record from the record list.
5. Click the **Login Profiles** tab.
6. Select the **Named User** option.
7. Click **Save**.

Named users for applications

HP Service Manager tracks floating and named licenses for each application based on the number of users with the ability to update records in the application. Administrators can define a user as a named User for the application in the operator record or in the nameduser table.

Triggers keep the operator records and named user records synchronized. When you update the named.modules field in the operator record, Service Manager also updates the respective named user record. If you update a named user record; Service Manager updates the corresponding operator record.

Note: The out of box SM Reports module includes license utilization reports.

Define named users for applications

Applies to User Roles:

System Administrator

You can grant access and update rights to named users.

To define named users for applications by using the Named Applications method, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.

4. Select the operator record to update.
5. Click the **Login Profiles** tab.
6. In the **Named Applications** field, type or select the application for which you want to enable operator access.
7. Click **Save**.

Note: If you want to grant access and update rights for multiple named users in a specific application, you can do this using the Named User method in Database Manager.

To define named users for applications by using the Named User method, follow these steps:

1. Click **Tailoring > Database Manager**.
2. In the **Form** field, type `nameduser`
3. Type or select optional search criteria.
4. Click **Search**.
5. In the **Application** field, specify the application to be accessed by the operator.
6. In the **Named users** field, type or select the operators to be assigned update rights for the specified application.
7. Click **Save**.

Disable application license tracking

Applies to User Roles:

System Administrator

You must have administrative access to the database to perform this procedure.

To disable application license tracking, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **General** tab.

3. Select the **Disable Application License Tracking** check box.

4. Click **Save**.

HP Service Manager license report

--- HP Service Manager License Report ---

Permanent License.

Server Quiesced State : Allow All Logins

(Licensed)		Licensed Module Usage	Named(Licensed)	Float
		IR Expert(Foundation)	Enabled	
		Configuration Management(Foundation)	1(25)	0(
25)		Desktop Administration(Foundation)	0(25)	0(
25)		HP SOAP API SDK for SC/SM(Foundation)	Enabled	
		HP SCAuto for HP Network Node Manager(Foundation)	Enabled	
		HP SCAuto for HP Operations (ITO/VPO)(Foundation)	Enabled	
		HP SCAuto for Email(Foundation)	Enabled	
		Self-Service Ticketing(HelpDesk)	UnLimited	
		Incident Management(HelpDesk)	0(100)	1(
100)				
		Service Desk(HelpDesk)	0(100)	1(
100)				
		Problem Management(HelpDesk)	0(100)	1(
100)				
		Scheduled Maintenance(HelpDesk)	0(100)	0(
100)				
		RAD Compiler	0(0)	0(
25)				
		Service Catalog	0(100)	0(
0)				
		Change Management	0(100)	1(
100)				
		Request Management	0(100)	1(
100)				
		Service Level Management	0(100)	0(
100)				
		Contract Management	0(100)	0(
100)				
		Asset Contracts Management	0(100)	1(
100)				

100)	Knowledge Management	0(100)	1(
0)	Knowledge Management ESS	0(100)	0(
	HP SCAuto SDK for MVS(SCAuto)	Enabled		
	HP SCAuto SDK for Unix/Windows(SCAuto)	Enabled		
	HP SCAuto for Tivoli Netview AIX(SCAuto)	Enabled		
	HP SCAuto for Spectrum(SCAuto)	Enabled		
	HP SCAuto for Lotus Notes(SCAuto)	Enabled		
	HP SCAuto for Tivoli Netview OS390(SCAuto)	Enabled		
	HP SCAuto for TBSM(SCAuto)	Enabled		
	HP SCAuto for CA Unicenter AMO(SCAuto)	Enabled		
	HP SCAuto for CA Unicenter TNG(SCAuto)	Enabled		
	HP SCAuto for Tivoli(SCAuto)	Enabled		
	HP SCAuto for Tally NetCensus(SCAuto)	Enabled		

Generate a user license report

Applies to User Roles:

System Administrator

You must have administrative access to the server operating system to perform this procedure.

To generate a user license report, follow these steps:

1. Change directories to the RUN folder of your HP Service Manager installation. For example, run the following command on Windows:

```
cd C:\Program Files\HP\Service Manager x.xx\Server\RUN
```

2. Type the following command:

```
sm -reportlic: 1
```

3. Press **Enter**.

Stathistory table

The stathistory table updates every time a user logs on to the system. A stathistory record tracks the named and Floating licenses on an application basis.

The application creates a new stathistory record daily. If a stathistory record already exists, the record updates. If one does not exist, the application creates a new record. The stathistory record names are:

Application	License type
Application name	- named
Application name	- Floating

For example, to search for floating license Configuration Management records, type:

Configuration Management - Floating

Each stathistory record updates with the number of named or Floating licenses used at that moment. The number updates only when it is greater than the number already in the table. This enables the administrator to keep track of the highest number of licenses used at any time.

View the stathistory table

Applies to User Roles:

System Administrator

To view the stathistory table, follow these steps:

1. Click **Tailoring > Database Manager**.
2. In the **File** field, type: `stathistory`.
3. Click **Search**.
4. Select any record to view it.

Self-service licenses

The number of licenses that are active depends on the number of users logged on who can access an application to add or update records. Self-service users who initiate service requests through an employee self-service (ess.do) portal do not consume a named or floating license for login, but may consume an application license. For example, if you have the ability to approve changes, whenever you log in to the ESS client, you consume a Change Management license. It does not matter if the only thing you do while logged in to the ESS client is submit a new interaction or check interaction status, you will consume a full Change Management license because you have the capability to approve a change. If you also have approval capability for Request Management, you will consume a Request Management license even when logged in to ESS. Self-service users can log on to an ess.do URL to perform certain activities (such as, searching the knowledgebase to find an answer or logging new interactions) without contacting the Service Desk.

Users with privileges to log on to Service Desk (or other HP Service Manager applications) are power users. They use a Windows client or a valid (non-ESS) Web client URL (index.do) and consume a named or floating license. They can add, update, or delete records.

You can review the sm.log file for messages that specify when a user consumes a license.

Note: License utilization reports are included out-of-box in the Service Manager SM Reports module.

Folder entitlement

Folder entitlement isolates company information in folders, ensuring that the right users have the right access to sensitive company data. For example, a company that manages more than one organization could create separate security folders for each organization. Users in organization A could be granted access to Folder A and users in organization B could be granted access to Folder B. The information in an organization is tied to a security folder when users open records, such as incident records. Therefore, users in organization A could not access incidents, changes, or requests made by organization B, and vice versa. When folder entitlement is enabled, a new field appears when users open records. This field allows users to select the security folder, allowing them to tie the information in the record to that security folder. Users outside the organization who have not been granted permission to access the data in the folder cannot see the record. When users outside the organization search incidents, changes, or requests, the records are not found.

In HP Service Manager, a System Administrator enables or disables folder entitlement. For more information on enabling and disabling folder entitlement, see the related topics.

The available out-of-box company security folders on the Folder Entitlement tab are DEFAULT and advantage. However, the System Administrator can add folders to meet your business needs.

For each security folder added, a System Administrator must grant permissions to a specific application security profile, thereby granting permissions to all operators associated with that profile. Permission settings are selected for operators based on roles that reflect their responsibilities. When defining roles, each role displays a top level view for all folders. You can then click on each folder and set rights on individual fields for a folder, or modify workgroups. If a user does not have specific rights defined for a folder, the default rights from the user profile are assigned.

The System Administrator can set the default folder for an individual operator. This setting allows the records opened by the operator to be automatically associated with the default security folder selected.

Note: Using the legacy listener with the security folder is NOT supported.

Enable folder entitlement

Applies to User Roles:

System Administrator

To enable folder entitlement, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **General** tab.
3. Select the **Enable Folder Entitlement** check box.
4. Click **Save**.
5. Click **OK**.
6. Log out of HP Service Manager and log back in.

Folder Entitlement is now enabled.

Disable folder entitlement

Applies to User Roles:

System Administrator

To disable folder entitlement, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
2. Click the **General** tab.
3. Deselect the **Enable Folder Entitlement** check box.
4. Click **Save**.
5. Click **OK**.
6. Log out of HP Service Manager and log back in.

Folder entitlement has been disabled. There are no longer any security folders assigned to operators.

Add a security folder

Applies to User Roles:

System Administrator

To add a security folder, follow these steps:

1. From the System Navigator, click **System Administration > Ongoing Maintenance > Security Folders**.

The **Folder Definition** form opens.

2. Type the name of the new folder in the **Folder Name** field.
3. Type the **Description** of the security folder.
4. Click **Add**.
5. Click **OK**.

To use an existing security folder to add a new folder:

1. From the System Navigator, click **System Administration > Ongoing Maintenance > Security Folders**.

The **Folder Definition** form opens.

2. Add optional search criteria, and then click **Search**.
3. Select a folder from the list that most closely matches the new folder you want to add.
4. Type the new name of the folder in the **Folder Name** field.
5. Add or change the **Description** for this new security folder.
6. Click **Add**.

Caution: Make sure that you do not click Save because doing so will replace the existing folder

with the new security folder you are attempting to add.

7. Click **OK**.

Delete a folder

Applies to User Roles:

System Administrator

To delete a folder, follow these steps:

1. From the System Navigator, click **System Administration > Ongoing Maintenance > Security Folders**.
2. Type the folder name, or click **Search** to select the folder name from a record list.
3. Select the folder and click **Delete**.
4. Click **OK**.

Note: You cannot delete a folder that is currently in use. An error message displays if you attempt to delete a folder that is in use.

Specify use of the default folder from the operator record

Applies to User Roles:

System Administrator

The System Administrator can set the default folder for an individual operator. This setting allows the records opened by the operator to be automatically associated with the default folder set in the operator record.

To specify use of the default folder from the operator record, follow these steps:

1. From the System Navigator, click **System Administration > Ongoing Maintenance > Operators**.

The Operator search form opens.

2. Type optional search criteria, and then click **Search**.

3. Select the operator record to be edited.
4. In the **General** tab, select the **Folder Entitlement** tab.
5. In the **Default Folder** field, select a security folder as the default folder for this operator.
6. Click **Save**.
7. Click **OK**.
8. Log out of HP Service Manager, and then log back in.

The default folder selected will automatically be used the next time the operator opens a new record.

Add folder permissions to a security role

User Role: System Administrator

To add folder permissions to a security role:

1. Click **System Administration > Security > Roles**.
2. Click **Search** to select a security role from the record list.
3. Click the security role to be viewed.
4. Under **Rights**, select the applicable default rights parameters for the security role.
5. Under **Security Folders**, select folders.
6. Click **Save**.

Chapter 6: Calendars

The HP Service Manager calendar is an optional feature that enables the System Administrator to define custom work schedules for each group in the organization. These custom calendars determine when alerts and notifications occur for particular groups.

By default, Service Manager uses a calendar with a 24-hour work day and a 7-day work week to determine when alerts and notifications occur. In the default 24-hour, 7-day calendar, Service Manager sends alerts and notifications without regard to operator work shifts. For example, if an operator schedules a notification to occur in 6 hours, then Service Manager sends the notification after 6 hours have passed regardless of whether any operator is present to receive it. A notification scheduled at 5:00 p.m. in the default calendar arrives at 11:00 p.m. the same day.

Using a custom calendar, however, the same 6-hour delay occurs only during the defined work schedule. For example, a System Administrator can define an 8-hour work day lasting from 8:00 a.m. to 5:00 p.m., which includes a 1-hour break from 12:00 p.m. to 1:00 p.m. If an operator then schedules a notification to occur 6 hours after 5:00 p.m., the notification actually occurs at 3:00 p.m. the next work day, or 6 working hours after the notification start time.

System Administrators can create custom calendar records to use throughout Service Manager. The `caldutyhours` table contains custom calendar records that a System Administrator can assign to Service Manager activities:

- Change Management work schedule
- Change Management group definitions
- Incident Management assignment group definitions
- Incident Management deadline alert group definitions
- Request Management target order times
- Request Management target completion times
- Service Level Agreement service hours
- Service Level Agreement availability schedules
- Service Level Agreement response time schedules

- Service Desk on call times
- Vendor schedules

Holiday records

HP Service Manager includes out-of-box records for common holidays in the United States. To add a holiday, you must create a new holiday record in the calholidays table and associate that holiday with a group in calholtable.

Service Manager uses calholtable to organize holidays into different groups. For example, one group of holidays might list all holidays observed in France. This group would include worldwide holidays like Christmas and New Year's Day and those unique to France. A second group might also list the worldwide holidays, but add those unique to North America.

Associated tables

Service Manager uses information in these tables:

- calholidays contains a record for each holiday observed by your company.
- calholtable contains a record with the name of each group of holidays.

Add a master data record

Applies to User Roles:

System Administrator

Note: In ITIL best practices, a Configuration Administrator manages master data. In Service Manager, however, only a System Administrator has rights to master data, because the master data is shared by all Service Manager applications. You may need to contact a System Administrator to implement master data changes or to request permission to perform this function.

After you validate that the data sets for a new master data record request meet your company's specifications, you can add the master data record to Service Manager. For example, you may need to add a master data record for a new company location or a new vendor/supplier.

To add a master data record:

1. Click **System Administration > Base System Configuration**, and then double-click the master data category you want to add a record to.

For example, if you want to add a master data record for a new company location, click **Locations**.

2. Specify the new master data information and preferences.
3. Click **Add**.

Service Manager adds the new master data record.

Create a data reconciliation report summarizing the data modifications and any reconciliation errors in accordance with your company procedures.

Part of Workflow(s):

[Manage master data \(ST 3.6\)](#)

Applies to User Roles:

[Configuration Administrator](#)

Delete a master data record

User roles: System Administrator, Configuration Administrator

Note: In ITIL best practices, a Configuration Administrator manages master data. In Service Manager, however, only a System Administrator has rights to master data, because the master data is shared by all Service Manager applications. You may need to contact a System Administrator to implement master data changes or to request permission to perform this function.

After you validate that the data sets for a master data record delete request meet your company's specifications, you can delete a master data record in Service Manager. For example, you may need to delete a location record because the site was closed.

Warning: When you delete a master data record, it is possible that some configuration item records will still include the old master data value. Before you delete master data records, HP recommends you conduct a mass update to replace the master data value scheduled for deletion with the new approved value. This prevents obsolete data from remaining in Service Manager CI records.

To delete a master data record:

1. Click **System Administration > Base System Configuration**

2. Double-click the master data category for the record you want to delete.

For example, if you need to delete a master data record for a user who is no longer with the company, click **Contacts**.

3. Fill in optional search criteria, and then click **Search**.

Service Manager returns a list of records matching your search request.

4. Double-click the master data record you want to delete.

5. Click **Delete**.

Note: When you delete the contact record, the corresponding operator record will also be deleted.

6. Click **Yes** to confirm the deletion.

Service Manager deletes the master data record and notifies you that the corresponding operator record has also been deleted.

Part of Workflow(s):

[Manage master data \(ST 3.6\)](#)

Applies to User Roles:

[Configuration Administrator](#)

Update a master data record

User roles: System Administrator, Configuration Administrator

Note: In ITIL best practices, a Configuration Administrator manages master data. In Service Manager, however, only a System Administrator has rights to master data, because the master data is shared by all Service Manager applications. You may need to contact a System Administrator to implement master data changes or to request permission to perform this function.

After you validate that the data sets for a master data record update request meet your company's specifications, you can update the master data record in Service Manager. For example, you may need to change the cost center for a department or change the status of a master data record to retired or obsolete.

To update a master data record:

1. Click **System Administration > Base System Configuration**, and double-click the master data category for the record you want to update. For example, if you need to update a master data record to change the conversion rate for an international currency, click **Conversion Rates**.
2. Fill in optional search criteria.
3. Click **Search**.
Service Manager returns a list of records matching your search request.
4. Double-click the master data record you want to update.
5. Specify the new master data information. If you need to change the status of the record to indicate that it is retired or obsolete, update the record in accordance with your company procedures. For example, your company procedures might instruct you to add the words retired or obsolete to the record name.
6. Click **Save**.
Service Manager updates the master data record.
7. Search for related active configuration items to ensure that the record updates do not conflict with the configuration administration.

Create a holiday group

Applies to User Roles:

System Administrator

To create a holiday group:

1. Click **Tailoring > Database Manager**.
2. Type **calholtable** in the Form field.
3. Click **Search**.
4. Type the name of the new holiday group in the **Holiday Group Name** field.
5. Click **Add**.

On-call schedules

On-call schedules help managers or administrators determine whether they have enough resources on call to cover all shifts for each day. The on-call schedule specifies who is to be notified, when, and the notification method. An administrator must complete the On Call Information form to identify individual operator or contact assignments before HP Service Manager can create an on-call schedule record.

At midnight, the problem background processor generates the on-call schedule for the next day. The background processor uses information in these tables to produce the on-call schedule for the next 24 hours:

- caldutyhours contains shift definition records.
- operator and contacts provide information about the operator.
- oncallsched defines on call assignments, notification methods, and time zone variations.
- tzfile defines time zones.

Time zones

The On Call Information form has a time zone field where you can note deviations from the server time zone for any operator. For example, consider this scenario:

- A European company has headquarters in London, where the corporate server is located.
- The company record specifies that Western European Time (WET) is the default time zone.
- Teresa Thompson is an employee, but she works remotely from California.
- Her manager notes that her Local Time in the on-call schedule form is Pacific Standard Time (PST).
- When her manager sends her to Chicago for two weeks of on-site customer support, the manager makes an entry in the Exception Time Zone field that temporarily changes her location to Central Standard Time (CST).
- When she returns to California, the manager removes this exception entry from the on-call schedule form before Service Manager generates the next day's record.

On-call schedule exceptions

The On Call Information form enables you to define exceptions to the standard notifications and time intervals in the daily schedule. There is an Exceptions tab where you can note deviations from the server time zone and notification method for any operator. For example, consider this scenario and how the Exceptions tab captures schedule variations.

- A European company has headquarters in London, where the corporate server is located.
- The company record specifies that Western European Time (WET) is the default time zone.
- Teresa Thompson is an employee, but she works remotely from California.
- Her manager notes that her Local Time in the On Call Information form is Pacific Standard Time (PST).
- When her manager sends her to Chicago for two weeks of on-site customer support, the manager makes an entry in the Exception Time Zone field that temporarily changes her location to Central Standard Time (CST).
- When she returns to California, the manager removes this exception entry from the on-call schedule form before HP Service Manager generates the next day's record.

Daily Schedule

Service Manager displays daily schedule information for regular on call dates and times using a relative date and time format that is not dependent on a specific time zone. The relative time format is *dd hh:mm:ss*. For example, the Servicedesk Agent always begins work at 8:00:00 and stops work at 17:00:00.

Exceptions

Service Manager displays on call exception dates and times using an absolute date and time format. The absolute date and time are for the time zone specified in the On Call Information form. If you omit a time zone, the default value is the time zone in the company record. The absolute time format is *mm/dd/yyyy hh:mm:ss*. For example, Teresa Thompson worked in the Central time zone only one day. She began work on 03/14/2009 08:00:00, and stopped work on 03/14/2009 at 17:00:00.

Create an on-call schedule

Applies to User Roles:

System Administrator

To create an on-call schedule:

1. Click **Tailoring > Notifications > Daily On Call Records**.
2. Fill in the following fields.

Field	Sub-field	Description
Group Name		Specify the name of the group.
Daily Schedule tab		Use this tab to type the schedule for each contact in the group.
	Contact	Type the contact or operator name of the person to receive the notification.
	Start Time	Type the time that the person starts being on call. Type the time in the 24-hour time format. By default, HP Service Manager treats a blank start time as equivalent to 00:00:00 or midnight.
	End Time	Type the time that the person ends being on call. Type the time in the 24-hour time format. By default, Service Manager treats a blank end time as equivalent to 23:59:59 or one second until midnight.
	Days of the week	Type true for any day that the person is on call, and type false for days the person is not on call. By default, Service Manager treats a blank entry as false.
	Notify Method	Specify the name of the message class used to notify this person.
	Condition	Type <code>true</code> to enable the notification in all conditions. Type an expression that is true or false to define the condition for notification. Type <code>false</code> to disable the notification in all conditions. By default, Service Manager treats a blank entry as true.
	Local Time	Click the drop-down list to select the local time zone where the contact resides. This is optional if all contacts are in the time

Field	Sub-field	Description
	Zone	zone specified in the company record.
Exceptions tab		Use this tab to define alternative notification methods and conditions during exception dates such as holidays and vacations.
	Contact	Type the contact or operator name of the person receiving the notification.
	Start Date	Type the date and time on which the exception schedule begins. Type the time in the 24-hour time format. By default, Service Manager treats a blank start time as equivalent to 00:00:00 or midnight.
	End Date	Type the date and time on which the exception schedule ends. Type the time in the 24-hour time format. By default, Service Manager treats a blank end time as equivalent to 23:59:59 or one second until midnight.
	Notify Method	Specify the name of the alternate message class used to notify the operator during the exception schedule.
	Condition	Type <code>true</code> to enable notification in all conditions. Type an expression that is true or false to define the condition when notification occurs. Type <code>false</code> to disable notification in all conditions. By default, Service Manager treats a blank entry as true.
	Replace Daily	Type <code>true</code> to use notification conditions defined only on the Exception tab. Type <code>false</code> to use notification conditions defined on the Daily Schedule and Exception tab. By default, Service Manager treats a blank entry as false.
	Exception Time Zone	Click the drop-down list to select an exception time zone if the contact is in a different location temporarily. For example, an operator might be deployed to a customer site for a week.

3. Click **Add**.

Work schedules

A work schedule defines the work hours for one or more operators. HP Service Manager can generate a complex 24x7 schedule that spans multiple time zones, includes all shift and break information,

accommodates any regional shift to Daylight Savings time, and automatically accounts for local or national holidays. Service Manager uses the following information to create a work schedule:

- Shift and break information
- Holiday information (optional)

Service Manager uses work schedule information in various calculations. One of the more important calculations is when to trigger an alert that an incident should escalate to the next level.

The caldutyhours table

The caldutyhours table contains records that identify the time to start and stop work, and the time to start and stop a break. The caldutyhours table contains the following out-of-box records.

Shift name	Holiday table	Duration
Long	standard	50-hour week with no breaks
Short	standard	42.5-hour week with no breaks
Day shift	standard	40-hour week with one hour breaks
Day shift 2	standard	40-hour week with one hour breaks
Graveyard shift	none	40-hour week with no breaks
Managers	none	40-hour week with no breaks
Ops graveyard	none	40-hour week with no breaks
Second shift	none	50-hour week with no breaks
Standard	none	40-hour week with no breaks
Swing shift	none	50-hour week with no breaks

Work schedules can apply to a group, such as an assignment group, or to an individual named in the operator or contacts table. When you create schedule records, start and stop times must not overlap, and breaks must occur within the defined work shift.

Add a master data record

Applies to User Roles:

System Administrator

Note: In ITIL best practices, a Configuration Administrator manages master data. In Service Manager, however, only a System Administrator has rights to master data, because the master data is shared by all Service Manager applications. You may need to contact a System Administrator to implement master data changes or to request permission to perform this function.

After you validate that the data sets for a new master data record request meet your company's specifications, you can add the master data record to Service Manager. For example, you may need to add a master data record for a new company location or a new vendor/supplier.

To add a master data record:

1. Click **System Administration > Base System Configuration**, and then double-click the master data category you want to add a record to.

For example, if you want to add a master data record for a new company location, click **Locations**.

2. Specify the new master data information and preferences.
3. Click **Add**.

Service Manager adds the new master data record.

Create a data reconciliation report summarizing the data modifications and any reconciliation errors in accordance with your company procedures.

Part of Workflow(s):

[Manage master data \(ST 3.6\)](#)

Applies to User Roles:

[Configuration Administrator](#)

Delete a master data record

User roles: System Administrator, Configuration Administrator

Note: In ITIL best practices, a Configuration Administrator manages master data. In Service Manager, however, only a System Administrator has rights to master data, because the master data is shared by all Service Manager applications. You may need to contact a System Administrator to implement master data changes or to request permission to perform this function.

After you validate that the data sets for a master data record delete request meet your company's specifications, you can delete a master data record in Service Manager. For example, you may need to delete a location record because the site was closed.

Warning: When you delete a master data record, it is possible that some configuration item records will still include the old master data value. Before you delete master data records, HP recommends you conduct a mass update to replace the master data value scheduled for deletion with the new approved value. This prevents obsolete data from remaining in Service Manager CI records.

To delete a master data record:

1. Click **System Administration > Base System Configuration**
2. Double-click the master data category for the record you want to delete.

For example, if you need to delete a master data record for a user who is no longer with the company, click **Contacts**.

3. Fill in optional search criteria, and then click **Search**.

Service Manager returns a list of records matching your search request.

4. Double-click the master data record you want to delete.
5. Click **Delete**.

Note: When you delete the contact record, the corresponding operator record will also be deleted.

6. Click **Yes** to confirm the deletion.

Service Manager deletes the master data record and notifies you that the corresponding operator record has also been deleted.

Part of Workflow(s):

[Manage master data \(ST 3.6\)](#)

Applies to User Roles:

[Configuration Administrator](#)

Update a master data record

User roles: System Administrator, Configuration Administrator

Note: In ITIL best practices, a Configuration Administrator manages master data. In Service Manager, however, only a System Administrator has rights to master data, because the master data is shared by all Service Manager applications. You may need to contact a System Administrator to implement master data changes or to request permission to perform this function.

After you validate that the data sets for a master data record update request meet your company's specifications, you can update the master data record in Service Manager. For example, you may need to change the cost center for a department or change the status of a master data record to retired or obsolete.

To update a master data record:

1. Click **System Administration > Base System Configuration**, and double-click the master data category for the record you want to update. For example, if you need to update a master data record to change the conversion rate for an international currency, click **Conversion Rates**.
2. Fill in optional search criteria.
3. Click **Search**.
Service Manager returns a list of records matching your search request.
4. Double-click the master data record you want to update.
5. Specify the new master data information. If you need to change the status of the record to indicate that it is retired or obsolete, update the record in accordance with your company procedures. For example, your company procedures might instruct you to add the words retired or obsolete to the record name.
6. Click **Save**.
Service Manager updates the master data record.
7. Search for related active configuration items to ensure that the record updates do not conflict with the configuration administration.

Chapter 7: Clocks

Clocks are background processes that track the duration of specific conditions in HP Service Manager. You can add a clock to track almost any event or condition. By default, Service Manager creates clocks only for the following conditions:

- When an incident record changes status (for example, when an incident record changes from Open to Pending status, or from Open to Closed status)
- When an operator edits an incident record and the System Administrator has enabled the Track Operator Times option (for example, when an operator edits an incident record to add details or a solution)

To track additional Service Manager conditions, you can manually start or stop a clock using the following tools:

- Format control utility
- Command line
- Macro

Clock example

The following example illustrates how Service Manager uses clocks to track the duration of each phase of an incident record. In this example, the clocks **total.time** and **pending.time** track the elapsed time that an incident record is open and pending, respectively.

Date and time	Current incident record phase	Status of clock total.time	Status of clock pending.time
July 1 1: 00 p.m.	Open	clock starts Total 00: 00	Clock inactive
July 2 4: 00 p.m.	Pending	Clock stops Total 27: 00	Clock starts Total 00: 00
July 4 2: 00 p.m.	Open	Clock restarts Total 27: 00	Clock stops Total 46: 00
July 4 2: 30 p.m.	Closed	Clock stops Total 27: 30	Clock stopped Total 46: 00

Add a clocks record

Applies to User Roles:

System Administrator

To add a clocks record, follow these steps:

1. Click **System Administration > Base System Configuration > Monitoring > Clocks**.
2. Type or select the following information.
 - **Type** is the RAD application that the clock tracks. You can choose from the following types:
 - Problem
 - Downtime
 - cm3r
 - SLA
 - Incident
 - **Char Key** specifies the name of the application record that starts and stops the clock.
 - **Char Number** specifies the numeric ID of the record that starts and stops the clock.
 - **Name** is the label for the clock.
 - **Total** displays the total time that the clock has been running.
 - **Closed Total** displays the total time that the clock used when it was last run.
 - **Schedule** is the name of the work schedule for the clock to use.
 - **Close Date** displays the date and time when the clock stopped running.
 - **Start array** specifies the dates and times for the clock to start.
 - **Stop array** specifies the dates and times for the clock to stop.
3. Click **Add**.

Add a clock to track incident record status changes

Applies to User Roles:

System Administrator

To add a clock to track incident record status changes, follow these steps:

1. Click **Tailoring > Database Manager**.
2. In the **Table** field, type or select the table name **pmstatus**.
3. Click **Search**.
4. Type or select optional search criteria.
5. Click **Search**.
6. Select the status to track with a clock.
7. In the **On Entering This Status** section, type the following information:
 - **Start These Clocks:** type the names of the clocks to start when an incident enters this status.
 - **Stop These Clocks:** type the names of the clocks to stop when an incident enters this status.
8. In the **On Exiting This Status** section, type the following information:
 - **Start These Clocks:** type the names of the clocks to start when an incident exits this status.
 - **Stop These Clocks:** type the names of the clocks to stop when an incident exits this status.
9. Click **Save**.

Enable tracking of operator times

Applies to User Roles:

System Administrator

You can track how long each operator edits an Incident record by enabling a tracking option in the Incident Management environment.

To enable tracking of operator times:

1. Click **System Administration > Ongoing Maintenance > Environment Records > Incident Management Environment**.
2. Select the **Track Operator Times?** checkbox.
3. Click **Save**.

Start or stop a clock from a macro

Applies to User Roles:

System Administrator

To start or stop a clock from a macro, follow these steps:

1. Click **Tailoring > Tailoring Tools > Macros**.
2. Click **Add**.
3. Type or select the following information to describe your macro.

Field	Description
Macro Name	Type the name of your new macro
Applies When	Select the condition when your macro runs
Macro Type	<ul style="list-style-type: none">○ To start a clock select Start A Clock○ To stop a clock select Stop A Clock
Macro Condition	Type <code>true</code> , or a condition statement that evaluates to true or false, to determine when to run the macro

4. Click **Set Parameters**
5. Type or select the following parameters to describe the clock.

Field	Description
Name	This value describes the name of the clock where HP Service Manager stores duration

Field	Description
of Clock	<p>information. This name must uniquely identify the clock.</p> <ul style="list-style-type: none"> ◦ Select Fixed Key Field to type a specific clock name. ◦ Select Evaluating Expressions to define a dynamic name based on an expression. <p>Note: An evaluating expression must contain the \$L.name variable.</p>
Type of Clock	<p>This value describes the type of clock to start. Service Manager automatically places a value in this parameter based on your Macro Type selection.</p> <ul style="list-style-type: none"> ◦ Select Fixed Key Field to type a specific clock type. ◦ Select Evaluating Expressions to define a dynamic clock type based on an expression. <p>Note: An evaluating expression must contain the \$L.type variable.</p> <p>The possible clock type values are:</p> <ul style="list-style-type: none"> ◦ problem ◦ downtime ◦ cm3r ◦ SLA ◦ incidents
Clock Key Field	<p>This value identifies the record, event, or object to track. This value must be unique throughout Service Manager. For a record, you can type number in \$L.new to enter the unique ID associated with the record. Service Manager automatically places a value in this parameter based on your Macro Type selection.</p> <ul style="list-style-type: none"> ◦ Select Fixed Key Field to type a specific clock key field. ◦ Select Evaluating Expressions to define a dynamic key field based on an expression. <p>Note: An evaluating expression must contain the \$L.key variable.</p>

6. Click **Save**.

7. Click **OK**.

Start or stop a clock from format control

Applies to User Roles:

System Administrator

To start or stop a clock from format control, follow these steps:

1. Click **Tailoring > Format Control**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select a form, and then click the **Subroutines** tab.
5. In the **Application Name** field, type one of the following options:
 - `apm.start.clock` to start a clock.
 - `apm.stop.clock` to stop a clock.
6. Type the following information into the **Names** and **Values** fields:

Names	Values	Description
Name	Type one of the following values: <ul style="list-style-type: none">◦ <code>problem</code>◦ <code>downtime</code>◦ <code>cm3r</code>◦ <code>SLA</code>◦ <code>incident</code>	This value describes the type of clock to start. For Incident Management clocks, type <code>problem</code> or <code>SLA</code> .
prompt	Type the name of the	This value describes the name of the clock where HP Service Manager stores duration information. This name must only be unique within the

Names	Values	Description
	clock.	format control.
query	Type the Unique key for the clock to use.	This value identifies the record, event, or object for the clock to track. This value must be unique throughout Service Manager. For a record, you can type the value <code>number in \$file</code> to enter the unique ID associated with the record.
string1	Type one of the following values: <ul style="list-style-type: none"> ◦ <code>stop</code> ◦ <code>strobe</code> 	This value is only required if you are calling the apm.stop.clock application. The value <code>stop</code> stops the clock named in the format control. The value <code>strobe</code> forces the clock to recalculate the clock's current running time.
time1	Type the time the clock is to stop or start.	This value determines when the clock stops or starts. To stop the clock at the current date and time, type <code>tod()</code> .

7. Type or select any additional format controls.

8. Click **Save**.

View a clock record

Applies to User Roles:

System Administrator

To view a clock record, follow these steps:

1. Click **System Administration > Base System Configuration > Monitoring > Clocks**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Choose the clock record to view.

Chapter 8: Self-service

Self-service enables any user to connect with a HP Service Manager application to request a service, provide information, or track previous requests. Self-service users can also be granted approval capabilities that enable the user to approve change requests. Typically, this capability is given to high-level managers with a need to approve special requests who may otherwise have no need to use Service Manager on a regular basis.

The self-service feature provides a way for administrators to grant access to infrequent users, field personnel, or any other user outside of the IT organization without consuming a user license. These users need no special training or software. If users can connect to the Service Manager server using a supported browser, they can open incidents or make service requests.

Note: Users that are logged in to the ESS client can only see records in which they are the service recipient, primary contact, or records for which they are an approver.

Working with self-service requests

Self-service has features that enable you to open, view, update, copy, resubmit, or close service requests. Users are able to create new requests, using a supported browser, that become service desk interaction records. Self-service users can review their pending requests and make changes to them as needed. Self-service users can also use the Service Catalog interface to order items and services from the service catalog.

Visible updates for self-service requests

When a self-service user makes an update to an open request, the user can view the update text in the History section of the interaction record. When a HP Service Manager operator views the same record, the **Activities** section has three subsections that relate to updates.

- Record new activities on the **Updates** section
- View journal entries on the **Journal Updates** section when the administrator enables **Journal Updates** in the Environment record
- View the updates in the list of updates for an activity type

When the operator makes an update to an open self-service request, Service Desk hides the update text from the self-service user. To show the update text to the self-service user, the operator must select the **Visible to Customer** check box in the **Activities** section of the interaction form.

Creating self-service users

There are different ways to create a self-service user:

- Manually create an operator and contact record for a single self-service user

HP Service Manager has an out-of-box template record to assist you with this task.

- Create a self-service operator from a contact record with a single operation
- Create multiple self-service operators from a contact record list with a single operation

ESS and ESSM-Approval users

ESS users have a regular Service Desk profile that enables them to log on to Service Desk only through a self-service web client URL. A user with an ESSM-Approval profile (for example, a manager) can approve change requests specified by a dollar amount or company. Typically, this capability is given to high-level managers with a need to approve special requests who otherwise have no need to use HP Service Manager on a regular basis.

Self-service template record

HP Service Manager has an out-of-box operator template record, `Template_SelfService`, that contains all required operator settings. The password field is null. Therefore, the first time a registered user logs in, no password (or a blank password) appears. Service Manager prompts the self-service user to create a password.

The self service out-of-box user role record lists the following capability words:

- service desk
- svcCatEmployeeRequester
- service catalog
- change request

If you create self-service users manually, make sure that you include the applicable settings in the out-of-box records.

Create a self-service user

Applies to User Roles:

System Administrator

A new self-service user requires an operator record and a contact record. Hewlett-Packard recommends that you also create a user role for all self-service users. Alternatively, you can use the out-of-box self-service user role record.

Create self-service user contact record and operator record in one operation

To create the contact record and the operator record in one operation, follow these steps:

1. Click **System Administration > Base System Configuration > Contacts**.
2. Specify information for the new contact that you want to create. The following fields are required for a self-service user:
 - **Contact Name**
 - **Full Name**
 - **Email**

HP Service Manager uses the email address as the user's Service Manager ID when it creates the new operator record.
3. (Optional) Choose the **Primary Configuration Item** to be associated with this user.
4. Click **Add**.
5. When the new contact record is created, click **More** or the **More Actions** icon, and then click **Create Operator**.
6. Select **Self Service User** for the operator type, and then click **Next**.
7. Click **Save**.
8. Click **OK**.

Create self-service user manually

To create a self-service user manually, follow these steps:

Note: If you create the operator record manually, you can use the out-of-box template record (Template_SelfService) to create a self-service user. If you choose this method, you must also create a matching contact record.

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria, and then click **Search**.
3. Select **Template_SelfService**.
4. Replace the **Login Name** and **Full Name**.
5. Verify the following:
 - **User Role** field contains **SELF SERVICE**.
 - **Service Profile** field contains **SELF SERVICE**.
6. Add optional information, such as **Language** and **Default Company** name.
7. Click the **Login/Contact Profiles** tab and choose a resource type from the **Resource Type** list.
8. Click the **Notification** tab and in the **Email Addr.** field, type the self-service user's email address.
9. Click the **Self Service** tab:
 - To limit the new user to only self-service requests, select the **Self Service Access Only** check box.
 - Type the name of the **Self Service Menu** to display when the user logs on using a self-service URL. The out-of-box menus are **ESSSM** and **ESSM-Approval**. ESSM-Approval provides the Approval Request link to the Approval view on the self-service starting page for those users with approval capability.
 - Click the list to choose the **Self Service Starting Page** to display when the user logs on using a self-service URL. For example, choose **Submit a Request**.
10. Add optional information to any tab.

11. Click **Add**.
12. Create a self-service user contact record:
 - a. Click **System Administration > Base System Configuration > Contacts**.
 - b. Type the new contact information.
 - c. Click **Add**.

Note:

- The Service Manager ID field in the contact record must match the operator Login Name in the operator record.
- If you choose the User Quick Add Utility, Service Manager prompts you to create the contact record for the user if it does not exist.
- You can apply the Template_SelfService template to a new operator record.

Create a self-service user from an existing contact

Applies to User Roles:

System Administrator

To create a self-service user from an existing contact, follow these steps:

1. Click **System Administration > Base System Configuration > Contacts**.
2. Use search or advanced search to find one or more records.
3. Select a contact record.
4. Click **More** or the **More Actions** icon above the form of the contact record, and then click **Create Operator**.
5. Select **Self Service User** for the operator type, and then click **Next**.
6. Click **Save**.
7. Click **OK**.

Note: The self-service user name is the user's email address.

Create multiple self-service users from a contact list

Applies to User Roles:

System Administrator

Caution: This function will fail if anyone in the contact list already has an operator record. At that point it stops and does not create operator records for any remaining contacts in the list.

To create multiple self-service users from a contact list, follow these steps:

1. Click **System Administration > Base System Configuration > Contacts**.
2. Use search or advanced search to find one or more records.
3. Select the contacts for which you want to create self-service users.
4. Click **More** or the **More Actions** icon, and then select **Mass Create Operators**.
5. Select **Self Service User** for the operator type, and then click **Next**.
6. Click **OK**.

What is a self-service power user?

A self-service power user has two ways to access Service Desk. The access method depends on the task to complete:

- They have a Service Desk profile that enables them to log on to Service Desk (or other HP Service Manager applications) using the Windows client connection dialog or any valid Web client URL to view, add, update, or delete records. For example, the user has a Service Desk profile that enables the user to take service requests and provide services to a user community.
- They have a self-service profile that enables them to initiate service requests through a self-service URL. For example, a self-service user can use this feature to request services.

The following table shows how a user can access Service Manager in self-service or power user mode.

URL	Description
http: //server_name: port_number/SM/ess.do	The standard Web client interface for self-service users. The viewrecordlist parameter is disabled.
http: //server_name: port_number/SM/index.do	The standard Web client interface for power users. Self-service mode using the parameters set in the web.xml file.
http: //server_name: port_number/SM/accessible_ess.do	The accessible Web client in self-service mode. The viewrecordlist parameter is disabled because it does not conform to accessibility requirements.

Grant self-service access

Applies to User Roles:

System Administrator

To grant self-service access, follow these steps:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Type or select optional search criteria.
3. Click **Search**.
4. Select an existing operator record.
5. On the **General** tab, click **Fill** to choose a Service Profile, or click **Find** to modify the existing profile.

For example, you can add desired self-service privileges, such as Open, Update, or Close to the existing Service Profile.

6. Click the **Self Service** tab. Make sure that the operator record has these settings:
 - The **Self Service Access Only** check box must be cleared.
 - Type the name of the **Self Service Menu** to display when the user logs on using a self-service URL. The out-of-box menus are **ESSSM** and **ESSM-Approval**.

ESSM-Approval provides the Approval Request link to the Approval view on the self-service Starting page for those users with approval capability.

- Click the list to choose the **Self Service Starting Page** when the user logs on by using a self-

service URL.

For example, choose **Submit a Request**.

7. Click **Save**.

Note: The Login Name in the operator record must match the HP Service Manager ID in the contact record.

Configuring the self-service working environment

The self-service user experience requires special forms that the user sees, and security settings that enable user access. You can use the out-of-box records and forms created for self-service users, customize them, or create new ones. The following table lists the records that you must configure to define a user's self-service working environment.

Record	Content	Form (if applicable)	Description
User role record	A template record that combines a collection of application profiles and capability words into a single record.		Click Tailoring > Database Manager . Type <code>userrole</code> in the table field and click Search . Select userrole from the record list. Place your cursor in the User role field and click Search to display a record list of all out-of-box user role descriptions.
Service Desk profile record	Specifies which form to display when the self-service user chooses different tasks. You can change the user experience by creating a unique profile for all self-service users in a group, department, or company. Each profile identifies the forms that the user sees. For example, if you create separate company profiles, each form set would have unique corporate branding.	There should be a form listed for each task enabled for a self-service user. For example, the form to display to open, update, search, or display a list of requests.	Click Tailoring > Database Manager . Type <code>smenv</code> in the table field and click Search . Select smenv from the record list. Place your cursor in the Profile name field and click Search to display a record list of all out-of-box Service Desk environment profile records.

Record	Content	Form (if applicable)	Description
	<p>You can view the Environment profile record by clicking System Administration > Ongoing Maintenance > Profiles > Service Desk Profiles. Click Search to generate a list of all existing profiles.</p>		
		ESS Initial Format identifies the form to open a request.	Click Tailoring > Forms Designer , type <code>ess.SD.open</code> in the Form field, and click Search to view the out-of-box form.
		ESS Edit Format identifies the form to update a request.	Click Tailoring > Forms Designer , type <code>ess.SD.update</code> in the Form field, and click Search to view the out-of-box form.
		ESS Search Format identifies the form to search for a request.	Click Tailoring > Forms Designer , type <code>ess.SD.search</code> in the Form field, and click Search to view the out-of-box form.
		ESS List Format identifies the form to display a list of requests.	Click Tailoring > Forms Designer , type <code>ess.SD.qbe</code> in the Form field, and click Search to view the out-of-box form.
Service Desk environment record	Specify on this record whether self-service users see a blank list screen when they issue a pre-defined search. This behavior is controlled at the system level.		Click System Administration > Ongoing Maintenance > Profiles > Service Desk Profiles . Place your cursor in the Profile name field and click Search . Select the profile name for which you would like to restrict from viewing records lists. Click the Security tab. Click the Rights tab. Select the View check box. Click Save and then click OK .
Operator record (Self-Service tab)	Self Service Menu field: Specifies the layout of the user's home page when they log on as a self-service user.		Describes the actions available to the user in the left navigation pane (ESSSM).
	Self Service Starting Page field: Specifies the first form that appears in the main window.		Identifies the default start page in the main browser window. For example, if you select Display ESS Menu , the starting page displays the same menu items that appear in the left navigation pane. If you select Submit a Request , the starting page is the form to open a new request.

Create a Service Desk self-service security role

Applies to User Roles:

System Administrator

The out-of-box self service security role is indented for self-service users. You can create a security role for self-service users based on this one.

To create a Service Desk self-service security role, follow these steps:

1. Navigate to **System Administration > Security > Roles**.
2. Locate the **self-service** security role through a search. This security role has only View rights to some modules.
3. Create a new security role from this role or update this role as needed.

Now, you can assign the new or updated security role to self-service users by using the Mass Update feature.

Self-service licenses

The number of licenses that are active depends on the number of users logged on who can access an application to add or update records. Self-service users who initiate service requests through an employee self-service (ess.do) portal do not consume a named or floating license for login, but may consume an application license. For example, if you have the ability to approve changes, whenever you log in to the ESS client, you consume a Change Management license. It does not matter if the only thing you do while logged in to the ESS client is submit a new interaction or check interaction status, you will consume a full Change Management license because you have the capability to approve a change. If you also have approval capability for Request Management, you will consume a Request Management license even when logged in to ESS. Self-service users can log on to an ess.do URL to perform certain activities (such as, searching the knowledgebase to find an answer or logging new interactions) without contacting the Service Desk.

Users with privileges to log on to Service Desk (or other HP Service Manager applications) are power users. They use a Windows client or a valid (non-ESS) Web client URL (index.do) and consume a named or floating license. They can add, update, or delete records.

You can review the sm.log file for messages that specify when a user consumes a license.

Note: License utilization reports are included out-of-box in the Service Manager SM Reports

module.

Who uses self-service?

Self-service access is useful for all individuals in an organization. It enables them to make requests through self-service Web pages. These requests include service disruptions, service requests, catalog item requests, requests for information (RFI), or complaints. Typically, these requests generate an interaction in Service Desk, or they are a request for specific item or service in a service catalog. The following table shows typical organizational roles and how different employees might use the self-service feature.

User name	Tasks
Employee user	Uses self-service to make requests for self and on behalf of other employees and managers. Example, a user needs spreadsheet software upgraded to the newest version.
Administrative assistant	Uses self-service to make requests primarily for others. Example: a manager directs an assistant to request a color printer for the office.
Department Manager	Uses self-service to make requests for self and direct reports. Example: a manager requests new computer systems for each software developer in a group.
IT Technician	Makes service requests for self. Example: a technician needs to change an address in an employee record.
High level executive	Makes approvals for high dollar catalog orders. Example: a senior manager needs to approve a request at the business executive level.

Choosing a configuration item for self-service requests

Each self-service request can associate one Configuration Item (CI) with the request. For example, the request might be for service on your computer, or to request a new display device. To add a CI to a request, click **Search** to display a **Search Configuration Item** form. You can specify filtering criteria first, or just click Search again to view a list of available CIs.

Self-service tailoring

A System Administrator can modify the look and feel of self-service forms to reflect their corporate branding by using the Forms Designer or by modifying the display options and menu selections. However, a self-service user is not able to customize the self-service environment.

Because self-service is part of the Web tier, you can also customize the Web tier presentation to include font changes, logos, graphics, or navigation pane alterations. Customizations can affect the top header, navigation pane, or main page area.

Customize the self-service interface

Applies to User Roles:

System Administrator

You can customize the self-service interface by changing the menu and forms that HP Service Manager displays to the user.

Task 1: Change the menu record

The self-service menu record contains option numbers, descriptions, and the RAD application called by the option. If you change the contents of the menu record, especially the options, change the corresponding forms to match.

To change the menu record, follow these steps:

1. Click **Tailoring > Database Manager**.
2. In the **Form** field, type `menu`.
3. Click **Search**.
4. Double-click the **menu** form.
5. In the **Menu Name** field, type `ESSM`.
6. Click **Search** to display the self-service menu record.
7. If you make changes, click **Save**.

Task 2: Change the forms

The self-service menu record contains option numbers that correspond to the Button ID on the form. If you changed the options in the menu record, the Button ID on the form must match the associated option number in the menu record.

To change the forms, follow these steps:

1. Click **Tailoring > Forms Designer**.
2. In the **Form** field, type `menu.gui.ess.SD`.
3. Click **Search**.
4. Click **Design**.
5. After you make the changes, click **OK**.

Chapter 9: Views and favorites administration

A view uses a pre-defined query to display a set of records. As a system administrator, you can use Views/Favorites to create a new view, edit an existing view, or delete a view. A view includes the following elements, which can be specified or modified when the view is created or edited.

- View definition:
 - View Fields - fields displayed in the view.
 - Group By - how the records are grouped.
 - Sort By - how the records are sorted.
- Audience specifies which users can use the view.
- Ownership specifies who is allowed to manage the view and who is allowed to manage the content displayed by the view.

System administrators access the Views/Favorites function from the System Administration menu:

System Administration > Base System Configuration > Miscellaneous > Views/Favorites

Create a view

Applies to User roles:

System Administrator

You can create a view for one or more users to customize the default log-on view. For example, if a group of users regularly searches on the same query, you can provide them with a shared query view as their default whenever they log on to HP Service Manager.

This topic assumes that you are familiar with Service Manager table and field names.

To create a view, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > Views/Favorites**.
2. Click **New**.

The **New View** wizard opens.

3. Select the Area to create the view in and then click **Next**.
4. Specify the name and type for the view you wish to create, and whether it is a system view or personal view.
5. Select who the view will be available to, and then click **Next**:
 - Everyone
 - Selected Groups
 - Selected Roles
6. Select the fields you want in your view:
 - a. Click **Fields**.
 - b. To add fields, select items from the table menu and click **Add to List**.

Note: If you select a field that has a link to another table, select from the secondary menu to add fields you want in the view.

7. Select view properties for Group By, Sort By, Filter, and Autoformat as desired.

8. Click **Finish**.

After the system adds the view, you can provide additional information for the view definition

9. In the **Audience** tab, select an audience for the view and then click **Save**.
10. You can also update or add additional properties for the view with the View definitions, Query definitions, and Ownership tabs.

Add a view for a new table

Applies to User Roles:

System Administrator

When you want to expand the list of views in a queue, you can use the **New View** wizard. However, if the table does not yet exist, you need to first configure the table as an object record. You can then add the view to the table.

Note: These procedures use the `kmdocument` table as an example for configuring and adding a Knowledge Documents view to a table.

To configure an object record for a new table, follow these steps:

1. Click **Tailoring > Document Engine > Objects**.
2. Type the file name (table name) in the **File name** field. For this example, type `kmdocument`.
3. In the **Manage Queues** tab, type an expression in the **Manage condition** field that evaluates to true. For example, type `lioption("Knowledge Management")`.
4. Create a form to be used to display the view. Type your entry in the **Manage default view** field. For example, type `Knowledge Documents`.
5. Click **Fill** in the **Manage display format** field and choose **inbox.view**.
6. Click **Add**.
7. Log out of HP Service Manager, and then log back in. This enables the new object `kmdocument` table that you configured to be added to the view list. You can now add the new view to the table.

To add a view to a table, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > Views/Favorites**.
2. Click **New**. The **New View** wizard opens.
3. Select an entry for Area (**Knowledge Documents**) and then click **Next**.
4. Type the name of the view in the **Name** field and then click **Next**.
5. Click **Fields**.

6. Select **Title** in the **Knowledge Documents** list entries and then click **Add to List**. The Title entry appears in the Destination Fields box.
7. Click **Finish**. You receive a message that states the view record was added. You also see the View Definition form to add additional properties to the view you created.

The view appears under Favorites and Dashboards in the navigation pane.

Delete a view

Applies to User roles:

System Administrator

To delete a system view, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > Views/Favorites**.
2. Click **Search** to find a system view.
3. Select a system view from the records list.
4. Click **Delete**, and then click **Yes** to confirm.

Change fields in a view

Applies to User roles:

System Administrator

You can add, delete, or change the order of fields in a system view. This topic assumes that you are familiar with HP Service Manager table and field names.

Note: You can only change fields for views with a Table view type.

To change fields in a system view, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > Views/Favorites**.
2. Click **Search** to find the view you want to change.
3. Select the view from the records list.
4. On the View definitions tab, click **View Fields**.
5. To add fields, select items from the table menu and click **Add to List**.

Note: If you select a field that has a link to another table, select from the secondary menu to add fields you want in the view.

6. To delete fields, highlight the field you want to delete in the **Destination Fields** window and click **Remove Field**.
7. To move a field location up, highlight the field you want to move in the **Destination Fields** window and click **Move Field Up**.
8. To move a field location down, highlight the field you want to move in the **Destination Fields** window and click **Move Field Down**.
9. Click **Next**.
10. Click **Save**.

Service Manager updates the View record.

11. Click **OK**.

Change roles for a view

Applies to User roles:

System Administrator

To change roles for a view, follow these steps:

1. Click **System Administration > Base System Configuration > Miscellaneous > Views/Favorites**.
2. Click **Search** to find a view.
3. Select the view to updated from the records list.
4. In the **Audience** tab, make the applicable updated.
5. Click **Save**.

HP Service Manager updates the View record.

6. Click **OK**.

Autoformatting

Autoformatting is part of a view in that it is a view that has been customized by a set of rules that specify certain display conditions for records that satisfy the conditions. For example, you can create a view that displays all incident records older than one week and then in that view create an autoformatting rules that displays records as red if their urgency is critical.

System administrators access autoformatting by selecting **Customize Current View** from the **More Actions** menu for a view or queue.

Add a new autoformatting rule

Applies to User Roles:

System Administrator

To add a new autoformatting rule, follow these steps:

1. From the System Navigator, click **Service Desk > Interaction Queue**.
2. From the Queue menu, select **Approval** to open the Approval Queue.
3. Click **More** or the **More Actions** icon, and then **Customize Current View**.

The **Configure View Properties** wizard opens.

4. Click the **Autoformat** button.
5. Click the **Add Rule** button to open a new autoformat rule.
 - a. Type a name in the name field.
 - b. Select a color from the list in the Color field.
 - c. Select a field for your new rule in the Field list.
 - d. Select an operator in the Operator field, such as `starts with`.
 - e. In the next field, select a comparison value, such as `a` to establish the rule `starts with` the letter `a`.
6. Click **Next** to view a list of current rule definitions. The Configure Autoformat Rules form opens.

You can use this form to perform the following operations:

- Add, edit, or remove autoformatting rules
 - Move the order of rules up or down; the first in the order overrides the others
 - Return to the main **Configure View Properties** wizard form
7. Click **Next** to return to Configure View Properties.

8. Click **Next** for the new rule to take effect.

The records that match your rule criteria now display in the color selected for this rule.

Adjust the order of an autoformatting rule

Applies to User Roles:

System Administrator

To adjust the order of an autoformatting rule, follow these steps:

1. From the System Navigator, click **Service Desk > Interaction Queue**.
2. From the Queue menu, select **Approval** to display the Approval Queue.
3. From the next Queue menu, select **Incident** to view the Incident queue.
4. From the View menu, select a view, such as **Autoformat date view**.

Note the existing autoformatting rules defined.

5. Click **More** or the **More Actions** icon, then **Customize Current View**.

The **Configure View Properties** wizard opens.

6. Click **Autoformat**.
7. Select a rule to adjust the order of and click the **Move Up** or **Move Down** button to adjust the order of the rule.

Note that the first rule in the order overrides all others in the record list.

8. Click **Finish** to return to the Incident queue.

Edit an autoformatting rule

Applies to User Roles:

System Administrator

To edit an autoformatting rule, follow these steps:

1. From the System Navigator, click **Service Desk > Interaction Queue**.
2. From the **Queue** list, click **Approval** to open the Approval Queue.
3. From the next **Queue** menu, click **Incident** to view the Incident queue.
4. From the next **View** menu, select a view, such as **Autoformat date view**.

Note the existing autoformatting rules defined.

5. Click **More** or the **More Actions** icon, then **Customize Current View**.

The **Configure View Properties** wizard opens.

6. Click the **Autoformat** button.
7. Select a rule to edit and click the **Edit** button.

The **Autoformat Rule** wizard opens.

8. In the name field, you can optionally change the name of the rule.
9. For the rule to be active, select the **Is Active** check box. For the rule to be inactive, clear the **Is Active** check box.
10. In the **Color** field, you can optionally modify the color in which the rule appears in the queue by using the color selections.
11. Optionally modify the field name by using the field selections.
12. In the **Operator** field, you can optionally modify the operator to use for this rule.

Valid options for operators in autoformatting rules are:

- On
 - On or After
 - On or Before
 - Is Between
13. You can optionally modify the date in the date field by selecting a date using the calendar widget or by manually typing in a new date.
 14. Click **Next** to view your modified rule definition.
 15. Click **Finish**.
 16. From **Specify View Type**, select **Save as a system view** or **Save as a personal view**.
 17. Click **Finish** to return to the Incident queue and view your changes.

Remove an autoformatting rule

Applies to User Roles:

System Administrator

To remove an autoformatting rule, follow these steps:

1. From the System Navigator, click **Service Desk > Interaction Queue**.
2. From the Queue menu, select **Approval** to open the Approval Queue.
3. Click **More** or the More Actions icon, then **Customize Current View**.

The Configure View Properties wizard opens.

4. Click the **Autoformat** button.
5. Select the rule to remove.
6. Click **Remove Rule**.
7. Click **Yes** to confirm your choice.

Customize current view

System administrators use the Customize Current View feature to modify the properties of an existing view. In this case, a view is a query that has been saved to generate a list of records. The out-of-box system provides a set views that may include My tasks or All my open request. The View field in an application lists the views available for the user.

System administrators can access Customize Current View from the **More Actions** menu on any of the display views, queues, or record lists for any of the applications. The system provides a wizard to configure the view properties.

Chapter 10: ITIL Alignment

HP Service Manager is fully aligned with ITIL terms and definitions. The following features of Service Manager are good examples of alignment with ITIL:

- Detailed descriptions of the focus of each ITIL process and supporting module in Service Manager. This includes the scope of the function or process, the goals, the roles and thus profiles typically required to deliver the function and their responsibilities. This information is included in the help server.
- Process diagrams that define the out-of-box process flows to deliver the function are included in the help server.
- The screens, work flows, profiles and system logic is pre-defined in the Service Manager system to deliver the functions as described in the help server.

Access Control

Authorized users can create, modify, and close records through the different HP Service Manager modules. Access to functionality within each module is governed by Service Manager security utilities, which define access based on role; for example, one user may be able to create and modify, but not close, records.

Service Manager security utilities govern access to modules, functionality within modules, and underlying data.

Mandatory Fields

HP Service Manager provides two basic methods for setting field-level controls including making a field mandatory. The system provides two methods to indicate that a field is mandatory in the user interface.

If the field is only required to be mandatory on a screen-by-screen basis, the field can be set as mandatory using the format control validations. This control can be visually indicated by a property in Forms Designer.

If the field needs to be set as mandatory for all access points throughout the system, a data policy for the field can be set using the supplied configuration tools. In this case the visual indication is automatic.

On screen, Service Manager identifies mandatory fields with a red asterisk indicator.

Reporting

HP Service Manager includes two options for generating management reports using key performance indicators: Service Manager Dashboard queries and charts, Reporting, and Service Manager Crystal Reports. These tools allow you to generate predefined and ad hoc reports to display any information. The following describes these tools.

Service Manager Reports

The Service Manager Reports module provides reports and dashboards to enable faster analysis and improved time to resolution. These reports organize data into various chart formats, and the dashboards display one or more reports to provide global information about critical activities or metrics. These reports display relationships among categories of data. For example, one report might display the number of incidents per customer, while another displays the number of incidents by priority. Viewing these reports together as a dashboard enables you to make better business decisions, such as assigning resources to close incidents. Report Managers can share a report or dashboard.

The Service Manager Reports module aims to provide a lightweight reporting feature for active operational data, and the reports are therefore designed to retrieve, represent and visualize up to 100,000 active records out of millions. To define analytical reports against the entire data set, you need to use a third-party business intelligence tool.

Service Manager Crystal Reports

For operational reporting or regularly scheduled reporting requirements, HP provides an OEM version of Crystal Reports with Service Manager. HP also delivers over 40 predefined reports. You can run reports on an ad hoc basis and system administrators can define an automatic report-generation schedule using the Service Manager Report Scheduler tool. Crystal Reports 2008 is required to view, generate, or modify these reports and is included with Service Manager.

Service Manager ships with the following predefined reports:

- Request Management Reports
 - Request Aging Report
- Service Desk Reports
 - Escalated Interactions
 - First Time Fixed Interactions

- Interactions Closed in a Given Year
- Interactions Resulting in Related Issues
- Number of Service Desk Requests by Department
- Service Desk Interactions Opened and Closed
- Top 20 Operators by Average Interaction Time in Last 90 Days
- Change Management Reports
 - Changes Closed Meeting SLM Target
 - Changes Scheduled for This Week
 - Changes Opened and Closed
 - Percentage of Emergency Changes
 - Percentage of Rejected Changes
 - Percentage of Successful Changes
- Configuration Management Reports
 - CI Relationships
 - CI Summary
 - Percentage of CIs Related to Other CIs
- Incident Management Reports
 - Backlog of Incidents
 - Incidents Opened and Closed
 - Incident Aging Report
 - Incident Reassignment Analysis
 - Incidents by Assignment and Priority

- Incidents Closed Meeting SLA Target
- Open and Closed Incidents by Service
- Open Incidents Monthly Analysis by Category
- Percentage of Incidents by Priority
- Reopened Incidents
- Knowledge Management Reports
 - Knowledge Management Activity
 - Knowledge Management Demand
 - Knowledge Management Summary
 - Knowledge Management Usage by Department
 - Self-Service Escalated Knowledge Management Search Escalation
 - Self-Service Knowledge Management Search History
- Problem Management Reports
 - Average Time to Diagnose
 - Open and Closed Problems by Service
 - Problems Opened and Closed
 - Problems Closed Meeting SLA Target
- Service Level Management Reports
 - Service Level Management Availability Duration Metrics
 - Service Level Management Availability Uptime Metrics
 - Service Level Management Response Metrics
 - Service Level Management Summary

In addition, you can perform a search within each module using different combinations of conditions, and the search results can be presented in list or chart.

You can also create your own management reports using Crystal Report and build your reports on any field in the database.

Management Reporting

HP IT Executive Scorecard

The HP IT Executive Scorecard is a key element in the HP IT Performance Suite and is a systematic approach to digitizing the sensing, measuring, and instrumentation of the entire IT-controlled landscape into single consolidated views for IT leaders and practitioners. The HP IT Performance Suite includes comprehensive families of proven software for strategy, planning, and governance, application lifecycle management, IT operations, information management, security intelligence, and risk management. These solutions are unified by one of the most complete IT data models for collecting and relating data feeds from individual products.

What makes the HP IT Performance Suite much more than just a collection of management software is the HP IT Executive Scorecard—a single pane of glass that pulls all the information and analysis together. In short, HP IT Executive Scorecard can help track performance and communicate in business terms.

The HP IT Executive Scorecard allows companies to:

- Use a single pane of glass to view IT business services, programs, and financial status
- View performance and problem areas promptly
- Show historical data to highlight improvements and identify negative trends early
- Automate and decrease effort required for the data-gathering process to enable real-time reporting
- Cascade key performance indicators (KPI) across layers of scorecards
- Collaborate by adding annotations to KPIs and objectives
- Access the information from a desktop, tablet, or smartphone
- Add notes using collaboration in the context of a KPI or objective

With its balanced scorecard, best-practice dashboards, and over 135 key performance indicators already defined, the HP IT Executive Scorecard is a unique differentiator. The HP IT Executive Scorecard

is an analytical product that renders performance from a broad range of data sources, including (but not limited to) HP Business Service Management, HP Service Manager, HP Asset Manager, and HP Project and Portfolio Management.

From a business point of view, the need to control information technology (IT) is driving a new level of maturity in performance management. Many organizations turn to executive scorecards to help drive performance and more are now pouring this approach into the context of IT. The out-of-box Scorecards in the HP IT Executive Scorecard are based around up to four high-level perspectives. These equate to high-level goals of IT or the business. The four used in HP IT Executive Scorecard are: IT Value, Customer, Operational Excellence, and Future Orientation.

The scoring of those objectives is based on one or more KPIs. In this way, the persona can gain a quick view of overall performance in an area of interest and drill down further if required into the KPI or KPIs that are responsible for the performance score.

KPIs reflect how well the organization is doing in areas that most impact financial measures valued by shareholders, such as profitability and revenues.

A KPI evaluates the performance according to expectations. The context is provided using:

- Thresholds, which defines upper and lower ranges of acceptable performance
- Targets, which records the predefined gains, such as 10 percent new customers per quarter
- Benchmarks, which is based on industry wide measures or various methodologies, such as Six Sigma
- Trend, which is the direction of the performance of the KPI, either Up, Down, or Static

A KPI is a Metric, but a Metric is not always a KPI. The key difference is that KPIs always reflect strategic value drivers whereas Metrics represent the measurement of any business activity. Metrics always show a number that reflects performance. KPIs put that performance in context. Metrics are not matched against a threshold. An example of a metric could be an MTTR (mean time to recover) which measures the average time between the occurrence of a set of incidents and their resolution. An example of a KPI could be an MTTR, which measures the average time between the occurrence of a set of incidents and their resolution, compared to a defined threshold. For example, MTTR less than one hour.

The out-of-box KPIs can be altered to suit different personas or augmented by new KPIs created within HP IT Executive Scorecard.

Audit Trail

For all records in HP Service Manager, a date time stamp and a user stamp are updated in the record when it is created or saved.

Service Manager provides an audit trail capability that identifies each step taken in the resolution of a record. Each time the record is updated (whether manually or automatically), a separate historical activity is created for the record. An authorized user may review each historical activity to develop a comprehensive understanding of the history of the record and its resolution, including which operators took what actions at what times. These updates are displayed into an aggregated journal of all updates.

Service Manager also provides an auditing feature that records modifications to fields within the Service Manager database. Field modifications are detected by comparing the fields in the original version of a record to the updated version. When modifications are detected, an Audit Log entry is recorded for each changed field showing the name of the modified field, the old and new version of the data, the current date/time, and the current operator's user ID.

Archiving

Closure of processed problems, incidents, changes, interactions, and other records is a standard part of the workflow for each module. Typically, the closure action not only supports saving the record but separate validations, rules, and possibly even separate forms to help ensure business success.

The most typical approach for archiving records is to leverage the chosen RDMS tools from Oracle, MS SQL or DB2 to perform database administration for purging and archiving.

HP Service Manager provides an archive and purge tool that can be configured by table and criteria for archiving. This is a facility only the administrator would use. This capability allows the ability to archive either manually or on a scheduled basis.

One new capability in this area is the ability to take advantage of the HP archive tool suite. These tools allow data to be archived out of Service Manager into a system-accessible file system. The production or alternative instance of Service Manager can then be used to access these data records. See the link below for additional details.

Notification and Escalation

HP Service Manager provides alerts and escalations in the following ways:

- Notifications

Service Manager provides a broad and deep solution to deliver notifications to stakeholders whenever a record is opened, updated or closed. The notification engine allows administrators complete control over the following:

- a. What notification vehicle and format to deliver
- b. What conditions on which to send the notification
- c. To whom the notification should be sent

- Alerts

Modules include the ability to set criteria for the generation of alerts. For example, the administrator can set rules for three stages of alert and a deadline condition. When these targets are met, specified users receive alerts and notifications through the Service Manager tool, email, etc.

- Escalations

Business rules can be used to trigger automated escalations of records under various conditions. Examples include: should the status remain unchanged for too long; the record reassigned too often between assignment groups; or for other rules as defined. In addition, to document the violation of these rules the administrator can configure Service Manager to act in certain ways should these rules be breached. For example, if a record remains in open state for too long, reassign it to the assigned user's manager.

- Service Level monitoring

Alerts and escalations can be triggered through evaluation of Service levels as defined in the Service Level Management module. This approach is used to set Service Level Objectives and Service Level Agreements with associated actions should service levels approach breach conditions. In this way, escalation is accomplished proactively to avoid breach rather than react to breach.

Send Documentation Feedback

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

Feedback on Application Setup help topics for printing (Service Manager 9.41)

Just add your feedback to the email and click send.

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

We appreciate your feedback!

